ITU STUDY GROUP Q.22/1 REPORT ON BEST PRACTICES FOR A NATIONAL APPROACH TO CYBERSECURITY: A MANAGEMENT FRAMEWORK FOR ORGANIZING NATIONAL CYBERSECURITY EFFORTS

ITU-D SECRETARIAT DRAFT JANUARY 2008

International Telecommunication Union

www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf

Acknowledgements

This document is an ITU-D secretariat-based derived base version of the October 2007 draft of the *Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts*. It is based on studies underway in the ITU Telecommunication Development Sector's Study Group 1, Question 22/1: *Securing information and communication networks: best practices for developing a culture of cybersecurity*.

This activity calls for ITU Member States and Sector Members to create a report on national best practices in the field of cybersecurity. More information on Question 22/1 activities can be found at the website www.itu.int/ITU-D/cyb/cybersecurity/.

As a practical initiative by the ITU-D ICT Applications and Cybersecurity Division to assist ITU Member States who wish to elaborate national cybersecurity/critical information infrastructure protection (CIIP) frameworks, this draft is derived from work currently underway in Question 22/1.

This document is formatted to be printed recto-verso.

The latest version of this document is available at:

www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf

For further information on this document, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland

Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

TABLE OF CONTENTS

Introduction

This report provides national administrations with a management framework for addressing cybersecurity at the national level and for organizing and implementing a national cybersecurity strategy. As existing national capabilities vary greatly and threats constantly evolve, the report does not provide a prescriptive approach to securing cyberspace. Rather, the framework describes a flexible approach that can assist national administrations to review and improve their existing institutions, policies, and relationships addressing cybersecurity issues.

Although this report is focused on cybersecurity, we note that protection of physical network assets is an equally important priority. We also note that best practices in cybersecurity should in no way suppress freedom of speech, free flow of information and/or due process of law.

The five key elements outlined in this report are:

- Developing a National Strategy for Cybersecurity;
- Establishing National Government–Industry Collaboration;
- Deterring Cybercrime;
- Creating National Incident Management Capabilities; and
- Promoting a National Culture of Cybersecurity.

Each of these elements form part of a comprehensive national approach to cybersecurity.

For the purposes of this report, *cybersecurity* is defined as the *prevention of damage to, unauthorized use of, exploitation of, and -- if needed -- the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems*.

As there is sometimes confusion, it is useful to have an overview of the relationship between the terms cybersecurity, critical infrastructure (CI), critical information infrastructure (CII), critical information infrastructure protection (CIIP) and non-critical infrastructure. These are discussed in more detail and illustrated in Figure 1 below.

While definitions may vary slightly, ***critical infrastructures*** (CI) are generally considered as the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these. CI are composed of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data). What constitutes "critical" may vary from country to country, but typically might include elements of information and communications technologies (ICT), energy, banking, transportation, public health, agriculture and food, water, chemical, shipping, and essential government services sectors. Countries at all stages of development need to plan for and develop policies to protect what they determine to be their CI in order to provide reasonable assurance of resilience and security to support national missions and economic stability.

Each of these economic sectors has its own physical assets, such as bank buildings, power plants, trains, hospitals and government offices. However, these critical sectors of a nation's economy all depend upon information and communication technologies. Across the board, these sectors and their physical assets today depend upon the reliable functioning of this ***critical information infrastructure*** (CII) to deliver their services and to conduct business. Consequently, significant disruption to this CII could have an immediate and debilitating impact that reaches far beyond the ICT sector and affects the ability of a nation to perform its essential missions in multiple sectors. A ***critical information infrastructure protection*** (CIIP) program is intended to protect the virtual component of CII.

Cybersecurity protects against all forms of cyber incidents by strengthening the safety of the critical information infrastructure on which critical sectors depend and securing the networks and services which serve the day-to-day needs of users. Cyber incidents may affect the critical and non-critical information infrastructures alike and may take many forms of malicious activity such as use of botnets to conduct denial of service attacks and distribute spam and malware (e.g. viruses and worms) which affect the ability of the networks to operate. In addition, cyber incidents may include illicit activities such as phishing and pharming, as well as identity theft. The cyber threat continues to increase as the tools and methodologies used become more and more widely available, and the technical capability and sophistication of cyber criminals expand. Countries at all stages of development have experienced these cyber incidents.

A national approach to cybersecurity includes raising awareness about existing cyber risks, creating national structures to address cybersecurity, and establishing the necessary relationships that may be utilized to address events that occur. Assessing risk, implementing mitigation measures, and managing consequences are also part of a national cybersecurity program. A good national cybersecurity program will help protect a nation's economy from disruption by contributing to continuity planning across sectors, protecting the information that is stored in information systems, preserving public confidence, maintaining national security, and ensuring public health and safety.

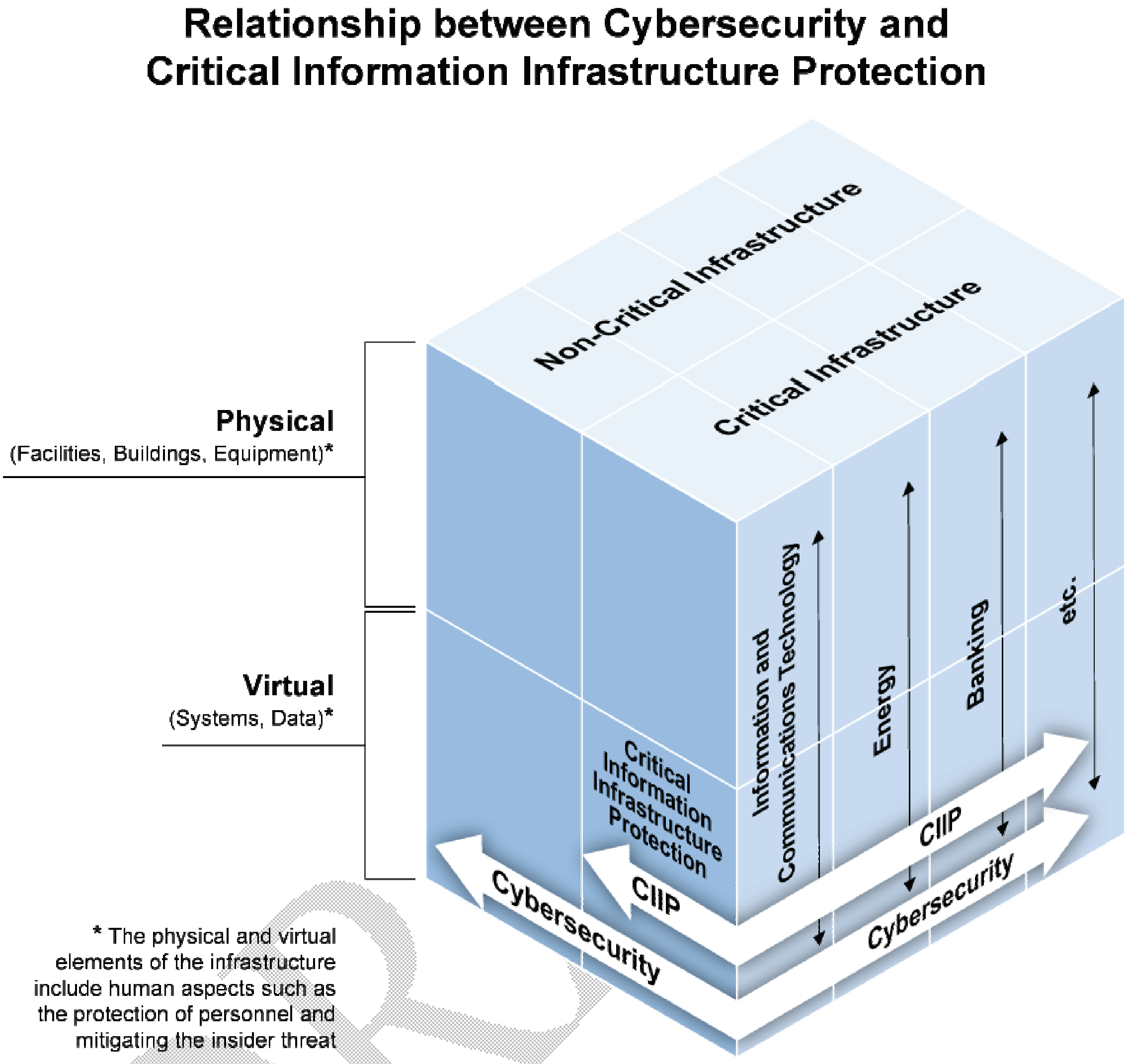
Relationship between Cybersecurity and
Critical Information Infrastructure Protection
Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat
Non-Critical Infrastructure
Critical Infrastructure
Information and Communications Technology
Energy
Banking
etc.
Critical Information Infrastructure Protection
CIIP
Cybersecurity
CIIP
Cybersecurity

Figure 1: The Conceptual Relationship Between Critical Information Infrastructure Protection and Cybersecurity.

Part I: Developing and Obtaining Agreement on a National Cybersecurity Strategy

Developing and implementing a national cybersecurity plan requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, industry, and citizens) in the process.

Background

For reasons of national security and economic well-being, governments need to enable, promote, and ensure the protection of their critical information infrastructures. Today, information infrastructures cross nations' industrial sectors and national borders. The ubiquity of the critical information infrastructures creates tremendous opportunity and economic advantages. With these benefits also come interdependencies and risks.

For many years most nations have treated the national public switched telephone network (PSTN) as a critical infrastructure and have protected it accordingly. In many countries, commercial firms own significant portions of this PSTN infrastructure and have cooperated with the government and each other in this effort. However, the rapid rise of digitally-based ICTs in interconnected wired and wireless communication networks has dramatically changed the nature and requirements for network security and may have made traditional PSTN-based security policies and procedures insufficient to meet new requirements for such security.

The changes brought about by ICTs require a much greater emphasis on cooperation by governments, businesses, other organizations and individual users who develop, own, provide, manage, service, and use information systems and networks. While governments often continue to have the lead role in establishing public policy related to network security, it is critical to ensure that other stakeholders, including infrastructure operators and vendors, are integrated into the overall planning and policy process. By working together, government and industry can effectively leverage their respective expertise and manage CII risks. This integration fosters increased trust and ensures that policies and technologies are developed and applied in the appropriate and most effective manner. At the international level, protecting critical information infrastructures and enhancing cybersecurity requires cooperation and coordination among nation states and with international partners[1].

A. Overview of the Goals under this Part

<u>I.A.1.</u> Create awareness at a national policy level about cybersecurity issues and the need for national action and international cooperation.

<u>I.A.2.</u> Develop a national strategy to enhance cybersecurity to reduce the risks and effects of both cyber and physical disruptions.

<u>I.A.3.</u> Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents.

B. Specific Steps to Achieve these Goals

The foregoing goals are common to all countries; however, the specific steps taken to implement these goals will vary according to each country's unique needs and circumstances. In many countries, the national government will undertake these steps.

<u>I.B.1.</u> Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy-level discussions.

1. For a nation seeking to enhance cybersecurity and secure its critical information infrastructure, a first step is to establish cybersecurity as national policy. In general a national cybersecurity policy statement (1) recognizes the importance of CII to the nation, (2) identifies the risks it faces (usually an all-hazards approach2), (3) establishes the cybersecurity policy goal, and (4) broadly identifies how it will be implemented, including through collaboration with the private sector.

[1] For example, the ITU has several initiatives underway to support these international efforts including ITU-D Programme 3, WTDC Resolution 45 (Doha, 2006), ITU Plenipotentiary Resolution 130 (Antalya, 2006) and activities in ITU-T Study Group 17.

2. Once an overall cybersecurity policy is clearly defined, it can be amplified by a national strategy that delineates roles and responsibilities, identifies priorities, and establishes timeframes and metrics for implementation. Additionally, the policy and strategy may also place the national efforts in the context of other international cybersecurity activities. In order to achieve an overall cybersecurity policy, it may be necessary to raise awareness of the issues among key decision makers. The decision makers need to understand that it may take several years or more to achieve the agreed upon cybersecurity goals.

3. A national cybersecurity framework should not be comprised of immutable policies. Instead, the framework and policies should be flexible and able to respond to the dynamic risk environment. The framework should establish policy goals. By establishing clear policy goals, government agencies and non-government entities can work together to achieve the stated goals in the most efficient and effective manner.

4. The national policy should be developed cooperatively through consultation with representatives of all relevant participant groups including government agencies, industry, academia, and relevant associations. Promulgating the resulting policy at the national level, preferably by the head of government, encourages the cooperation of all participants. Such promulgation should be adaptive and integrate state, local, and community-based approaches based on national needs and contexts.

<u>I.B.2.</u> Identify a lead person and institution for the overall national effort; determine where within the government a Computer Security Incident Response Team[3] with national

[2] An *all-hazards* or *multi-hazards* approach to risk management includes consideration of all potential natural and technological hazards; this includes natural and manmade (accidental or intentional) emergencies and disasters.

[3] A CSIRT is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and assist their constituents to recover from breaches (A Step-by-Step Approach on How to Set Up a CSIRT is at (www.enisa.europa.eu/pages/05_01.htm). CSIRTS are also sometimes called Computer Emergency Response Teams or Computer Emergency Readiness Teams (CERTs), CSIRTS and CERTS perform the same function.

responsibility[4] should be established; and identify lead institutions for each aspect of the national strategy.

1. The launch of a cybersecurity initiative requires the identification of someone to lead the national cybersecurity effort, a person in government at the policy level who understands the issues of cybersecurity and who can direct and coordinate the efforts of governmental institutions and can effectively collaborate with industry. Ideally this person should have political stature and a close relationship with the head of government. This high-level authority is necessary to ensure the coordination among entities that currently may seldom interact. In time, this coordination effort will provide an institutional foundation on which the country's cyber security technical leaders and organizations can build. Once the nation has organized itself for cybersecurity, the person or institution that launched the effort may no longer need to play the key or lead role.

2. Other institutions responsible for developing and implementing different parts of a national security strategy must be identified.

I.B.3. Identify the appropriate experts and policymakers within government ministries, government, and private sector, and their roles.

1. Effective national action requires the inculcation of a "culture of cybersecurity" among all participants. All individuals and institutions within government and outside of government that develop, own, provide, manage, service, and use information systems and networks must understand the role they need to play and the actions that need to be taken. Senior policymakers and industry leaders must establish goals and priorities within their institutions. Senior technical experts must provide guidelines and frameworks for action.

I.B.4. Identify cooperative arrangements for and among all participants.

1. National government should foster both formal and informal collaborative arrangements that permit and encourage communication and information-sharing between industry and government. Cybersecurity will be implemented at the technical or tactical

[4] For the purposes of this Report, a nationally designated CSIRT will be referred to as an "N-CSIRT."

level by a wide array of institutions, both governmental and non-governmental. These efforts must also be coordinated and include mechanisms for information sharing.

I.B.5. Establish mechanisms for cooperation among government and private sector entities at the national level.

1. Policy development and the elaboration and implementation of the national plan must be undertaken through open and transparent processes. These efforts must take into account the views and interest of all participants.

I.B.6. Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts[5].

1. The effort to improve national cybersecurity will be helped by participating in regional or international forums that can provide education and training, often in the form of conferences and workshops. Such forums raise awareness of the issues, provide expert presentations and permit countries to share their ideas, experiences and perspectives. Participation and/or membership in regional as well as international organizations working toward similar goals can also assist in this effort.

2. Participation in available programs and activities of multilateral organizations that seek to improve and enhance global cybersecurity—such as the International Telecommunication Union (ITU) -- is another way to foster international collaboration. Other examples of multilateral organizations include the Organization for Economic Cooperation and Development (OECD), Organization of American States (OAS), and Asia-Pacific Economic Cooperation (APEC). In addition, there are other conferences where governments can share information on cybersecurity issues, such as the Meridian Conference.

3. In addition, participation in industry-led efforts, such as the Anti-Phishing Working Group and other similar international endeavours, also should be considered.

[5] Activities relating to follow-up on ITU Plenipotentiary Resolution 130 may be considered relevant.

I.B.7. Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity.

1. Only by understanding risks can government and infrastructure owners and operators (including the vendors who support them) begin a government-industry collaboration to identify and prioritize key functions and elements for protection. Once identified, the critical information infrastructure functions can be prioritized or ranked as to which is most important and in what context. It is important to remember that the notion of “criticality” is situation-dependent, and what could be critical in one instance may not be critical in the next. As nations identify and prioritize critical functions, they need to remember that criticality will change with technology, infrastructure, and process enhancements.

2. Achieving the protection of CII and cyberspace is very challenging. Protecting CII and cyberspace and the critical functions comprised therein involves the continuous application of a series of risk management practices (i.e., assessing threat, vulnerability, and consequence, identifying controls and mitigations, implementing controls, and measuring effectiveness) that enable operators to manage risks and ensure resilience across their essential missions. Individually, information infrastructure providers generally have sophisticated risk management methodologies and practices in place because of the real-time nature of the services they deliver. However, the interconnectivity, interdependence, and technical complexity of the information infrastructure limit the ability to easily assess overall risk or readiness. As a result, there is a significant benefit to leveraging public-private collaborations to assess the shared dependencies and infrastructure risks (natural disaster, technological failure, terrorist attack, etc.).

I.B.8. Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities.

1. The national cybersecurity strategy should include a national assessment survey, which could be used for self-evaluation of progress being made or as part of training or supported assessment effort. By utilizing a common self-assessment tool, countries can identify strengths and potential gaps in their national framework and establish a process for aligning them with their desired goals. (A self-assessment tool may be developed by Q.22 to accompany this best practices document.)

I.B.9. Identify training requirements and how to achieve them.

1. As a result of comparing the recommended best practices contained in this report with its current cybersecurity practices (i.e., conducting a gap analysis), a country may find there are aspects of its cybersecurity program that need improvement. The solution may be technical (for example, new equipment or software), legal (e.g., drafting new laws or regulations to address inappropriate cyber conduct), or organizational. A gap analysis is also likely to reveal where additional human capacity building (training) is needed.

C. Reference Material for Additional Information on this Topic

I.C.1. Awareness raising (I.B.1, I.B.2)

- UN World Summit on the Information Society Declaration of Principles and Plan of Action: www.itu.int/WSIS/
- ITU Development Sector Cybersecurity website: www.itu.int/ITU-D/cyb /
- ITU Cybersecurity Gateway: www.itu.int/cybersecurity/gateway/
- OECD Guidelines and Culture of Security: www.oecd.org/sti/cultureofsecurity
- UNGA Resolutions 55/63, 56/121, 57/239, 58/199: www.un.org/Depts/dhl/resguide/gares1.htm
- The (U.S.) National Strategy to Secure Cyberspace: www.dhs.gov/interweb/assetlibrary/national_Cyberspace_Strategy.pdf
- United States Sector Specific Plans: www.dhs.gov/xprevprot/programs/gc_1179866197607.sthm
- Information Technology Association of America White Paper on Information Security: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- "Information Society in an Enlarged Europe," Budapest, 2/26/04: ec.europa.eu/archives/commission_1999_2004/liikanen/media/speeches/
- "i2010: How to Make Europe's Information Society Competitive," Brussels, 2/22/05: europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/05/107&type=HTML&aged=0&language=EN&guiLanguage=en
- European Network and Information Security Agency: www.enisa.europa.eu/
- The Meridian Conference: www.meridian2007.org

I.C.2. National Strategy (I.B.2, I.B.3, I.B. 4, I.B.5, I.B.7)

- U.S. National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb/
- National Implementation Strategies of 11 OECD members: www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- UK Centre for the Protection of National Infrastructure (CPNI): www.cpni.gov.uk/
- UK Critical Information Infrastructure Protection Directory (government only) - to participate or obtain information email: ciip-directory@niscc.gov.uk
- New Zealand: www.digitalstrategy.govt.nz
- Canada: www.psepc-sppcc.gc.ca

I.C.3. Assessment and program development (I.B.5, I.B.7, I.B.8)

- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program, **October 2003**
- NIST SP 800-30 Risk Management Guide for Information Technology Systems: July 2002
- Control Objectives for Information and Related Technology (COBIT) 3.0/4.0
- Disaster Recovery Institute International (DRII)
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 Series, Information technology—Security techniques—Information security management systems
- ISO/IEC 13335, Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management
- ISO/IEC 17799, 2005 Information technology—Security techniques—Code of practice for information security management
- ISO/IEC 21827, Systems Security Engineering—Capability Maturity Model (SSE-CMM®)
- Information Technology Infrastructure Library (ITIL) Security Management
- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems
- NIST Draft Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

I.C.4. International assistance points of contact (I.B.6)

- Forum of Incident Response Security Teams (FIRST): www.first.org
- Anti-Phishing Working Group: www.antiphishing.org
- World Information Technology Services Alliance: www.witsa.org
- Internet Engineering Task Force: www.ietf.org
- World Wide Web Consortium: www.w3c.org
- Institute of Electrical and Electronics Engineers: www.ieee.org
- Messaging Anti-Abuse Working Group: www.maawg.org

[**Remark:** This reference list of materials will be updated regularly, taking into consideration the outputs of the ITU Global Cybersecurity Agenda, the project implementing Resolution 45 (WTDC-06), the work carried out by ITU-T Study Group 17, the leading Study Group on security in ITU-T, as well as the follow-up on WSIS Action Line C5 on cybersecurity and the results of the work on relevant ITU PP-06 Resolutions, such as Resolutions 130 and 149.]

Part II: Establishing National Government-Industry Collaboration

Protecting critical information infrastructure and cyberspace is a shared responsibility that can best be accomplished through collaboration between government at all levels and the private sector, which owns and operates much of the infrastructure. It is important to recognize that although the world's information security systems have largely become an interoperable and interconnected whole, the structure of this network can vary greatly from country to country. Therefore, an effective and sustainable system of security will be enhanced by collaboration among owners and operators of these systems.

Background

Both the government and industry have an enduring interest in assuring the resilience of the infrastructure. Accordingly, government-industry collaboration is fundamental to enhancing cyber security because no one entity alone can protect the entire infrastructure. As much of the cyber infrastructure in many countries is owned and/or operated by industry, it is imperative that government and industry work together in a meaningful way. Successful government-industry collaboration requires three important elements: (1) a clear value proposition; (2) clearly delineated roles and responsibilities; and (3) trust.

Value proposition

The success of the partnership depends on articulating the mutual benefits to government and industry partners. The benefits to governments are that infrastructure vendors and operators provide capabilities that typically fall outside government's core competencies, such as:

- Ownership and management of the majority of the critical infrastructure in many sectors, in many countries;
- Understanding of assets, networks, systems, facilities, functions, and other capabilities;
- Incident response expertise and experience;
- Ability to innovate and provide products, services, and technologies to quickly focus on requirements; and
- Design, deployment, operation, administration and maintenance of the global Internet.

In assessing the value proposition for industry, there is a clear benefit to working with government to enhance CIIP and cybersecurity. Governments can bring value to the collaborative relationship in a number of ways, which include:

- Providing owners and operators with timely, analytical, accurate, aggregated, and useful information on critical infrastructure threats;
- Engaging industry at the outset in the development of CIP initiatives and policies;
- Articulating to corporate leaders, through the use of public platforms and direct communications, both the business and national security benefits of investing in security measures that exceed their specific business strategies;
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices and, as needed, to update and enhance their security operations and practices beyond what their parochial business interests demand;
- Working with industry to develop and clearly prioritize key missions and enable their protection an/or restoration;
- Providing support for research needed to enhance future CI protection efforts;
- Identifying the resources to engage in cross-sector interdependency studies, through exercises, symposiums, training sessions, and computer modelling, that result in guided decision support for business continuity planning; and
- Enabling time-sensitive information sharing as well as restoration and recovery support to priority infrastructure facilities and services during an incident.

Roles and Responsibilities

Together, government and industry can develop a common understanding of their respective roles and responsibilities related to cybersecurity. The government can provide coordination and leadership of protection efforts. For example, continuity of government requires ensuring the security and availability of governments' cyber and physical infrastructure necessary to support its essential missions and services. In addition, the government can play a key coordinating role during a catastrophic event or it can help in instances when industry lacks sufficient resources to respond to an incident. The government can promote and encourage voluntary private sector efforts to improve security, including establishing the policies and protocol needed to share timely analytical and useable information about threats, and providing incentives for industry to enhance security beyond what their corporate interests demand. Finally, the government can sponsor and fund studies and research and development to improve security processes and tools.

Trust

A fundamental element of successful collaboration between government and industry is trust. Trust is necessary for establishing, developing, and maintaining sharing relationships between government and industry. Robust collaboration and information exchange between industry and government enhances situational awareness, facilitates cooperation on strategic issues, helps manage cyber risk and supports response and recovery activities. Through improved information sharing and analysis, the government and industry will be better equipped to identify threats and vulnerabilities, and to exchange mitigating and preventive tactics and resources.

Listed below are general goals which governments should consider as they collaborate with industry.

A. Overview of the Goals under this Part

II.A.1. **Develop government-industry collaborative relationships that work to effectively manage cyber risk and to protect cyberspace.**

II.A.2. **Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.**

B. Specific Steps to Achieve these Goals

II.B.1. **Include industry perspectives in the earliest stages of development and implementation of security policy and related efforts.**

1. In many countries, most critical infrastructures, and the cyber elements on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from private sector innovation. Therefore, governments alone cannot sufficiently secure cyberspace. Awareness of industry perspectives and inclusion of the primary owners and operators of critical infrastructure are invaluable for government cybersecurity efforts to develop and implement cyber security policy and frameworks for risk management. Governments can be informed by industry through participating in government-industry working groups, soliciting comments from industry for cyber security policy and strategy development, and coordinating efforts with private sector organizations through information sharing mechanisms. Government should ensure that the private

sector is engaged in the initial stages of the development, implementation, and maintenance of initiatives and policies.

2. Governments and industry should collaboratively adopt a risk management approach that enables government and the private sector to identify cyber infrastructure, analyze threats, assess vulnerabilities, evaluate consequences, and identify mitigations.

3. Governments and industry should collaboratively pursue research and development (R&D) activities that seek to manage cyber risk. Visibility into R&D priorities and initiatives being undertaken by the private sector and government can ensure that resources are allocated and used efficiently, that R&D initiatives are developed on a timely basis, and ultimately, that products and services are in the pipeline in time to enhance national cyber security.

II.B.2. Encourage development of private sector groups from different critical infrastructure industries to address common security interests collaboratively with government.

1. The formation of these groups, such as business associations, in various critical infrastructure sectors can help to address common cybersecurity needs. These groups may focus on strategic and/or operational issues and management of security concerns relative to the industry as a whole. These issues may include risk management, awareness, policy development and implementation, and a multitude of others. Such private sector groups provide an institutionalized process for engagement with government and can serve as a forum for sensitive dialogue on cyber security matters.

2. In some countries, groups have been established by several critical infrastructure sectors to bring sector representatives together to share information on security threats, vulnerabilities, and impacts. Often, these groups also provide real-time alerts and warning to members to facilitate efforts to mitigate, respond to, and recover from actual incidents impacting the critical infrastructures.

3. These groups should consider adopting practices that enable collaboration and information exchange among members (i.e., government and private sector) in a trusted forum. Some of these practices may include providing the following: anonymity for members; access to cross sector and government information; access to sensitive threat, vulnerability, and analytical products; and subject matter expertise on emergency response coordination, operational practices, and exercises. While considering these practices to

enable collaboration, it is important to incorporate means for the protection or proprietary and business-sensitive information.

II.B.3. Bring private sector groups and government together in trusted forums to address common cybersecurity challenges.

1. Several conditions are necessary to build trust and promote successful collaboration between government and the private sector. A written agreement that guides the collaboration and exchange between government and the private sector is recommended. Participants need a shared vision and purpose. Strong individual or organizational leadership sets priorities, allocates resources, and makes commitments necessary to sustain government-industry collaboration. Rules of engagement are also needed to guide individual and organizational behaviour within the collaborative relationship.

2. Participants must see tangible and measurable outcomes. Creating a value proposition for the collaboration for individuals and organizations and clearly articulating that value is key to the development and maintenance of government-industry collaborative relationships.

II.B.4. Encourage cooperation among groups from interdependent industries.

1. Incidents involving one kind of infrastructure can have cascading effects and result in incidents in other kinds of infrastructures. For example, power outages may disrupt telephone and Internet services. Moreover, although people may plan for emergencies in their own industry, they must also consider the impact that incidents may have on other sectors. Sharing information across infrastructures can help efforts to respond to incidents that cut across multiple sectors and are nationally significant.

II.B.5. Establish cooperative arrangements between government and the private sector for incident management.

1. Rapid identification, information exchange, and remediation can often diminish the damage caused by cyber incidents. At the national level, government-industry collaboration is needed to conduct analyses, issue warnings, and coordinate response efforts.

2. Governments and industry should collaboratively develop a framework for strategic, operational, and awareness coordination for improving incident management. This framework should contain a formal construct for sharing information that includes focal points for policy-related issues and operational information exchange. The framework

should also include policies and procedures for sharing and reporting incidents, protecting and disseminating sensitive (government and industry) proprietary information, and mechanisms for communicating and disseminating information. Private sector information often contains company proprietary information that if released to the public could result in lost market share, adverse publicity, or other negative consequences. Similarly, government information may be classified or sensitive and not for release to the public. Policy and technical measures to safeguard information while balancing the public's right to know should be put in place. Governments can continue to build trust by enhancing information sharing policies and government-industry relationships through continual evaluation of policies. Cyber exercises can also test government-industry communications and coordination related to cyber incident response and recovery efforts by exercising mechanisms deployed in times of real crisis.

C. Reference Material for Additional Information on this Topic

II.C.1. Structures for Government-Industry Collaboration

- United States Information Sharing and Analysis Centers (*ISACs) & Coordinating Councils*
- Financial Services ISAC www.fsisac.com/
- Electric Sector ISAC www.esisac.com/
- Information Technology ISAC www.it-isac.org
- Telecommunications ISAC www.ncs.gov/ncc/
- Network Reliability and Interoperability Council (NRIC): www.nric.org/
- National Security and Telecommunications Advisory Committee (NSTAC): www.ncs.gov/nstac/nstac.html
- IT Sector Specific Plan: www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- United States Sector Specific Plans: www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- Information Technology Association of America White Paper on Information Security: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- Industry-Government Cooperation on Standards: American National Standards Institute-Homeland Security Standards Panel:

www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3

- National Telecommunications and Information Administration: www.ntia.doc.gov/
- IT Sector Coordinating Council (SCC): www.it-scc.org
- U.S. National Infrastructure Protection Plan: www.dhs.gov/xprevprot/programs/editorial_0827.shtm

II.C.2. Cybersecurity information sharing

- National Information Assurance Council (NIAC) report on sector partnership model working group: itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- US-CERT alerts: www.us-cert.gov/cas/
- Network Reliability and Interoperability Council, www.nric.org
- National Institute of Standards and Technology, Computer Security and Research Center, csrc.nist.gov/
- Internet Engineering Task Force: www.ietf.org
- World Wide Web Consortium: www.w3c.org
- Institute of Electrical and Electronics Engineers: www.ieee.org
- Messaging Anti-Abuse Working Group: www.maawg.org

II.C.3. Awareness raising and outreach: Tools for business and home use

- Information for technical and non-technical users: www.us-cert.gov/
- StaySafeOnLine: www.staysafeonline.org/
- Federal Trade Commission: Onguard Online www.ftc.gov/infosecurity and www.OnGuardOnline.gov
- U.S. CERT posters and information sheets: www.uscert.gov/reading_room/distributable.html
- OECD’s Anti-Spam Toolkit: www.oecd-antispam.org
- London Action Plan Spam Enforcement Cooperation Network: www.londonactionplan.org

Part III: Deterring Cybercrime

Cybersecurity can be greatly improved through the establishment and modernization of criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime.

Background

Deterring cybercrime is an integral element of the management framework for organizing national cybersecurity efforts described in this report.

A. Overview of the Goal under this Part

III.A.1. Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with, among others, the provisions of the Convention on Cybercrime (2001).

1. Every country needs laws that address cybercrime per se, the procedures for electronic investigations, and assistance to other countries. These laws may or may not be in a single place in a country's code. For simplicity's sake, this document assumes that each country will have one primary cybercrime statute plus a collection of related procedural and mutual assistance legal texts. Of course, countries should use whatever structure they determine is best suited to their national circumstance.

B. Specific Steps to Achieving this Goal

III.B.1. Assess the current legal authorities for adequacy. A country should review its existing criminal code to determine if it is adequate to address current (and future) problems. Suggested steps:

1. It is recommended that a country use the provisions of the Convention on Cybercrime (2001) among others as a checklist against which to measure its laws. The convention includes requirements for substantive laws (that is, the minimum standards for what is criminalized, such as damaging or destroying computer data); procedural mechanisms (that is, necessary investigative methods, such as the ability to trace the source of email messages); and international legal assistance (that is, procuring evidence or extradition). The convention is available from the Council of Europe in various languages at www.coe.int/cybercrime/ .

2. It is also available from Interpol in various languages at www.interpol.int/public/TechnologyCrime/.

3. A country should consider whether its laws rely on outdated technological expectations. For example, a country may have a law that authorizes government officials to listen to telephone conversations while they are taking place. If this law refers in its text to attaching clips to telephone lines or to a telephone switching station, it may not - because of its own terms - stretch to cover mobile telephones. Similarly, a statute may discuss the tracing of voice transmissions only. Such a statute will likely need to be changed to cover transmissions of data.

4. A country's cybercrime law should be evaluated by all [concerned] ministries and legislative committees that might have an interest in it, even if they have nothing to do with criminal justice, so that no useful idea is missed. An information technology official might notice, for example, that the cybercrime law is inadequate to reach a new technology that is coming into increasing use but is not yet widely known to legal drafters in that country.

5. In addition, it is recommended that a country's existing criminal law should similarly be evaluated by some or all of the following: the local private sector, by any local affiliate of the international private sector, by local non-governmental organizations, by academics, by unaffiliated interested citizens, by willing foreign governments, and anyone else with a recognized interest.

III.B.2. Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime.

1. It is recommended that the text of a national cybercrime law be drafted to comply, among others, with the provisions of the Convention on Cybercrime (2001). Countries that are members of the Council of Europe should consider signing and ratifying the convention as quickly as possible. Countries that are not members of the Council of Europe are nevertheless immediately eligible to seek accession to the convention. The convention was not written to suit any particular legal system or culture; rather, it is flexible and usable by any legal system. Inquiries about accession by countries that are not members of the Council of Europe may be directed by email, telephone or letter to the COE. A preliminary inquiry may be made informally. A country's own treaty law experts or those at the Council of Europe can advise on how closely a country must comply with the convention before ratifying or acceding.

2. A country's cybercrime law draft should be evaluated by all ministries and legislative committees that might have an interest in it, even if they have nothing to do with criminal justice, so that no useful idea is missed. It sometimes happens that ministries of justice, interior, information technology, trade, etc, will claim that the draft cybercrime law has nothing to do with them or that the draft cybercrime law is exclusively theirs. Neither claim is true, but it is helpful to encourage ministries to work together to ensure that the law is practical and enforceable. [NB: this paragraph is repetition of II.B.1 3]

3. Countries with relevant legal systems should consult the Model Law on Computer and Computer Related Crime of the Commonwealth countries, available at www.thecommonwealth.org/Internal/38061/documents/.

4. Any cybercrime statute should address not merely classic cybercrimes such as computer crimes, such as computer intrusions, but also physical-world crime that depends on electronic evidence - fraud via email, bombings coordinated by email, kidnappings with electronic ransom notes, etc.

5. Data protection laws written for civil and commercial life should not be extended or interpreted to impede inappropriately the flow of criminal evidence between countries. [Suppose, for example, that the central bus station in Country A's capital is bombed, and the emails between the perpetrators are stored in Country B. It could be tragic if Country B refuses to transfer criminal evidence because, under its law, Country A has been deemed to have insufficient privacy protections in credit-card transactions.]

6. Countries that decide to hire consultants to do the drafting should consider their qualifications and supervise their work throughout the process. Persons who have not been trained specifically under the law of a country may not adequately integrate all the necessary provisions, especially procedural and mutual legal assistance sections. Moreover, persons who do not have prosecutorial experience are unlikely adequately to consider the practicalities of proving a case. Some consultants are qualified to assist in drafting electronic commerce laws but not criminal laws.

7. Other countries may be consulted for suggestions beyond what is contained in the convention. For example, countries may require Internet service providers to retain some of the data transiting their systems for some period, often six months; or they may require computer incidents of a certain significance to be reported to government authorities; or they may require proper identification before a person uses a cybercafé.

8. If time permits, a country [should/may] seek comments on the draft cybercrime law (or amendments) from other countries and multilateral organizations. Such comments can be obtained privately and, as noted above, it is helpful to obtain the viewpoints of several countries based on shared experience.

9. At the earliest possible stage (consistent with national procedures), a country should seek comments also from those concerned with a recognized interest in the subject matter: the local private sector, any local affiliate of the international private sector, local non-governmental organizations, academics, unaffiliated interested citizens, and others.

III.B.3. Establish or identify national cybercrime units.

1. It is important for every country, regardless of the level of development, to have at least a basic cybercrime investigation capacity. For example, the use of cell phones has expanded rapidly in less-developed countries, and cell phones can be used to commit fraud, to transfer money, to conspire, to transmit viruses to electronic networks, to set off explosives, etc..

2. Each country should select or train a cybercrime investigative unit that will have competence for national cybercrime investigations. Sometimes it will be obvious which law enforcement service or services this should be. Sometimes competing law enforcement agencies will disagree over the selection and senior authorities will have to make a difficult decision. Even if it appears that the country does not currently have anyone with the necessary skills, it is normally true that there is a law enforcement officer somewhere who is interested in electronic technology and is ambitious to learn more and go further with the field.

3. Cybercrime investigative units, even if they consist of only a limited number of investigators, require support. They require relatively up-to-date equipment, reasonably reliable network connections, and continuing training. Such support may come from the government of the country; from international organizations or other countries; and from private sector donations.

4. Where possible, it is advisable for units to have at least basic computer forensic capacity. Such capacity will require software tools and additional training. (If forensic capacity is considered impossible to achieve, countries should accept beforehand that crucial evidence, even in crucial cases, may be lost.) In some circumstances, forensic assistance for specific cases may be available from other countries. In addition, training in

cyberforensics may be available both from other countries and from relevant organizations. For example, the Computer Emergency Response Team Coordination Center of Carnegie-Mellon University in the United States (www.cert.org) offers some cyber forensics training for free or at very low prices online or by CD-ROM.

5. Once a cybercrime unit is set up, it should publicize its existence and capabilities to other law enforcement services and to prosecutors in the country. It is not useful to have a cybercrime unit in the capital if a regional law enforcement force is investigating a terrible crime that involves electronic evidence but does not know that there is a cybercrime unit that could search the target's computer or offer other help. Unfortunately, it is very common worldwide that a country's law enforcement establishment is unaware that the country possesses a cybercrime unit.

6. Cybercrime units or potential units should foster relationships with international partners to the greatest possible extent. At initial stages, advice about setting up the unit is available from other countries and from international law enforcement organizations. At later stages, training of many types and even equipment and software are available from other countries, from international law enforcement organizations, from relevant multilateral organizations, and from the private sector. Such contacts will also be valuable for another reason: in a world that will become more and more networked, it is critical to be able to request assistance from foreign law enforcement.

7. Cybercrime units should also take up contact with every relevant and interested sector within their countries, for example, domestic non-governmental organizations, computer security incident response teams, private sector entities, and academia, to ensure they know of the unit's existence and capabilities, can collaborate with it, and understand how to report possible cybercrime.

III.B.4. Develop cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector.

1. Cooperative relationships among government authorities, other elements of the national cybersecurity infrastructure and the private sector are important for several reasons:

a) to exchange information between the groups (for example, to advise that a new law is contemplated or a new technology is in development)

b) to exchange opinions (for example, “If we draft a new law along those lines, would you see any privacy problems with it?” or “Is there any way you can alter that technology so that email traces can still be done if there are legitimate public safety reasons?”)

c) to exchange training, though most often training will be offered by the private sector to the government

d) to exchange warnings about threats or vulnerabilities

e) so that people from different sectors will get to know each other well enough to trust one another in emergencies.

2. A good first step in forming such relationships is for one or more people to create a list of people and organizations in the country with specific cyber skills and responsibilities in all of the relevant sectors. Contact information for those people can then be noted on the list. It is probably best to keep such a list informal to avoid struggles over who is and who is not on the list.

3. In every country, there are likely to be numerous sectors that have a helpful focus on cybersecurity - legislators, ministries, non-governmental organizations, computer security incident response teams, academia, the private sector, and individuals. Some of these may be wholly domestic and some may be affiliated with larger foreign entities.

<u>III.B.5</u>. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.

1. To address cybercrime issues properly it is important that prosecutors and judges have some understanding of areas such as computers, software, and networks as well as of the increasing importance of electronic evidence. Similarly, legislators should have some understanding of those topics and of whether a country’s laws are adequate to address cybercrime. One solution to this problem is training.

2. If basic technical training is required, it can come from a variety of sources, depending on the country’s resources:

a) any domestic service or ministry with technical competence, such as a law enforcement service or an information technology ministry;

b) foreign governments;

c) relevant multinational organizations;

d) the local private sector;

e) the international private sector, especially (but not exclusively) if it does business locally;

f) relevant academia;

g) domestic or foreign computer security incident response teams; and

h) domestic and foreign relevant non-governmental organizations.

3. It may also be helpful to train senior policy-makers, government officials, etc, about the threats to electronic networks (for example, how the national banking system could be attacked) and about the threats posed by electronic networks (for example, the use of the Internet to locate vulnerable children for sexual trafficking). Training regarding these aspects of electronic networks should be available from the sources above.

4. Training may be desired for prosecutors and judges regarding prosecution of cybercrime or other crime involving electronic evidence, or of the use of electronic evidence, or of methods of obtaining international cooperation. Such training may be available from:

a) any domestic service or ministry with the correct competence, such as a prosecutor's office or a justice ministry;

b) foreign governments;

c) relevant multinational organizations;

d) relevant academia;

e) relevant domestic and foreign non-governmental organizations, and

f) relevant individuals.

5. A country may wish to have training in legislative drafting. Such training may be available from the groups listed in the paragraph above. The local private sector and the international private sector, especially (but not exclusively) if it does business locally, may be possible sources of expertise. However, it is more likely that the private sector entities will be able to assist with electronic commerce laws than with cybercrime, criminal procedure, and international mutual legal assistance laws.

6. For all of these types of training, the sources may offer to give the training themselves in the requesting country or they may offer training modules (electronic or printed) that instructors from that country can use in doing the training themselves. In some cases, as

with the CERT-CC training described at section III.B.3.4, such training can be provided without charge or with minimal charge.

7. In some countries, the key to national awareness of cybercrime issues has been the support of senior officials, or sometimes even one powerful senior official, particularly those who control budgets. If it is well-known that a minister is very interested in cybersecurity, his or her ministry - and perhaps the rest of the government - may offer better support to working-level people who are trying to accomplish something in the field.

III.B.6. Participate in the 24/7 Cybercrime Point of Contact Network.

1. In 1997, a network of emergency cybercrime contacts was established to improve international assistance in urgent investigations that involve electronic evidence. Many cybercrime investigators felt that it was too difficult to learn where to obtain quick assistance from other countries. In addition, many investigators felt that decades-old mutual legal assistance treaties were not helpful for fast-moving cases involving, for example, midnight computer intrusions into a country's financial systems. This network has grown to include almost 50 countries as of early 2007. The network is open to any country with the necessary capacity to assist as described below.

2. To join the network, countries must offer a contact point reachable twenty-four hours a day, seven days a week – thus the informal name, "the 24/7 network." The contact point can be a person who is reached directly or via an office. S/he must understand three things: 1) technology, so that requests can be transmitted without the delay of lengthy technological explanation; 2) his/her own domestic law; and 3) what domestic law allows him/her to do to assist other countries. If the contact point does not personally have these three types of knowledge, s/he must be able to reach any necessary person in his/her government immediately, if necessary (not merely the next business day).

3. Communications must go, at least initially, from the 24/7 contact point in Country A to the 24/7 contact point in Country B to ensure consistency and security. This means that contact points should not give out the contact information to other offices in their own countries. Rather, contact points should make the first international contact on behalf of a requesting office (for example, a provincial law enforcement force) in their countries. After initial cooperation between two countries has been established, a contact point may, if desired, withdraw from the investigation and let the provincial law enforcement in Country A communicate directly with Country B.

4. By joining the network, countries do not guarantee that they will always assist each other, nor does the contact network replace normal mutual legal assistance between countries. Rather, the contact network guarantees only that a requesting country will receive intelligent, capable attention immediately, even in the middle of the night. After any initial assistance, countries may (or may not) require that slower mutual assistance channels be used.

5. Twenty-four-hour-a-day availability does not mean that an office is staffed day and night with a certain number of computer workstations and cyber investigators waiting to answer telephone calls or emails. Most countries do not operate such an office. More commonly, one law enforcement officer (possibly different officers on a rotating basis) in a country will be reachable by telephone - perhaps sleeping with a cell phone nearby.

6. To join, countries should contact the chair of the High-Tech Crime Subgroup of the G8 (membership is not restricted to G8 members; rather, almost 50 countries already belong) at christopher.painter@usdoj.gov or +1 (202) 514-1026 in Washington, DC, USA. A short, simple form must be completed. The process does not require formal international agreements such as memoranda of understanding or treaties. From time to time, the 24/7 network offers training and networking conferences for the contact points. Travel to these conferences has been subsidized as needed.

7. The unit that joins the network has the responsibility to let local or national law enforcement services or cybercrime units in its country know of its existence and of its availability to assist in making contacts outside the country.

C. Reference Material for Additional Information on this Topic

- Convention on Cybercrime (2001) (COE web site): conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
- G-8 High-Tech Crime Principles and 24X7 information assistance mechanism: www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- UNGA Resolutions 55/63, 56/121: www.un.org/Depts/dhl/resguide/gares1.htm
- US DOJ Computer Crime and Intellectual Property Section website: www.cybercrime.gov

- APEC TEL cybercrime-related documents: www.apec.org/apec/apec_groups/working_groups/telecommunications_and_information.html

Part IV: Creating National Incident Management Capabilities: Watch, Warning, Response and Recovery

It is important to maintain a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, whose national mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, industry, academia, and the international community.

Background

A key role for government in addressing cybersecurity at the national level pertains to preparing for, detecting, managing, and responding to cyber incidents that occur. Implementing an incident management mechanism requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, and international organizations is necessary to effectively align capabilities and expertise to manage incidents and raise awareness of potential incidents and steps toward remediation. Government has a key role in ensuring coordination among these entities.

A. Overview of the Goals under this Part

Establishing national incident management capabilities requires a series of closely related activities, including:

IV.A.1. Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to, and recover from cyber incidents.

IV.A.2. Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents.

IV.A.3. Participate in watch, warning, and incident response information sharing mechanisms.

IV.A.4. Develop, test, and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.

B. Specific Steps to Achieve these Goals

The development of a national cyberspace response capability is a long-term effort that begins with establishing a sustainable national incident management capability or national computer security incident response team (N-CSIRT).

<u>IV.B.1</u>. **Identify or establish a national CSIRT (N-CSIRT) capability.**

1. Effective response to a significant cyber incident may limit the damage to information systems, ensure an effective means of responding, and reduce the length and cost of recovery. In conjunction with public and private sectors, an N-CSIRT is needed as a focal point within government, especially in incidents of national significance, to coordinate defense against and response to cyber incidents. In these instances, N-CSIRTs must work together with appropriate authorities, but would not direct or control their activities.

2. An N-CSIRT is expected to provide services and support to prevent and respond to cyber security-related issues and serves as a single point of contact for cyber security incident reporting, coordination, and communications. The mission of an N-CSIRT should include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical information infrastructure. Specifically, an N-CSIRT should perform several functions at the national level including but not limited to:

- detecting and identifying anomalous activity;
- analyzing cyber threats and vulnerabilities and disseminating cyber threat warning information;
- analyzing and synthesizing incident and vulnerability information disseminated by others, including vendors and technology experts to provide an assessment for interested stakeholders;
- establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cyber security issues;
- providing early warning information, including information about mitigating vulnerabilities and potential problems;
- developing mitigation and response strategies and effecting a coordinated response to the incident;
- sharing data and information about the incident and corresponding responses;

- tracking and monitoring information to determine trends and long term remediation strategies; and
- publicizing general cyber security best practices and guidance for incident response and prevention.

IV.B.2. Establish mechanism(s) within government for coordination among civilian and government agencies.

1. A key role for an N-CSIRT is to disseminate information, including information about current vulnerabilities and threats, to interested stakeholders. One stakeholder community that must be engaged in response activities is government agencies.

2. Effective coordination with these entities can take a number of forms, for example: maintaining a website for exchanging information; providing information via mailing lists, including newsletters, trends and analysis reports; producing publications that include alerts, tips, and information about various aspects of cyber security including new technologies, vulnerabilities, threats, and consequences.

IV.B.3. Establish collaborative relationships with industry to prepare for, detect, respond to, and recover from national cyber incidents.

1. The government and N-CSIRT must collaborate with industry. As industry in many countries owns much of the critical information infrastructure and information technology assets, government must work with industry to achieve its overarching goal of effective incident management.

2. Collaborative relationships with industry that are built on trust allow governments to gain insight into much of the critical infrastructure that is owned and operated by industry . Government-industry collaboration can help manage risk associated with cyber threats, vulnerabilities, and consequences and build situational awareness through information sharing, outreach and mutual engagements.

3. Encourage the development of industry operational entities and develop relationships with companies to foster information sharing practices between industry and government that enable sharing of operational information in real time.

4. A few ways to encourage this collaboration may include identifying benefits for both government and industry, developing and implementing programs that ensure the protection of sensitive proprietary data, establishing public-private working groups on cyber risk management and incident management, sharing incident response/management best

practices and training materials, and collaboratively defining government and industry roles and responsibilities for incident management, to put in place consistent, predictable protocols over time.

IV.B.4. Establish point(s) of contact within government agencies, industry and international partners to facilitate consultation, cooperation, and information exchange with the N-CSIRT.

1. Identifying appropriate points of contact and establishing collaborative working relationships for consultation, cooperation, and information exchange are fundamental to a coordinated and effective national and international incident response mechanism. These relationships can promote early warning of potential cyber incidents and exchange of information about trends, threats, and responses among incident response entities and other stakeholders.

2. Maintaining up-to-date points of contacts and communication channels with stakeholder communities can provide proactive, timely information exchange about trends and threats and expedite responses. It is important, to the extent possible, to establish contacts based on departmental functions rather than with individuals to ensure communication channels remain open even when individuals leave an organization. Relationships often begin by establishing trust with particular individuals, but should evolve into more formal, institutional arrangements.

IV.B.5. Participate in international cooperative and information sharing activities.

1. A cyber incident will likely not be confined to national borders, so effective response may rely on collaboration with international stakeholders. Building trusted communications with other governments and foreign incident response communities will enhance regular information sharing, so that when an incident occurs, a mechanism for cooperation on response would be available.

2. International cooperation and information sharing can be orchestrated in a number of ways. In particular, the N-CSIRT can establish mechanisms to facilitate regular information sharing, such as sharing daily reports and other informational products. Countries may also choose to create constructs for more formal collaboration.

IV.B.6. Develop tools and procedures for the protection of the cyber resources of government entities.

1. Effective incident management also requires the development and implementation of policies, procedures, methodologies, security controls and tools to protect government cyber assets, systems, networks, and functions. For a CSIRT, these can include Standard Operating Procedures (SOPs), guidelines for internal and external operations, security policies for coordinating with stakeholders, implementation of secure information networks for CSIRT operations, and secure communications. As a focal point for incident response, CSIRTs should coordinate with each other and help enable collaboration with other incident response entities. Governments should also provide continual incident response training to new and existing staff.

IV.B.7. Develop a capability through the N-CSIRT for coordination of governmental operations to respond to and recover from large-scale cyber attacks.

1. If there is an incident that rises to the level of national significance, there will be a need for a central point of contact to coordinate with other governmental entities as with other stakeholder communities, such as industry. It is important to develop plans and procedures to ensure that the N-CSIRT is prepared to address a possible incident.

IV.B.8. Promote responsible disclosure practices to protect operations and the integrity of the cyber infrastructure

1. Occasionally, governments, infrastructure, large enterprises, or security researchers may discover vulnerabilities in information technology products such as hardware and software. It is important that such vulnerabilities be shared with the vendor of the product in order to facilitate the development of an adequate patch or solution from the vendor prior to potential public disclosure. Such disclosure practices should be considered so that sensitive vulnerability information is not misused.

C. Reference Material for Additional Information on this Topic

IV.C.1. National Response Plan

- National Response Plan: www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- StaySafeOnline www.staysafeonline.info/
- Information Security and Privacy Advisory Board csrc.nist.gov/ispab/
- NIST: csrc.nist.gov/

IV.C.2 National CSIRT

- US CERT: www.us-cert.gov/
- NIATEC training courses: niatec.info

- Carnegie Mellon University/CERT Coordination Center: www.cert.org/csirts/
- European Network and Information Security Agency document: A Step-by-Step Approach on How to Set Up a CSIRT (www.enisa.europa.eu/pages/05_01.htm)
- India: www.cert-in.org.in
- Australia: www.auscert.org.au

IV.C.3 Cooperation and Information Sharing

- OECD's Anti-Spam toolkit: www.oecd-antispam.org
- IT-ISAC: www.it-isac.org/
- IT Sector Coordinating Council www.it-scc.org/
- ISO, Joint Technical Committee 1, Subcommittee 27 (ISO/JTC1/SC27) www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopelist=CATALOGUE
- Forum of International Response Security Teams: www.first.org

IV.C.4 Vulnerability Information/Tools and Techniques

- National Vulnerability Database (NVD) – nvd.nist.gov/nvd.cfm
- Open Vulnerability Assessment Language (OVAL) - oval.mitre.org/
- Build Security In - Collection of software assurance and security information to help software developers, architects, and security practitioners create secure systems - https://buildsecurityin.us-cert.gov/daisy/bsi/home.html
- Common Vulnerabilities and Exposures List (CVE) www.cve.mitre.org/about/

Part V: Promoting A National Culture of Cybersecurity

Considering that personal computers are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and use information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Government must take a leadership role in bringing about this Culture of Cybersecurity and in supporting the efforts of other participants.

Background

Promoting a national culture of cybersecurity is an integral element of the management framework for organizing national cybersecurity efforts described in this report.

A. Overview of the Goal under this Part

V.A.1. Promote a national Culture of Security consistent with UNGA Resolutions 57/239, *Creation of a global culture of cybersecurity*[6], and 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*[7].

1. The promotion of a national culture of security addresses not only the role of government in securing the operation and use of information infrastructures, including government operated systems, but also outreach to the private sector, civil society and individuals. Similarly, this element covers training of users of government and private systems, future improvements in security, and other significant issues including privacy, spam, and malware.

2. According to a recent OECD study, the key drivers for a culture of security at the national level are E-government applications and services, and protection of national critical information infrastructures. As a result, national administrations should implement E-government applications and services to both improve their internal operations and

[6] www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

provide better services to the private sector and to citizens. The security of information systems and networks should be addressed not solely from a technological perspective, but should include elements such as risk prevention, risk management, and user awareness. The OECD found that the beneficial impact of E-government activities is moving beyond public administrations towards the private sector and individuals. E-government initiatives appear to have acted as a multiplier fostering the diffusion of a culture of security.

3. Countries should adopt a multidisciplinary and multi-stakeholder approach to implement cyber security, and some are establishing a high-level governance structure for the implementation of national policies. Awareness raising and education initiatives are considered very important, along with the sharing of best practices, collaboration among participants, and the use of international standards.

4. International cooperation is extremely important in fostering a culture of security, along with the role of regional fora to facilitate interactions and exchanges.

B. Specific Steps to Achieve this Goal

V.B.1. Implement a cybersecurity plan for government-operated systems.

1. The initial step for government action to secure government-operated systems involves developing and implementing a security plan. Preparation of that plan should address risk management, as well as security design and implementation. Periodically, both the plan and its implementation should be reassessed to measure progress and to identify areas where the plan or implementation need improvement. The plan should also include provisions for incident management, including response, watch, warning, and recovery, and information sharing linkages. The security plan should also address action called for in V.B.**2** for training of users of these government systems and collaboration among government, industry and civil society on security training and initiatives. User awareness and responsibility are the key issues to be addressed by training.

[7] www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

V.B.2. Implement security awareness programs and initiatives for users of systems and networks.

1. An effective national cybersecurity awareness program should promote cyber security awareness among and within the general public and key communities, maintain relationships with governmental cyber security professionals to share information about cyber security initiatives, and develop collaboration to promote collaboration on cyber security issues. There are three functional components to consider when developing an awareness program: (1) stakeholder outreach and engagement, which builds and maintains trusted relationships among and between industry, government, and academia to raise cyber security awareness and effectively secure cyberspace; (2) coordination, which works to ensure collaboration on cybersecurity events and activities across the government; and (3) communications and messaging, which focuses on development of internal (within the government agency responsible for this program) and external communications (other government agencies, industry, educational institutions, home computer users, and general public).

V.B.3. Encourage the development of a culture of security in business enterprises.

1. Developing a Culture of Security in business enterprises can be achieved in a number of innovative ways. Many government initiatives have been directed at awareness-raising for small and medium-sized enterprises. Government dialogue with business associations or government-industry collaboration can help administrations design and implement education and training initiatives. Examples of such initiatives include: making information available (off line and online), e.g. booklets, manuals, handbooks, model policies and concepts; setting up web sites specifically targeted at SMEs and other stakeholders; provision of (online) training; provision of an online self-assessment tool; and offering financial assistance and tax support or other incentives for fostering the production of secure systems or taking proactive steps toward enhancing cyber security.

V.B.4. Support outreach to civil society with special attention to the needs of children and individual users.

1. Some governments have cooperated with the business sector to raise citizens' awareness of emerging threats and measures that should be taken to counter them. Some countries organize specific events, such as an information security day, week, or month with activities planned to promote information security to a broad audience, including the general public. Most initiatives aim to educate children and students either through school

mechanisms including teachers, professors and parents, or by direct distribution of guidance material. The support material used varies from web sites, games, and online tools, to postcards, textbooks, and diplomas for exams taken. Examples of such initiatives include delivering training courses to parents to inform them about security risks; providing support material for teachers; providing children with tools to play online while receiving educational messages related to information security; developing textbooks and games; creating an exam and a diploma; and a quiz about how to surf the web safely.

2. Government and the private sector can share the lessons they have learned in developing security plans and training users; learn from others' successes and innovations; and work to improve the security of domestic information infrastructures.

V.B.5. Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace.

1. Many information system vulnerabilities exist because of a lack of cyber security awareness on the part of users, system administrators, technology developers, procurement officials, auditors, chief information officers, and corporate boards. These vulnerabilities can present serious risk to the infrastructures even if they are not actually a part of the infrastructure itself. For example, the security awareness of system administrators is often a weak spot in an enterprise security plan. Promoting industry efforts to train personnel and adopt widely-accepted security certifications for personnel will help reduce these vulnerabilities. Government coordination of national outreach and awareness activities to enable a culture of security will also build trust with the private sector. Cyber security is a shared responsibility. Portals and websites can be a useful mechanism to promote a national awareness program, enabling government agencies, businesses, and individual consumers to obtain relevant information and carry out measures that will protect their portions of cyberspace.

V.B.6. Enhance Science and Technology (S&T) and Research and Development (R&D) activities.

1. To the extent that government supports science and technology and research and development activities, some of its efforts should be directed towards the security of information infrastructures. Through the identification of cyber R&D priorities, countries can help shape the development of products with security built-in as well as address

difficult technical challenges. To the extent that R&D is conducted in an academic institution, there may be opportunities to engage students in cybersecurity initiatives.

V.B.7. Review existing privacy regime and update it to the online environment.

1. This review should consider privacy mechanisms adopted by various countries, and by international organizations, such as the OECD. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, continue to represent international consensus on general guidance concerning the collection and management of personal information. By setting out core principles, the guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to transborder data flows, both on and off line.

V.B.8. Develop awareness of cyber risks and available solutions.

1. Addressing technical issues requires that governments, businesses, civil society and individual users work together to develop and implement measures that incorporate *technological* (i.e., standards), *process* (e.g., voluntary guidelines or mandatory regulations) and *personnel* (i.e., best practices) components.

2. An example of a threat is spam with associated threats such as malware (see Annex A).

3. Identity management is an example of a technological tool to address various cybersecurity needs (Annex B).

C. Reference Material for Additional Information on this Topic

V.C.1. Government systems and networks (V.B.1, V.B.2, V.B.7)

- UNGA RES 57/239 Annexes a and b. www.un.org/Depts/dhl/resguide/r57.htm
- OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" [2002] www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (Adopted Sept. 23, 1980): www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998) The Promotion of A Culture of Security for Information Systems and Networks in OECD Countries (DSTI/ICCP/REG(2005)1/Final.

- Multi State Information Sharing and Analysis Center: Main Page: www.msisac.org/
- The U.S. Federal Information Security Management Act of 2002 (FISMA) csrc.nist.gov/policies/FISMA-final.pdf
- U.S. HSPD-7, “Critical Infrastructure Identification, Prioritization and Protection” www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- U.S. Federal Acquisition Regulation (FAR), parts 1,2,7,11, and 39. www.acqnet.gov/FAR/
- The [U.S.] National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb/
- U.S. CERT site: www.us-cert.gov/
- U.S. NIST site: csrc.nist.gov/ and csrc.nist.gov/fasp/ and csrc.nist.gov/ispab/

V.C.2. Business and private sector organizations (V.B.3., V.B.5., V.B.7.)-

- National Cyber Security Partnership: www.cyberpartnership.org
- U.S. CERT: www.us-cert.gov/
- U.S. DHS/Industry “Cyber Storm” exercises: www.dhs.gov/xnews/releases/pr_1158340980371.shtm
- U.S. DHS R&D Plan: www.dhs.gov/xres/programs
- U.S. Federal Plan for R&D: www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- U.S. President’s Information Technology Advisory Committee report on Cyber Security research priorities: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

V.C.3. Individuals and civil society (V.B.4., V.B.6, V.B.7.)

- Stay Safe Online: www.staysafeonline.info/
- OnGuard Online: onguardonline.gov/index.html
- U.S. CERT: www.us-cert.gov/nav/nt01/
- OECD's Anti-Spam toolkit, www.oecd-antispam.org
- See also: The OECD questionnaire on implementation of a Culture of Security (which is found at DSTI/ICCP/REG(2004)4/Final) and the U.S. response to the questionnaire (which is found at webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase). The U.S. response to the questionnaire provides a comprehensive outline of U.S. efforts in this area.
- New Zealand: www.netsafe.org.nz
- Canada: www.psepc-sppcc.gc.ca

APPENDIX 1: LIST OF ACRONYMS

APEC-TEL	Asia-Pacific Economic Cooperation Telecommunications and Information Working Group
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (USA)
CCIPS	Computer Crime and Intellectual Property Section (of US Dept of Justice)
CERT-CC	Computer Emergency Response Team Coordination Center (of Carnegie-Mellon University, USA)
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
COE	Council of Europe
CPNI	Centre for the Protection of National Infrastructure (UK)
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures List (USA)
DHS	Department of Homeland Security (USA)
DOJ	Department of Justice (USA)
EU	European Union
FAR	Federal Acquisition Regulations (USA)
FCC	Federal Communications Commission (USA)
FIRST	Forum of Incident Response Security Teams
G8	Group of Eight (Nations)

ICT	Information & Communication Technologies
ISAC	Information Sharing and Analysis Centers (e.g., IT-ISAC (USA))
IT-ISAC	Information Technology Information Sharing and Analysis Center
ITAA	Information Technology Association of America
ITU	International Telecommunication Union
LAP	London Action Plan
MSCM	Mobile Service Commercial Message
NIAC	National Information Assurance Council (of ITAA)
NIATEC	National Information Assurance Training and Education Center (at University of Idaho, USA)
NIST	National Institute of Standards and Technology (USA)
NRIC	Network Reliability and Interoperability Council (FCC USA)
NSTAC	National Security and Telecommunications Advisory Committee (DHS USA)
NVD	National Vulnerability Database (USA)
OECD	Organisation for Economic Co-operation and Development
OVAL	Open Vulnerability Assessment Language
PSTN	Public Switched Telecommunication Network
R&D	Research and Development
S&T	Science and Technology
SME	Small and medium-sized enterprise
SMS	Short Message Service

SOP	Standard Operating Procedures
TCPA	Telephone Consumer Protection Act (USA)
UNGA	United Nations General Assembly
USG	US Government

APPENDIX 2: IMPLEMENTATION STRATEGY FOR CYBERSECURITY COOPERATION & MEASURES OF EFFECTIVENESS

The approach outlined above uses a program methodology designed to move countries forward in developing strong cyber security systems as a national priority. This methodology is divided into three distinct program stages that will move a country from an initial assessment of capabilities to program implementation and evaluation. This staged approach is set forth below:

Program Methodology for Cybersecurity Cooperation and Measures of Effectiveness

Stage 1 – Assess, evaluate and recommend a plan for a cooperative exchange program.

- **Assess**: The first step is for a country to conduct an assessment of the current status of its security program. This is accomplished by a team of experts using a standardized assessment instrument.
- **Evaluate**: Information gathered during this assessment provides an understanding of the strengths and weaknesses of the country's current cybersecurity program, and determines where efforts should be focused.
- **Recommend**: Understanding gained from the evaluation provides the basis for a plan to meet the country's requirements.

Stage 2 – Cooperative program development and implementation.

- **Cooperative Program Development**: Country experts meet either internally or with international counterparts to design, shape and adjust activities to meet the unique needs and circumstances of the particular country. The activities can encompass a range of cooperative exchange activities and identification of long-term material requirements.
- **Implement Program**: Domestic and perhaps international experts implement the program and offer concrete advice.

Stage 3 – Cooperative program evaluation to measure success and complete the program.

- **Cooperative Program Evaluated**: Periodically, the cybersecurity cooperative program is reevaluated for effectiveness internally or with country counterparts. Areas deemed deficient may become the subject for further cooperative exchanges and the foregoing process starts over. If a country is cooperating with others, such cooperation can phase out once the country's program is assessed as effective.

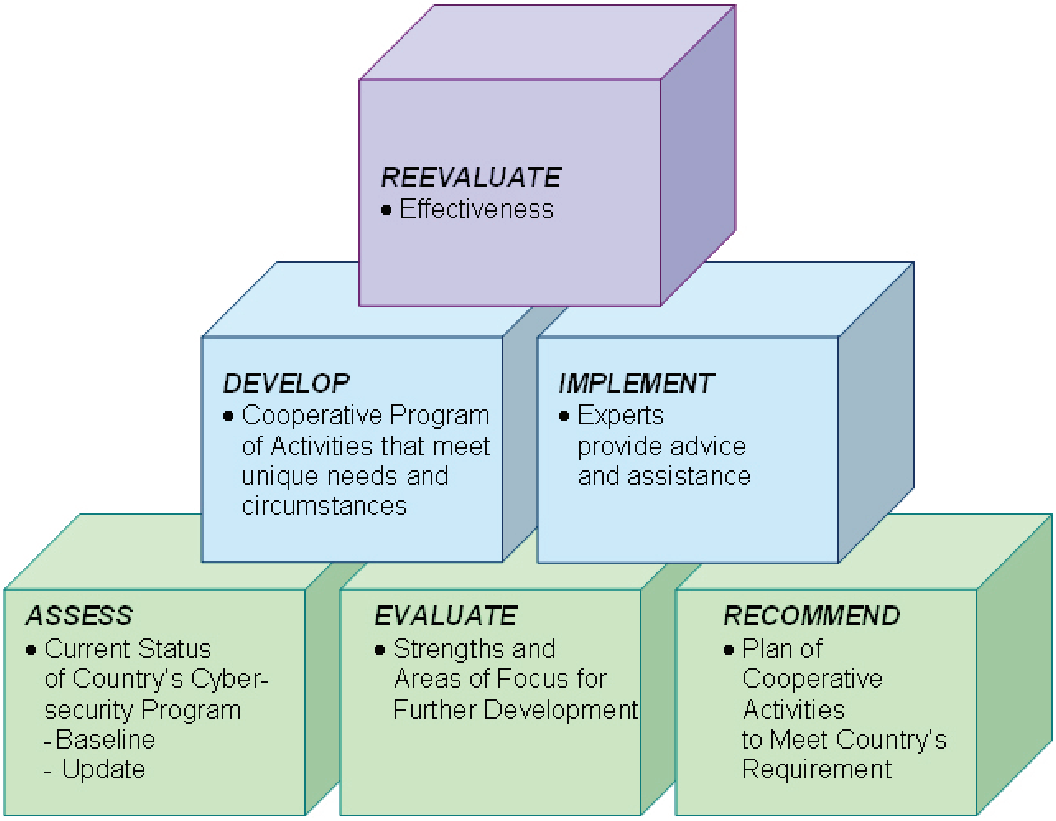
REEVALUATE
• Effectiveness
DEVELOP
• Cooperative Program of Activities that meet unique needs and circumstances
IMPLEMENT
• Experts provide advice and assistance
ASSESS
• Current Status of Country's Cyber-security Program
- Baseline
- Update
EVALUATE
• Strengths and Areas of Focus for Further Development
RECOMMEND
• Plan of Cooperative Activities to Meet Country's Requirement

Figure 1: Program Methodology for Building Capacity in Cybersecurity

Measures of Effectiveness

The following is one approach to measure performance over time in this area and to demonstrate progress to senior officials. The approach constructs a chain of logic that links basic inputs (country- or region-specific programs that consume time, money and staff resources) to the outcome finally desired (increased cybersecurity). The chain is illustrated below:

Measurement Category:	**Performance Element:**
Basic input:	**Country programs:** • Time • Money • Personnel
Basic work processes:	**Work, including possibly cooperative exchanges, in:** • National Strategy Development • Legal framework development • Incident Management • Government-Industry Collaboration • Culture of Cybersecurity

Measurement Category:	Performance Element:
Basic outputs:	**Number of :** • Meetings or cooperative exchanges • Contacts with senior policy and technical officials
Intermediate results:	**Country actions:** • New cyber crime laws and regulations • Enforcement actions • Establishment of CSIRT • Government-Industry awareness programs • Incident response inquiries • Participation in international organizations’ cybersecurity activities • Adherence to international conventions and guidelines
Eventual result:	Reduced cybersecurity risk resulting from a national legal and policy framework, incident response, and awareness efforts.
Final outcome:	Increased national cybersecurity and global security

ANNEX A: CASE STUDY ON SPAM & ASSOCIATED THREATS

Spam has gone from being a nuisance to consumers to a facilitator of a more serious cybersecurity problem. For example, spam can be a vehicle for deception, spreading malware such as viruses and spyware, and inducing consumers to provide confidential information that can later be used to commit identity theft (i.e., phishing). Senders can send their messages from anywhere in the world to anyone in the world at an extremely low cost to themselves, making spam an international problem that must be addressed through international cooperation. The following case study demonstrates how spam can be addressed within the framework discussed in this report.

National strategy and spam

With respect to a national strategy, countries should develop and maintain a combination of effective laws, law enforcement authorities and tools, technological tools and best practices, and consumer and business education to effectively deal with spam.

Legal and regulatory foundation and spam

With respect to a legal foundation and regulatory framework, authorities that have jurisdiction over spam must have the necessary authority to investigate and take action against violations of laws related to spam that are committed from their country or cause effects in their country. Authorities that have jurisdiction over spam should also have mechanisms to cooperate with foreign authorities. Requests for assistance from foreign authorities should be prioritized based on areas of common interest and in cases where significant harm occurs.

Government - industry collaborations and promotion of national awareness of spam issues.

All interested persons, including enforcement authorities, businesses, industry groups, and consumer groups should cooperate in pursuing violations of laws related to spam. Government enforcement agencies should partner with industry and consumer groups to educate users and promote information sharing. Government enforcement agencies should cooperate with the private sector to promote the development of technological tools to fight spam, including tools to facilitate the location and identification of spammers.

Phishing is often a preventable crime. Governments should work together with the private sector to improve means of protecting citizens from phishing, and educating consumers and businesses on safe authentication methods.

International (Multi-lateral) spam initiatives

Several multilateral fora exist within which initiatives to combat spam take place:

Stop Spam Alliance

The **StopSpamAlliance** is a joint international effort initiated by APEC, the EU's CNSA, ITU, the London Action Plan, OECD and the Seoul-Melbourne Anti-Spam group. Five associate partners have joined the StopSpamAlliance in 2007; the Asia-Pacific Telecommunity (APT), the Messaging Anti-Abuse Working Group (MAAWG), the Internet Society (ISOC), the Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE), and CAUCE North America.

The objective of the StopSpamAlliance is to help co-ordinate international action against spam and related threats more effectively by gathering information and resources improving information sharing among participating entities. www.stopspamalliance.org

London Action Plan

The FTC and U.K. Office of Fair Trading hosted an International Spam Enforcement Conference in London in 2004, which led to the creation of a London Action Plan on International Spam Enforcement Cooperation. As of January 2007, over 30 government agencies and over 20 private sector representatives, including several associations, have endorsed the plan. The LAP remains open to any spam enforcement agency and relevant private sector representatives from around the world.

The purpose of the LAP is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing, and dissemination of viruses. The LAP builds relationships between these entities based on a short document that sets forth a basic work plan for improving international enforcement and education cooperation against illegal spam. This document is non-binding, asking participants only to use best efforts to move the work plan forward. londonactionplan.org/

OECD Spam Toolkit and Council Recommendation on Spam Enforcement Cooperation

In April 2006, the OECD Spam Task Force released an Anti-Spam "Toolkit," which contains recommendations to help policy makers, regulators and industry players orient their policies relating to spam solutions and restore trust in the Internet and e-mail. The Toolkit contains eight elements, including anti-spam regulation, industry driven solutions and anti-spam technologies, education and awareness, and global cooperation/outreach. Recognizing that international cooperation is key to combating spam, the OECD governments also approved a "Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam," which urges countries to ensure that their laws enable enforcement authorities to share information with other countries and do so more quickly and effectively. www.oecd-antispam.org/sommaire.php3

APEC TEL Symposium on Spam

In April 2006, APEC TEL held a symposium on "Spam and Related Threats" that brought together thirty speakers and panelists to discuss the evolution of the spam problem and establish a common agenda of action for the TEL. Main topics addressed included: (1) the development and application of national anti-spam regulatory regimes, including enforcement and codes of practice; (2) the role of industry in combating spam, including government-industry collaboration; (3) technical responses to spam; (4) cross-border cooperation and enforcement, including the Council of Europe's Convention on Cybercrime and the OECD Council Recommendation on Enforcement Cooperation as primary tools for enhancing cooperation; and (5) the need for targeted consumer education and awareness raising. Concrete steps the TEL agreed to take going forward included: (1) encouraging information sharing on regulation and policy, drawing on resources such as the OECD Spam Toolkit; (2) developing a contact list for APEC spam authorities to augment similar resources developed by the OECD and the ITU; (3) encouraging economies to join voluntary cooperation forums such as the London Action Plan or the Seoul-Melbourne Agreement; (4) cooperating with the OECD on information sharing and guidance-related initiatives; and (5) supporting capacity building for developing economies to better deal with spam.

One approach: U.S. Anti-Spam Legislation

The following is a summary of the spam laws in the United States.

The United States has enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"), 15 U.S.C. § 7709, which establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them.

The main provisions of the CAN-SPAM Act include the following:

- **It bans false or misleading header information.** Your email's "From," "To," and routing information – including the originating domain name and email address – must be accurate and identify the person who initiated the email.

- **It prohibits deceptive subject lines.** The subject line cannot mislead the recipient about the contents or subject matter of the message.
- **It requires that your email give recipients an opt-out method.** You must provide a return email address or another Internet-based response mechanism that allows a recipient to ask you not to send future email messages to that email address, and you must honor the requests. You may create a "menu" of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end any commercial messages from the sender. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial email. When you receive an opt-out request, the law gives you 10 business days to stop sending email to the requestor's email address. You cannot help another entity send email to that address, or have another entity send email on your behalf to that address. Finally, it's illegal for you to sell or transfer the email addresses of people who choose not to receive your email, even in the form of a mailing list, unless you transfer the addresses so another entity can comply with the law.
- **It requires that commercial email be identified as an advertisement and include the sender's valid physical postal address.** Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email from you. It also must include your valid physical postal address.

The CAN-SPAM Act provides for significant penalties, including jail time, for spammers. The Federal Trade Commission (FTC) is authorized to enforce the CAN-SPAM Act. CAN-SPAM also gives the Department of Justice (DOJ) the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well. As of August 1, 2006, over 85 federal actions have been brought to combat spam.

The United States also has adopted rules to protect consumers from receiving unsolicited commercial messages (spam) on their wireless devices. With some exceptions, the rules prohibit the sending of commercial electronic mail messages, including e-mail and certain text messages, to wireless devices, such as cell phones, that offer commercial mobile radio service. The rules apply only to messages that meet the definition of "commercial" used in the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) — and to those messages in which the main purpose of the message is a commercial advertisement or promotion of a commercial product or service. Non-commercial messages, such as messages about candidates for public office or messages to update an existing customer about her account, are not subject to the rules.

To assist senders of commercial messages in identifying the addresses that belong to wireless subscribers, the rules require that wireless service providers supply the Federal Communications Commission (FCC) with the names of the relevant mail domain names. Mobile service commercial messages (MSCMs) may include any commercial message sent to an e-mail address provided by a mobile service provider for delivery to the subscriber's wireless device. Short message service (SMS) messages transmitted solely to phone numbers are not covered by these protections, but auto-dialed calls are already covered by the Telephone Consumer Protection Act (TCPA). MSCMs are prohibited unless the individual addressee has given the sender express prior authorization (known as an "opt-in" requirement). The rule prohibits sending any commercial messages to addresses that contain domain names that have been listed on the FCC's list for at least 30 days or at any time prior to 30 days if the sender otherwise knows that the message is addressed to a wireless device.

Under the FCC's rules, FCC can impose monetary forfeitures against spammers ranging from up to $11,000 per violation for non-licensees and to up to $130,000 per violation for common carrier licensees. In addition to monetary penalties, the FCC can issue a cease and desist order against a spammer that has violated any provision of the Communications Act or any FCC rule authorized by the Act. In addition, under the Communications Act, anyone who violates a provision of the Act is subject to criminal prosecution by the Department of Justice (in addition to a monetary penalty), and may face imprisonment for up to 1 year (up to 2 years for repeat offenders). To date, FCC has not initiated any enforcement proceedings related to such commercial messages.

Approaches To Limit Phishing

The Email system on the Internet was designed to robustly deliver mail in adverse circumstances during the 1970s when access to the Internet was limited to a very few researchers and members of the U.S. Defense Department. No effort was made to authenticate the identity of individuals sending email. While the email system has evolved since then, this basic omission has been present ever since. This means that anyone can send email to anyone with almost no form of authentication.

As mentioned above, phishing is merely an attempt to fool someone into going to the wrong web site with the intent of stealing that individual's private information. Phishing exists in large part because sometimes people expect to receive email from a popular site and they simply do not realize that the mail is not from the legitimate site. Because there is little authentication in email, it is difficult to determine whether a message is legitimate without careful inspection of the message. Such careful inspection requires substantial knowledge of the underlying mechanisms used on the web.

Phishing also exists because most people find it difficult to verify that the web sites they are going to are legitimate. Sometimes we do not look closely at the URL of a web page before entering sensitive information, and sometimes we just do not know what the correct URL should be.

The web servers used to "phish" sensitive information are often themselves the victims of malware, making it again extremely difficult to track phishers.

As was discussed above, a basic premise that spammers and phishers count on is the lack of knowledge regarding who the sender is. Today, participants within the Internet Engineering Task Force are working together to finalize a standard that would improve a recipient's ability to identify senders. As the effort concludes, vendors will begin to make implementations available to customers over the next year or two. There is also at least one free[8] implementation of the standard available. A source for assistance is the Anti-Phishing Working Group (APWG), an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing incidents (www.antiphishing.org/index.html).

Alone, this standard enables "white list validation", or the ability to verify that, for example, it really is your bank that is trying to reach you. With this standard, consumers can validate that it is indeed their friends and associates who are attempting to contact them. This standard in and of itself will limit some forms of phishing – but not all.

Malware, or malicious software that is made to run on a device without the knowledge or permission of the owner, is also a substantial problem. Governments can play a role in educating the public on the need to keep malware in check by making use of tools such as anti-virus software and applying the latest operating system patches and trusted computing techniques

[8] “Free” here refers to the ability to implement this feature royalty-free under conditions specified by the patent holder.

ANNEX B: IDENTITY MANAGEMENT

Background

The security of the traditional circuit-switched telecommunications network (PSTN) has been addressed over many decades of operation. However, the same cannot be said for distributed public IP networks with multiple-service providers, such as the Internet and Next Generation Networks (NGNs). IP traffic can be sent anonymously and this makes networks based on this technology vulnerable to misuse by its users. All electronic services (e-services such as e-business, e-commerce, e-health, e-government) are open to attack. This problem can be at least partly addressed by identifying users, especially when the users are people, so that they can be authenticated, granted appropriate access, and audited. Management of identities, therefore, underlies and enables most security mechanisms used in today's IP networks. This aspect of cybersecurity is something that service providers need to consider at the business level and governments need to consider on a national level as part of the national cybersecurity plan.

Introduction

In the context of IP networks, Identity Management (IdM) is the management of the life cycle (creation, maintenance, utilization, and revocation) of the attributes by which entities (such as service providers, end-user organizations, people, network devices, software applications and services) are known. A single entity may have multiple sets of identity attributes in order to access various services with differing security requirements, and these may exist in multiple locations.

IdM is a key component of cybersecurity because it provides the capability to establish and maintain trusted communications and networks among known users, providers, locations, and devices. It not only supports authentication of an entity's identity, it also permits authorization of a range of access privileges (rather than an all-or-nothing access) and easy change of access level when an entity's role changes. IdM also allows an organization to ensure its security policies are being properly applied by monitoring and auditing an entity's access activity. It allows an organization to know what level of access an entity is authorized to have, and who originated the authorization. IdM can provide access to entities both inside and outside an organization without diminishing security or exposing sensitive information. In short, a good IdM solution provides the trusted capabilities to automatically authenticate identities, authorize access, provision and manage entity identities and access privileges, and audit an entity's access.

IdM is a critical component in managing security and enabling the nomadic, on-demand access to networks and e-services that characterizes end-users' expectations in the information age. Along with other defensive mechanisms (e.g. firewalls, intrusion detection systems, virus protection), IdM plays an important role in protecting information and communication networks and services from cybercrimes such as fraud and identity theft. This, in turn, increases users' confidence that e-transactions will be secure and reliable, which facilitates the use of IP networks for e-services.

Importance to Global Network Infrastructure and Multi-national Coordination for Security

Security and assurance of the global network infrastructure will be dependent on IdM capabilities and practices implemented and used in various national, regional, and international networks. IdM best practices and implementation guidelines are important and necessary to provide identity assurance and protect the confidentiality, integrity and availability of the global network infrastructure.

IdM capabilities can be leveraged and used by national/regional networks and authorities to exchange information in support of national and trans-national protection measures (e.g., proper multi-factor authentication of individuals on air/sea carrier manifests, and the exchange of authenticated no-fly lists - to identify terrorists/criminals for border control).

IdM capabilities can be used to support national and international emergency telecommunications services by identifying users authorized for special services.

In addition, IdM capabilities can be used to support and coordinate responses to national and international cybersecurity incident by supporting authentication and response coordination as well as systems to trace-back and locate sources of the incidents.

Identity Management as an enabler of processes that control access to a network or service

One important function of IdM is to support the authentication of users of a network or service. When requesting access to a service or device, end-users (e.g. real persons, processes, sensors, devices and network elements, data objects, and software-based agents) make assertions as to their identity. Depending on the service provider's security requirements, these assertions may need to be validated to determine their authenticity before access is granted.

One authentication method is based on something the user knows (e.g. the two identifiers, *username* and *password*). This is the simplest but weakest authentication method because the username/password pair is easy to copy and misuse. Neither the authorized user nor the service provider has any way to know when it has been stolen.

A stronger authentication method is based on two or more factors: some combination of a device that a user *has* (and that can't be duplicated, such as a smart card), something the user *knows* (e.g. the identifier Personal Identification Number or PIN), and something the user *is* (e.g. biometric identifiers). This method is stronger because, for instance, a stolen device is useless without the PIN.

An even stronger authentication method is based upon a cryptographic public/private key pair process, such as public key infrastructure (PKI). This method involves a trusted third party (an "identity provider") in addition to the two parties to the transaction (e.g., a user and a service provider). In response to a request from the user or a query from the service provider, the identity provider validates the user's identity and associated public key (identifiers) and thus provides authentication of the user to the service provider. In a second step, the user and the service provider develop a cryptographic key for that session using their private keys. At this point the service provider can consider the other end-user to be bound to the session for the purposes of access control, security, and billing. The authenticated identity data is then applied to the service provider's access policies, and appropriate access privileges and permissions may be assigned.

IdM may support public/private key pair processes such as PKI and Pretty Good Privacy (PGP) for the exchange of credentials, depending on the security needs of the networks and services. Common cryptography algorithms used with PKI are Triple Data Encryption Algorithm (3DES), Advanced Encryption Standard (AES), and Elliptic-Curve Cryptography (ECC). Since some services depending on IdM involve very sensitive identity attributes critical to e-services (e.g. credit card transactions), a National Cybersecurity Plan should include an IdM risk assessment and, where appropriate, evolution to stronger per-bit and more computationally-efficient cryptography such as ECC.

Protection, Maintenance, Revocation and Control of Identity Data

Other important functions of IdM are to protect, maintain, and control trusted identity data.

Maintaining an end-user's privacy by protecting data that is specific and identifiable to the end-user is a matter of primary concern. While access to certain types of services may require only a limited set of identity attributes, service providers offering transactions that support e-services may collect and use a substantial number of identity attributes in providing these services.

Ensuring the continuing accuracy of the identity attributes is another primary concern. Consequently, identity attributes must be maintained as authoritative (accurate, timely, and consistent) if the transaction service is to remain viable. The emergence of competitive IdM environments has resulted in the proliferation of new identifiers (e.g. dynamic e-mail and instant message addresses), as well as the adaptation of old ones to new uses. These identifiers include E.164 telecommunication numbers, Object Identifiers (including X.509 digital certificates), ITU Carrier Codes, IP addresses, and Internet domain names. Continued maintenance of this data (i.e. identity proofing) is necessary to assure continued trust in its validity.

Where relevant, management of identity attributes should support the capability to rapidly check for identity attribute revocation (e.g. using a protocol such as the Online Certificate Status Protocol) using current open global secure protocols such as the Transaction Capabilities Application Part on PSTN signalling infrastructures, or, on IP infrastructures, E.115 or Internet Registration Information Service.

In many cases, end-users will require the capability to control the use of their own data and private information. In general, there are three conceptual models for control of IdM data: network-centric, service-centric, and user-centric. These models are determined based on the location of the data control and maintenance function as well as the degree to which the data includes identity attributes that end-users want to keep private. Typically, deployed identity management capabilities use a combination of these models. In addition, IdM data may be distributed or centrally maintained.

Discovery of Data

IdM also encompasses the concept of "discovery" of data that is needed for authentication and access. In a highly distributed, multi-provider environment (such as the Internet and Next Generation Networks), the identity data necessary to provide authentication and access for end-users can be located anywhere. End users, particularly people, may have multiple digital identities with different identity providers in different locations, which apply to the differing security needs of different services. When end-users are nomadic, service providers will need to locate and establish a trust relationship with an appropriate identity provider in order to complete the process of authenticating and granting access control to the end-user. On the other hand, in a scenario involving federations of service providers who are already known to each other, nomadic, on-demand service may only require a discovery process in order to locate the identity data for an end-user, a process which is similar to that which occurs today in mobile cell phone usage.

Electronic Government (e-Government)

The advantages to a service provider of implementing IdM include cost reduction, risk reduction, trust enhancement, and increased functionality. These reasons are equally valid when the service provider is a government. In an e-government scenario, the main objectives are also to cut costs and to provide more efficient and more effective services to the government's citizens and business partners.

Like other service providers, governments are confronted by the challenge of how to effectively and efficiently utilize identity in the networked world. In order to make e-government a reality, a government must perform risk analyses on the e-services it intends to offer and implement suitable protective measures. The value of many of the services may require a government to require strong authentication using mechanisms such as PKI.

Regulatory Considerations of IdM

Guarantees of privacy and data protection requirements are matters that national administrations and regional groups need to take into consideration in connection with IdM.

Reference Material for Additional Information on this Topic

Various forums are working on IdM issues. These include:

- ARK (California Digital Library Archival Resource Key): www.cdlib.org/inside/diglib/ark/
- ETSI/3GPP: www.3gpp.org/tb/sa/sa3/ToR.htm
- ETSI TISPAN: www.etsi.org/tispan/
- EU eID Roadmap: ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf
- European Citizen Card: europa.eu.int/idabc/servlets/Doc?id=19132
- FIDIS (EU Future of Identity in the Information Society): www.fidis.net
- FIRST (Forum of Incident Response and Security Teams): www.first.org
- Guide (EU Government User Identity for Europe): www.guide-project.org
- Handle: www.handle.net
- Higgins: www.eclipse.org/higgins/index.php

- IDSP (American National Standards Institute Identity Theft Prevention and Identity Management Standards Panel (IDSP): www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3
- IGF (ORACLE Identity Governance Framework): www.oracle.com/technology/tech/standards/idm/igf/index.html ; see Liberty Alliance
- ITRC (Identity Theft Resource Center): www.idtheftcenter.org
- Internet Engineering Task Force Security Area: sec.ietf.org
- ITU-T Identity Management Focus Group: www.itu.int/ITU-T/studygroups/com17/fgidm/
- ITU-T Next Generation Networks Question 13: www.itu.int/ITU-T/studygroups/com13/index.asp
- Liberty Alliance Project: www.projectliberty.org
- Light Weight Identity: lid.netmesh.org/wiki/Main_Page
- MODINIS-IDM Consortium: www.egov-goodpractice.org and www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium
- National Identity Card Schemes: e.g., www.identitycards.gov.uk and en.wikipedia.org/wiki/Identity_document
- OASIS (Organization for the Advancement of Structured Information Standards): www.oasis-open.org/home/index.php
- OECD (Organisation for Economic Co-operation and Development) Workshop on Digital Identity
- Management in Trondheim, Norway, May 8th-9th 2007: www.oecd.org/sti/security-privacy/idm
- OMA (Open Mobile Alliance): www.openmobilealliance.org
- The Open Group: www.opengroup.org
- OSIS (Open Source Identity System): osis.netmesh.org/wiki/Main_Page
- PAMPAS (EU Pioneering Advanced Mobile Privacy and Security (PAMPAS): www.pampas.eu.org
- PERMIS (EU Information Society Initiative in Standardization (ISIS) PrivilEge and Role Management Infrastructure Standards Validation): www.permis.org

- Prime (EU Privacy and Identity Management for Europe): https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/
- W3C (World Wide Web Consortium): www.w3.org
- Yadis: yadis.org/wiki/Main_Page