



INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION  
DEVELOPMENT BUREAU**  
ITU-D STUDY GROUPS

**Document -E**  
**[March 26, 2007]**  
**Original: English**

**[Interim Rapporteur's Group Meeting on ITU-D Question 22/1, April 30 – May 1, 2007]**

---

*FOR ACTION*

SOURCE: Rapporteur Question 22/1  
TITLE: Draft Report on Recommended Best Practices for achieving Cybersecurity

**RAPPORTEUR'S DRAFT**

**REPORT ON RECOMMENDED BEST  
PRACTICES  
FOR ACHIEVING CYBERSECURITY**

**REPORT ON RECOMMENDED BEST PRACTICES  
FOR ACHIEVING CYBERSECURITY**

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
<b><u>INTRODUCTION</u></b>	<b>1</b>
<b><u>Part I: Developing and Obtaining Agreement on a National Cybersecurity Strategy</u></b>	<b>1-1</b>
<i>A. Overview of the Goals under this Part</i>	
<i>B. Specific Steps to Achieve these Goals</i>	
<b><u>Part II: Developing a National Legal and Regulatory Foundation</u></b>	<b>2-1</b>
<i>A. Overview of the Goal under this Part</i>	
<i>B. Specific Steps to Achieve this Goal</i>	
<b><u>Part III: Creating a National Incident Management Organization: Watch, Warning, Response and Recovery</u></b>	<b>3-1</b>
<i>A. Overview of the Goals under this Part</i>	
<i>B. Specific Steps to Achieve these Goals</i>	
<b><u>Part IV: Establishing a National Industry-Government Partnership</u></b>	<b>4-1</b>
<i>A. Overview of the Goals under this Part</i>	
<i>B. Specific Steps to Achieve these Goals</i>	
<b><u>Part V: Promoting A National Culture of Cyber Security</u></b>	<b>5-1</b>
<i>A. Overview of the Goal under this Part</i>	
<i>B. Specific Steps to Achieve these Goals</i>	
<b>Appendix 1: Implementation Strategy for Cyber Security Cooperation and Measures of Effectiveness</b>	
<b>Appendix 2. List of Acronyms</b>	
<b>Annex A: CASE STUDIES: SPAM</b>	<b>A-1</b>

**REPORT ON RECOMMENDED BEST PRACTICES**  
**FOR ACHIEVING CYBERSECURITY**

## **INTRODUCTION**

For many years it has been the national policy of most nations to treat the national public switched telephone network (PSTN) as a critical infrastructure and protect it accordingly. Governments have had the lead responsibility for this effort. Commercial firms that in many countries own significant portions of this PSTN infrastructure have cooperated in this effort. However, the rapid rise of digitally-based information and communication technologies (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 inadequate.

The changes brought about by ICTs require a much greater emphasis on network security and cooperation by governments, businesses, other organizations and individual users who develop, own, provide, manage, service, and use information systems and networks (the participants). Greater use of ICTs has, in turn, created greater security risks.. However, while governments often continue to have the lead role in network security, it is critical to ensure that diverse participants are able to play a role in addressing security concerns. Policies and practices must be developed and implemented to incorporate security efforts. To establish a national program for cybersecurity/ Critical Information Infrastructure Protection (CIIP) requires an initial broad review of the adequacy of current national practices.

The terms “cybersecurity” and “critical information infrastructure protection” (CIIP) are equivalent in this document. The discussion in this report uses “cybersecurity”; however, CIIP should be understood to apply whenever cybersecurity is used.

This report outlines “recommended best practices for achieving cybersecurity” to assist governments in this effort. Key elements of this report include: Developing and Obtaining Agreement on a National Cybersecurity Strategy; Developing a National Legal and Regulatory Foundation; Creating a National Incident Management Organization: Watch, Warning, Response, and Recovery; Establishing a National Industry-Government Partnership; and Promoting a National Culture of Cybersecurity.

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

*Protection of critical information infrastructures and cyberspace is essential to national security and a nation's economic well-being. Critical information infrastructures and cyberspace are interconnected across industry sectors and national borders and their protection at the national, state/provincial, and local levels requires coordinated national action related to the prevention, preparation, response, and recovery from an incident on the part of government authorities; the private sector; and citizens/users; and at the international level requires cooperation and coordination with international partners.*

The formulation and implementation of a national cybersecurity strategy involves activities that appear in the other four parts of the Framework

### ***A. Overview of the Goals under this Part***

**I.A.1.** Create awareness at a national policy level of cybersecurity/ critical information and infrastructure protection issues and of the need for national action and international cooperation.

**I.A.2.** Develop a national strategy to protect critical information infrastructures and cyberspace from cyber and physical attacks.

**I.A.3.** Participate in international efforts to coordinate national activities related to the prevention of, preparation for, response to, and recovery from incidents.

### ***B. Specific Steps to Achieve these Goals***

The following 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.

**I.B.1.** Persuade key people 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 secure its critical information infrastructure, a first step is to establish cybersecurity as national policy, to be followed by the elaboration of a national strategy that implements that policy and relates the national efforts to international cybersecurity activities. In order to accomplish this, 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.

2. The national policy should be developed through consultation with representatives of all relevant participant groups and promulgated at the national level, preferably by the head of government, so as to ensure the cooperation of all participants.

I.B.2. Identify a lead person and institution for the overall national effort; determine where within the government a computer security incident response team (CSIRT) with national responsibility should be established; and identify lead institutions for each aspect of the national strategy.

1. The launch of a cybersecurity initiative requires 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 exhort the private sector to action. Ideally this person should have political stature and the ear of the head of government. This high-level authority is necessary to ensure the coordination among entities that currently may seldom interact. In time, this 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 level by a wide array of institutions. 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.

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 at the local level to the local participants and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts.

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.

**I.B.7.** Assess and periodically reassess the current state of cybersecurity 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 assessment tool, countries can work toward a “model” baseline for their national infrastructures. Appendix A provides an example of possible measurement indices for such a self-assessment.

**I.B.8.** Identify training requirements and how to accomplish 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)
- OECD Guidelines and Culture of Security:  
[www.oecd.org/sti/cultureofsecurity](http://www.oecd.org/sti/cultureofsecurity)
  - UNGA Resolutions 55/63, 56/121, 57/239, 58/199:  
<http://www.un.org/Depts/dhl/resguide/gares1.htm>
  - EU Commissioner Erkki Liikanen on "Information Society in an Enlarged Europe," Budapest, 2/26/04,  
[http://ec.europa.eu/archives/commission\\_1999\\_2004/liikanen/media/speeches/index\\_en.htm](http://ec.europa.eu/archives/commission_1999_2004/liikanen/media/speeches/index_en.htm)

- EU Commissioner Viviane Reding on "i2010: How to Make Europe's Information Society Competitive," Brussels, 2/22/05, <http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/05/107&type=HTML&aged=0&language=EN&guiLanguage=en>
- [http://europa.eu.int/comm/commissioners\\_barroso/reding/index\\_en.htm](http://europa.eu.int/comm/commissioners_barroso/reding/index_en.htm)
- European Network and Information Security Agency, <http://www.enisa.europa.eu/>

**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: <http://www.whitehouse.gov/pcipb/>
- National Implementation Strategies of 11 OECD members: [http://www.oecd.org/document/63/0,2340,en\\_21571361\\_36139259\\_36306559\\_1\\_1\\_1\\_1,00.html](http://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) <http://www.cpni.gov.uk/>
- UK Critical Information Infrastructure Protection Directory (government only) - to participate or obtain information email: [ciip-directory@niscc.gov.uk](mailto:ciip-directory@niscc.gov.uk)
- New Zealand: [www.digitalstrategy.govt.nz](http://www.digitalstrategy.govt.nz)
- Canada: [www.psepc-sppcc.gc.ca](http://www.psepc-sppcc.gc.ca)

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

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

- Forum of Incident Response Security Teams (FIRST): [www.first.org](http://www.first.org)

## **Part II: Developing a National Legal and Regulatory Foundation**

*The protection of critical information infrastructures and cyberspace requires updating criminal law and procedures and policy to address cybersecurity and respond to cybercrime.*

### ***A. Overview of the Goal under this Part***

**II.A.1.** Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime in accordance with the provisions of the Convention on Cybercrime (2001). 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 laws. Of course, countries will use whatever structure they prefer.

### ***B. Specific Steps to Achieving this Goal***

**II.B.1.** Assess the current legal authorities for adequacy. A country should review its 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) 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 English, French, German and Russian by searching for treaty number 185 at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=3/21/2007&CL=ENG>.

It is also available from Interpol in Arabic, Spanish, and Russian at <http://www.interpol.int/public/TechnologyCrime/Default.asp> and in Portuguese at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

2. 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 would need to be changed to cover transmissions of data.

3. A country's cybercrime law 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. 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.

4. A country's law should similarly be evaluated by 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.

II.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 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 competing ministries to work together to ensure that the law is practical and enforceable.

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

4. Any cybercrime statute should address not merely classic 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 should 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 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 anyone 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.

### II.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 exploded even in less-developed countries, and cell phones can be used to commit fraud, to transfer money, to conspire, to transmit viruses to electronic networks, and to set off explosives.

2. Each country should select or create a police service or services that will have competence for national cybercrime investigations. Sometimes it will be obvious which police service or services this should be. Sometimes competing police forces will struggle 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 police 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 one investigator, 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 organizations. For example, the Computer Emergency Response Team Coordination Center of Carnegie-Mellon University in the United States ([www.cert.org](http://www.cert.org)) offers some cyberforensics 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 police services and to prosecutors in the country. It is not useful to have a cybercrime unit in the capital if a regional police 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 world-wide that a country's law enforcement establishment is unaware that the country possesses a cybercrime unit.
6. Cybercrime units or potential units should take up contact 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 police organizations. At later stages, training of many types and even equipment and software are available from other countries, from international police organizations, from 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, including domestic non-governmental organizations, computer security incident response teams, private sector entities, and academia.

#### II.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 that will make email traces more difficult)
- 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 (in or out of the government) to create a list of who is who in the country 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.

#### II.B.5. Develop an understanding in the judiciary and legislative branches of government of cybercrime issues.

1. It is common that those who are familiar with network crime complain that the judges and legislators in their countries are unfamiliar with important areas such as computers and networks, whether the country’s laws are adequate to address such crime, the increasing importance of electronic evidence, etc. 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 police service or an information technology ministry;
- b) foreign governments;
- c) multinational organizations;
- d) the local private sector;
- e) the international private sector, especially (but not exclusively) if it does business locally;

- f) academia;
  - g) domestic or foreign computer security incident response teams; and
  - h) domestic and foreign non-governmental organizations.
3. It may also be helpful to train senior policy-makers, government officials, etc, about the threats that exist 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) multinational organizations;
  - d) academia;
  - e) domestic and foreign non-governmental organizations, and
  - f) 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 II.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.

II.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 police 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 police 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 cyberinvestigators waiting to answer telephone calls or emails. Most countries do not operate such an office. More commonly, one police 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](mailto: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 other interested police 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 website): <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
- G-8 High-Tech Crime Principles and 24X7 information assistance mechanism: [http://www.usdoj.gov/criminal/cybercrime/g82004/g8\\_background.html](http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html)
- UNGA Resolutions 55/63, 56/121: <http://www.un.org/Depts/dhl/resguide/gares1.htm>
- DOJ CCIPS website: <http://www.cybercrime.gov>
- APEC TEL Working Group E-Security Task Group Documents: <http://www.apectelwg.org/e-securityTG/index.htm>
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials: <http://www.apectelwg.org/e-securityTG/Resources.htm>

## **Part III: Creating a National Incident Management Organization: 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 mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities at the national, state and local levels; the private sector; academia; and the international community.*

A key role for government in addressing cyber security at the national level pertains to preparing for, detecting, managing, and responding to cyber incidents. Effective incident management 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 raise awareness of potential attacks and steps toward remediation.

### ***A. Overview of the Goals under this Part***

The following five goals represent elements of an incident management program.

III.A.1. Develop a national cyberspace security response system with effective organizations to prevent, predict, detect, respond to, and recover from cyber incidents.

III.A.2. Develop a national cyberspace threat and vulnerability reduction program in coordination with the intelligence and law enforcement communities to reduce the impact and severity of attacks.

III.A.3. Develop procedures and capabilities to manage risk to government computer systems and networks.

III.A.4. Participate in watch, warning, and incident response information sharing mechanisms.

### ***B. Specific Steps to Achieve these Goals***

The following paragraphs provide a more in-depth discussion of what is necessary to develop and sustain a national incident management capability.

III.B.1. Identify or establish a national computer security incident response team (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, a nationally

designated Computer Security Incident Response Team (CSIRT)<sup>1</sup> 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, CSIRTs must work together with law enforcement and intelligence authorities, but would not direct or control their activities.

2. A national 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 a national CSIRT should include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical information infrastructure. Specifically, a national 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.

**III.B.2.** Establish mechanism(s) within government for coordination among civilian, law enforcement, defense, and intelligence agencies.

1. A key role for a nationally designated 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 the government, including civilian, law enforcement, defense, and intelligence agencies.

2. Effective coordination with these entities can take a number of forms, for example: maintaining a website for exchanging information; and providing information via mailing lists, including newsletters, trends and analysis reports; producing

---

<sup>1</sup> Please See European Network and Information Security Agency document [A Step-by-Step Approach on How to Set Up a CSIRT](http://www.enisa.europa.eu/pages/05_01.htm) ([http://www.enisa.europa.eu/pages/05\\_01.htm](http://www.enisa.europa.eu/pages/05_01.htm)).

publications that include alerts, tips, and information about various aspects of cyber security including new technologies, vulnerabilities, threats, and consequences.

III.B.3. Establish partnerships with the private sector to prepare for, detect, respond to, and recover from national cyber incidents.

1. The government and national CSIRT must collaborate with the private sector. As the private sector 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 the private sector that are built on trust allow governments to gain insight into much of the critical infrastructure that is owned and operated by industry. Public-private partnerships foster collaboration that can reduce risk associated with cyber threats, vulnerabilities, and consequences and build global situational awareness through outreach and mutual engagements. Government and industry should also work together on Internet disruption, software assurance, control systems security, operations, information sharing, and combating cyber crime.
3. A few ways to encourage these partnerships may include explaining the 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 critical information infrastructure protection.

III.B.4. Establish point(s) of contact within government agencies, the defense and intelligence communities, the private sector and international partners to facilitate consultation, cooperation, and information exchange with the national incident response entity.

1. Identifying appropriate points of contact and establishing collaborative working relationships for consultation, cooperation, and information exchange is 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.

III.B.5. Undertake 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 national 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. Participation in multilateral organizations that seek to improve and enhance global cyber security—such as the Organization for Economic Cooperation and Development, Organization of American States, and Asia-Pacific Economic Cooperation—is another way to foster international collaboration.

III.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.

## ***C. Reference material for additional information on this topic***

### **III.C.1. National Response Plan**

- National Response Plan:  
[http://www.dhs.gov/dhspublic/interapp/editorial/editorial\\_0566.xml](http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml)
- StaySafeOnline <http://www.staysafeonline.info/>
- Information Security and Privacy Advisory Board <http://csrc.nist.gov/ispab/>
- NIST: <http://csrc.nist.gov/>

### **III.C.2 National CSIRT**

- US CERT: <http://www.us-cert.gov/>
- NIATEC training courses: <http://niatec.info>
- Carnegie Mellon University/CERT Coordination Center:  
<http://www.cert.org/csirts/>
- India: [www.cert-in.org.in](http://www.cert-in.org.in)
- Australia: [www.auscert.org.au](http://www.auscert.org.au)

### **III.C.3 Cooperation and Information Sharing**

- OECD's Anti-Spam toolkit: <http://www.oecd-antispam.org>
- IT-ISAC: <https://www.it-isac.org/>
- IT Sector Coordinating Council  
<http://www.ita.org/infosec/docs/ITSCCResponsestoGAO.pdf>
- International Standards Organization, Joint Technical Committee 1,  
Subcommittee 27 (ISO/JTC1/SC27)  
[http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopeli  
st=CATALOGUE](http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopeli<br/>st=CATALOGUE)

### **III.C.4 Vulnerability Information/Tools and Techniques**

- [National Vulnerability Database \(NVD\)](http://nvd.nist.gov/nvd.cfm) – <http://nvd.nist.gov/nvd.cfm>
- [Open Vulnerability Assessment Language \(OVAL\)](http://oval.mitre.org/) - <http://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 \(CVE\)](http://www.cve.mitre.org/about/)  
<http://www.cve.mitre.org/about/>

## **Part IV: Establishing National Industry-Government Partnerships**

*The protection of critical information infrastructure and cyberspace is a shared responsibility that requires a coordinated partnership between government at all levels and the private sector, which owns and operates much of this information infrastructure.*

Industry-government partnerships are fundamental to enhancing cyber security because no one entity can protect the entire information 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. Both the government and private sector have an enduring interest in assuring the availability of the infrastructure.

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 create a legal and regulatory environment that stimulates and facilitates voluntary private sector efforts to improve security, including establishing the policies and protocol needed to share timely analytical and useable information about threats. Finally, the government can sponsor and fund studies and research and development to improve security processes and tools.

Robust collaboration and information exchange between industry and government can enhance situational awareness, facilitate cooperation on strategic issues, mitigate cyber risk and support response and recovery activities. Through improved information sharing and analysis, the government and private sectors will be better equipped to identify threats and vulnerabilities, and to exchange mitigating and preventive tactics and resources.

Industry-government partnerships are founded upon the three pillars of trust, mutual benefit, and a clear understanding of roles and responsibilities. A fundamental element of successful industry-government partnerships is trust. Trust is necessary for establishing, developing and maintaining sharing relationships between the private sector and government. The success of industry-government partnerships is dependent on participants deriving value from the particular partnership. By providing an understanding of each party's roles and responsibilities in cybersecurity and participating in reciprocal information sharing, industry-government partnerships can mitigate and reduce risk and implement a more comprehensive approach to cyber security.

Listed below are general goals outlined in the Framework for National Action, which governments should consider as they develop relationships with industry and implement partnership arrangements.

### ***A. Overview of the Goals under this Part***

IV.A.1. Develop industry-government partnerships for the protection of cyberspace.

***B. Specific Steps to Achieve these Goals***

IV.B.1. Include industry perspectives in the 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, Government alone cannot sufficiently secure cyberspace. Awareness of industry perspectives and inclusion of the primary owners and operators of critical infrastructure to develop and implement cyber security policy and frameworks for risk management is invaluable for Government cybersecurity efforts. Governments can be informed by industry through participating in industry-government 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 as early as possible in the development, implementation, and maintenance of initiatives and policies.

IV.B.2. Encourage development of private sector groups from different 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 other issues. Such private sector infrastructure groups provide an institutionalized process for engagement with government and can serve as a forum for sensitive dialogue on cyber security matters.

2. In the United States, 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.

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

1. Several conditions are necessary to build trust and promote successful partnerships between government and the private sector. A written agreement that guides the partnership and exchange between government and the private sector is needed.

Participants need a shared vision and purpose. Strong individual or organizational leadership sets priorities, allocates resources, and makes commitments necessary to sustain industry-government partnerships. Rules of engagement are also needed to guide individual and organizational behavior within the partnership.

2. Participants must see tangible and measurable outcomes. Articulating the value of the partnership for individuals and organizations is key to the development and maintenance of industry-government partnerships.

#### IV.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.

#### IV.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, industry-government partnerships are needed to conduct analyses, issue warnings, and coordinate response efforts.

2. Governments and industry should collaboratively develop a plan for strategic, operational, and awareness coordination for improving incident management. Government and industry representatives should also consider a formal construct for sharing information, while considering information protection needs. 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 industry-government relationships through continual evaluation of policies. Cyber exercises can also test industry-government 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***

#### IV.C.1. Structures for Industry-Government Partnership

- United States Information Sharing and Analysis Centers (*ISACs*) & *Coordinating Councils*
  - Financial Services ISAC <http://www.fsisac.com/>
  - Electric Sector ISAC <http://www.esisac.com/>
  - Information Technology ISAC <http://www.it-isac.org>
  - Telecommunications ISAC <http://www.ncs.gov/ncc/>
  - Network Reliability and Interoperability Council (NRIC):  
<http://www.nric.org/>
  - National Security and Telecommunications Advisory Committee (NSTAC):  
<http://www.ncs.gov/nstac/nstac.html>
- ITAA White Paper on Information Security:  
<http://www.ita.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf>
- ITAA Comments on DHS National Infrastructure Protection Plan:  
[http://www.ita.org/infosec/docs/ITAA\\_NIPPComments1.doc](http://www.ita.org/infosec/docs/ITAA_NIPPComments1.doc)
- Industry-Government Cooperation on Standards: American National Standards Institute-Homeland Security Standards Panel:  
[http://www.ansi.org/standards\\_activities/standards\\_boards\\_panels/hssp/overview.aspx?menuid=3](http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3)
- National Telecommunications and Information Administration:  
<http://www.ntia.doc.gov/>

#### IV.C.2. Cybersecurity and CIIP information sharing

- National Information Assurance Council (NIAC) report on sector partnership model working group:  
[http://ita.org/eweb/upload/NIAC\\_SectorPartModelWorkingGrp\\_July05.pdf](http://ita.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf)
- US-CERT alerts: <http://www.us-cert.gov/cas/>
- Network Reliability and Interoperability Council, [www.nric.org](http://www.nric.org)
- National Institute of Standards and Technology, Computer Security and Research Center, <http://csrc.nist.gov/>

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

- Information for technical and non-technical users: <http://www.us-cert.gov/>
- StaySafeOnLine: <http://www.staysafeonline.org/>
- Federal Trade Commission: OnGuard Online [www.ftc.gov/infosecurity](http://www.ftc.gov/infosecurity) and [www.OnGuardOnline.gov](http://www.OnGuardOnline.gov)
- U.S. CERT posters and information sheets:  
[http://www.uscert.gov/reading\\_room/distributable.html](http://www.uscert.gov/reading_room/distributable.html)
- OECD's Anti-Spam Toolkit: <http://www.oecd-antispam.org>
- London Action Plan Spam Enforcement Cooperation Network:  
<http://www.londonactionplan.org>

## **Part V: Promoting A National Culture of Cyber Security**

*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 Cybesecurity and in supporting the efforts of other participants.*

### ***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*<sup>2</sup>, and 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*<sup>3</sup>.

- 1, This element of the Framework 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 , including businesses, 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. As the result of a 2003 survey on security, the OECD wrote a 2005 report<sup>4</sup> that highlighted three major findings from member country responses. They discovered that there are key drivers for a culture of security, there are commonalities in approaches to develop and implement national policies for a culture of security, and countries rely on international cooperation to foster a culture of security.
3. First, the OECD found that 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 are implementing E-government applications and services to both improve their internal operations and provide better services to the private sector and to citizens. These initiatives resulted from a common policy attribute: they do not address the security of information systems and networks solely from a technological perspective. They 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.

---

<sup>2</sup> [http://www.itu.int/osg/spu/cybersecurity/docs/UN\\_resolution\\_57\\_239.pdf](http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf)

<sup>3</sup> [http://www.itu.int/osg/spu/cybersecurity/docs/UN\\_resolution\\_58\\_199.pdf](http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf)

<sup>4</sup> “The Promotion of A Culture of Security for Information Systems and Networks in OECD Countries (DSTI/ICCP/REG(2005)1/Final.”

4. Second, countries are adopting 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 development of partnerships among participants, and the use of international standards.

5. Finally, international cooperation has been found to be 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 these Goals***

### **V.B.1. Implement security 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 identify areas where the plan or implementation thereof 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.

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

1. This element involves administrations undertaking initiatives to foster the overall security of government information systems. Examples of successful government information systems include e-government programs undertaken by central and local public authorities. In Austria, the “citizen card” was developed which has rapidly fostered a strong culture of security among federal and regional public sector officials. The card provides Austrian citizens and legal persons with an electronic signature and other technical means to securely interact with the public administration. In France, the EBIOS risk management approach has played a significant role in fostering risk assessment skills and approaches within government ministries and administrative offices. In Finland, the use of smart cards and encryption for e-mail between different ministries and agencies has strengthened the culture of security. The success of these initiatives is due to the dissemination of information about the new programs through seminars and/or conferences. For example, in Japan, the National Incident Response Team organized seminars tailored

for public officials in charge of coordinating emergency responses. Korea's information technology official training center was involved in similar activities.

V.B.3. Develop Culture of Security outreach partnerships with business.

1. Developing a Culture of Security partnership with business can be achieved in a number of innovative ways. Many government initiatives have been directed at awareness-raising for small and medium-sized enterprises (SMEs). Government dialogue with business associations or public-private partnerships 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; provision of (online) training; provision of an online self-assessment tool; developing software tools to integrate electronic signature into SMEs' services and applications; and offering financial assistance and tax support for fostering the production of secure systems.

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 information security day or week, with actions planned to promote information security in the general public. Most initiatives aim to educate children and students either through 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 of young children 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. Countries can examine how U.S. federal and state government actors have created portals and websites designed collectively to constitute a national awareness program, enabling government agencies, businesses, and individual consumers to 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 specific technical issues to enhance a coordinated response to spam and malware.

1. Addressing technical issues (such as combating spam and malware) 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.

***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.  
<http://www.un.org/Depts/dhl/resguide/gares1.htm>
- OECD “Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security” [2002]  
[http://www.oecd.org/document/42/0,2340,en\\_2649\\_34255\\_15582250\\_1\\_1\\_1\\_1,0\\_0.html](http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,0_0.html)
- OECD “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (Adopted Sept. 23, 1980):  
[http://www.oecd.org/document/20/0,2340,en\\_2649\\_34255\\_15589524\\_1\\_1\\_1\\_1,0\\_0.html](http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,0_0.html)
- OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998)
- Multi State Information Sharing and Analysis Center: Main Page:  
<http://www.msisac.org/>
- The U.S. Federal Information Security Management Act of 2002 (FISMA)  
<http://csrc.nist.gov/policies/FISMA-final.pdf>
- HSPD-7, “Critical Infrastructure Identification, Prioritization and Protection”  
<http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>
- Federal Acquisition Regulation (FAR), parts 1,2,7,11, and 39.  
<http://www.acqnet.gov/FAR/>
- The National Strategy to Secure Cyberspace: <http://www.whitehouse.gov/pcipb/>
- US CERT site: <http://www.us-cert.gov/>
- NIST site: <http://csrc.nist.gov/> and <http://csrc.nist.gov/fasp/> and <http://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](http://www.cyberpartnership.org)
- US CERT: <http://www.us-cert.gov/>
- DHS/Industry “Cyber Storm” exercises:  
[http://www.dhs.gov/xnews/releases/pr\\_1158340980371.shtm](http://www.dhs.gov/xnews/releases/pr_1158340980371.shtm)
- DHS R&D Plan: <http://www.dhs.gov/xres/programs/>
- U.S. Federal Plan for R&D:  
[http://www.nitrd.gov/pubs/csia/FederalPlan\\_CSIA\\_RnD.pdf](http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf)
- President’s Information Technology Advisory Committee report on Cyber Security research priorities:  
[http://www.nitrd.gov/pitac/reports/20050301\\_cybersecurity/cybersecurity.pdf](http://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: <http://www.staysafeonline.info/>
- OnGuard Online: <http://onguardonline.gov/index.html>
- US CERT: <http://www.us-cert.gov/nav/nt01/>
- OECD's Anti-Spam toolkit, [www.oecd-antispam.org](http://www.oecd-antispam.org)

- See also: The USG response to the OECD questionnaire on implementation of a Culture of Security ([DSTI/ICCP/REG\(2004\)4/Final](#)). Provides a comprehensive outline of USG efforts in this area. Available together with responses from other OECD countries at the OECD security web site:  
<http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase>
- New Zealand: [www.netsafe.org.nz](http://www.netsafe.org.nz)
- Canada: [www.psepc-sppcc.gc.ca](http://www.psepc-sppcc.gc.ca)

## Appendix 1

### Implementation Strategy for Cyber Security Cooperation and 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:

#### **Implementation Strategy for Cyber Security 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 cyber security 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.

#### **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 cyber security). The chain is illustrated in the table below:

<b><u>Measurement Category:</u></b>	<b><u>Performance Element:</u></b>
<b>Basic input:</b>	<b>Country programs:</b> <ul style="list-style-type: none"><li>▪ Time</li><li>▪ Money</li><li>▪ Personnel</li></ul>
<b>Basic work processes:</b>	<b>Work, including possibly cooperative exchanges, in:</b> <ul style="list-style-type: none"><li>▪ National Strategy development</li><li>▪ Legal and regulatory development</li><li>▪ Incident Management</li><li>▪ Industry-Government Partnerships</li><li>▪ Culture of Cyber Security</li></ul>
<b>Basic outputs:</b>	<b>Number of :</b> <ul style="list-style-type: none"><li>▪ Meetings or cooperative exchanges</li><li>▪ Contacts with senior policy and technical officials</li></ul>
<b>Intermediate results:</b>	<b>Country actions:</b> <ul style="list-style-type: none"><li>▪ New cyber crime laws and regulations</li><li>▪ Enforcement actions</li><li>▪ Establishment of CSIRT</li><li>▪ Industry-Government awareness programs</li><li>▪ Incident response inquiries</li><li>▪ Participation in international organizations' cybersecurity activities</li><li>▪ Adherence to international conventions and guidelines</li></ul>
<b>Eventual result:</b>	Reduced cyber security risk due to a national strategy, cyber crime laws, regulations, voluntary guidelines and better consumer self-awareness.
<b>Final outcome:</b>	Increased national cyber security and global security

## APPENDIX 2

### LIST OF ACRONYMS

APECTEL	Asia-Pacific Economic Cooperation <u>Telecommunications and Information Working Group</u>
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	<u>Common Vulnerabilities and Exposures List (USA)</u>
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
IGP	Industry-Government Partnership
ISAC	Information Sharing and Analysis Centers (various, such as IT-ISAC; USA)
IT-ISAC	Information Technology Information Sharing and Analysis Center)
ITAA	Information Technology Association of America
LAP	London Action Plan
MSCM	Mobile Service Commercial Message
NIAC	National Information Assurance Council (of ITAA)
NIATEC	<u>National Information Assurance Training and Education Center (at University of Idaho USA)</u>
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	<u>National Vulnerability Database (USA)</u>
OECD	<u>Organisation for Economic Co-operation and Development</u>
OVAL	<u>Open Vulnerability Assessment Language</u>
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

## **Annex A Case Studies**

### **Spam**

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 viruses and spyware, and inducing consumers to provide confidential information that can later be used to commit identity theft. Senders can send their messages from anywhere in the world to anyone in the world, 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.

**Public/ private partnerships 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.

#### *International (Multi-lateral) spam initiatives*

Several multi-lateral fora exist within which initiatives to combat spam take place:

##### 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.  
<http://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. <http://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 public-private partnerships; (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. Noncommercial 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.