

Management Framework
for Organizing National
Cybersecurity Efforts:

Self-Assessment Tool

Prepared by
Joseph P. Richardson

Origins

- World Telecommunication Development Conference (Doha, 2006):
 - ITU-D Study Group Question 22/1 (Geneva 2006): Securing information and communication networks: Best practices for developing a culture of cybersecurity.

ITU-D Q22/1

- Agreed to prepare a report on cybersecurity best practices for policy makers.
- Rapporteur's Group Meeting April 30 – May 1
 - agreed on draft text for cybersecurity best practices
Doc: RGQ22/1/088-E
- Study Group meets 17 September 2007 for Workshop on Frameworks for National Action

Self – Assessment Tool

- Based on Framework Best Practices Documents
- Focused at national *management* and *policy* level
- Intended to assist national governments:
 - Understand existing approach
 - Compare to Best Practices
 - Identify areas for attention
 - Prioritize national efforts

Considerations

- No nation starting at ZERO
- No “right” answer or approach
- Continual review and revision needed
- All “participants” must be involved
 - appropriate to their roles

Participants

- “Participants” responsible for cybersecurity:

Government, business, other organizations, and individual users who develop, own, provide, manage, service and use information systems and networks.

“UNGA Resolution 57/239 Creation of a global culture of cybersecurity”

The Self-Assessment Tool

- Examines management and policy level for each element of Framework
 - National Strategy
 - Deterring Cybercrime
 - National Incident Management Capabilities
 - Government-Private Sector Collaboration
 - Culture of Cybersecurity

The Self-Assessment Tool

- Looks at *organizational* issues for each element of Framework
 - The people
 - The institutions
 - The relationships
 - The policies
 - The procedures

Framework for Organizing a National Approach to Cybersecurity

Page 1 of 2

8/20/07

National Strategy

POLICY: Protection of cyberspace is essential to national security and a nation's economic well-being. Cyberspace interconnects industry sectors and crosses national borders. Coordinated national action by government, the private sector, and citizens/users is required for the prevention of, preparation for, response to, and recovery from incidents. Cooperation and coordination with international partners are also required.

1 – Overview of the Goals:

I.A.1. Create awareness at national policy level about cybersecurity and the need for national action and international cooperation.

I.A.2. Develop a national strategy to enhance cybersecurity to reduce the risks and effects of cyber disruptions.

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

2 – Specific Steps to Achieve Goals:

I.B.1. Persuade key people in government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy level discussions.

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 with national responsibility (N-CSIRT) should be established, and identify lead institutions for each element of the national strategy.

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

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

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

I.B.6. Identify international expert counterparts and foster international efforts to address cyber security issues, including information sharing and assistance efforts.

I.B.7. Establish an integrated risk management process for identifying and prioritizing protective efforts for critical information infrastructures and cyber security.

I.B.8. Assess current policy and reassess the current state of cyber security efforts and develop program priorities.

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

Deterring Cybercrime

POLICY: The protection of cyberspace requires updating criminal laws, procedures and policy to address and respond to cybercrime.

1 – Overview of Goals:

II.A.1. Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent 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. Each country may have one primary cybercrime statute plus a collection of related procedural and mutual assistance laws. Of course, countries may use whatever structure is best suited to their national circumstance.

2 – Specific Steps to Achieve Goals:

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.

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

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

II.B.4. Develop cooperative relationships with other elements of the national cyber security infrastructure and the private sector.

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

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

Incident Management

POLICY: The protection of cyberspace requires an organization to serve as the national focal point for securing cyberspace, whose mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between and among government entities at the national, state and local levels; the private sector; academia; and the international community.

1 – Overview of Goals:

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

III.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.

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

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

2 – Specific Steps to Achieve Goals:

III.B.1. Identify or establish a Computer Security Incident Response Team with national responsibility (N-CSIRT).

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

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

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 N-CSIRT.

III.B.5. Undertake international cooperative and information sharing activities.

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

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

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

Government-Private Sector Collaboration

POLICY: The protection of cyberspace is a shared responsibility that requires cooperation between government at all levels and the private sector, which owns and operates much of the underlying infrastructure.

1 – Overview of Goals:

IV.A.1. Develop government-industry collaborations that work to effectively manage cyber risk and to protect cyberspace.

IV.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.

2 – Specific Steps to Achieve Goals:

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

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

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

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

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

Culture of Cybersecurity

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

1 – Overview of Goals:

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

2 – Specific Steps to Achieve Goals:

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

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

V.B.3. Develop Culture of Cybersecurity outreach collaboration with business.

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

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.

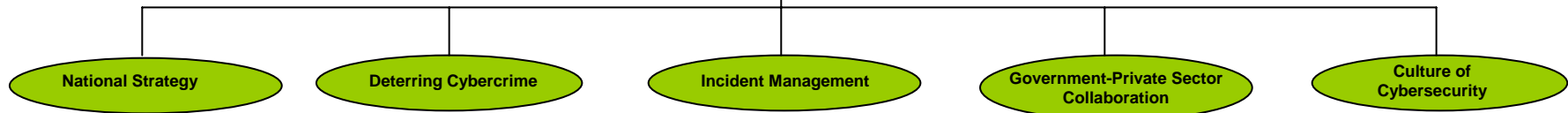
V.B.6. Enhance Science and Technology (S&T) and Research and Development (R&D) activities.

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

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

Framework for Organizing a National Approach to Cybersecurity

Page 2 of 2 8/20/07



3 – Reference Material & Training

Resources:

(available from the U.S. or internationally)

I.C.1. Awareness raising (I.B.1., I.B.4.)*

OECD Guidelines and Culture of Security:

<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

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&guiLang=ua=eu>

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.6., 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

UK Centre for Protection of National

Infrastructure (CPNI):

<http://www.cpni.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.)

In development:

NIST Special Publication 800-20 (2001),

800-30 (2002) and 800-50 (2003)

<http://csrc.nist.gov/publications/nistpubs/index.html>

ISO/IEC publications

3 – Reference Material and Training

Resources:

(available from the U.S. or internationally)

II.C.1. All Branches of Government

Convention on Cybercrime (2001) (COE website):

<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

G-8 High-Tech Crime Principles and 24/7

information assistance mechanism:

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-related documents:

http://www.apec.org/apec/apec_groups/working_groups/telecommunications_and_information.html

Culture of Cyber Security,

continued

V.C.3. Individuals and Civil Society (V.B.4.,

V.B.5., V.B.6., V.B.8.)

Stay Safe Online: <http://www.staysafeonline.info/>

OnGuard Online:

<http://onguardonline.gov/index.html>

U.S. CERT: <http://www.us-cert.gov/nav/nt01/>

OECD's Anti-Spam toolkit, www.oecd-antisipam.org

The OECD questionnaire on implementation of a

Culture of Security

(DST/ICCP/REG(2004)4/Final). Available

together with responses from other OECD

countries at

<http://webdomino1.oecd.org/COMNET/STI/ICCP/Secu.nsf?OpenDatabase>

New Zealand: www.netsafe.org.nz

Canada: www.psepc-sppcc.gc.ca

3 – Reference Material and Training Resources:

(available from the U.S. or internationally)

III.C.1. National Response Plan (III.B.4.)

National Response Plan:

http://www.dhs.gov/dhpublic/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 (III.B.1., III.B.2., III.B.7.)

US CERT: <http://www.us-cert.gov/>

NIATEC training courses: <http://niatec.info>

Carnegie Mellon University/CERT Coordination Center:

<http://www.cert.org/csirts/>

European Network and Information Security Agency

(ENISA): A Step-by-Step Approach on How to Set Up a

CSIRT (http://www.enisa.europa.eu/pages/05_01.htm

India: www.cert-in.org.in

Australia: www.auscert.org.au

III.C.3. Cooperation and Information Sharing (III.B.3.,

III.B.4., III.B.5., III.B.8.)

OECD's Anti-Spam toolkit: <http://www.oecd-antisipam.org>

IT-ISAC: <https://www.it-isac.org/>

IT Sector Coordinating Council

<http://www.itaa.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?CMMID=143&scopelist=CATALOGUE>

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

(III.B.6.)

National Vulnerability Database (NVD) –

<http://nvd.nist.gov/nvd.cfm>

Open Vulnerability Assessment Language (OVAL) –

<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/daisv/bsi/home.html>

Common Vulnerabilities and Exposures List (CVE)

<http://www.cve.mitre.org/about/>

* Parenthetical references in each column, e.g., (I.B.1.,

I.B.4.), identify associated Specific Steps in Part B., on

page 1

3 – Reference Material and Training Resources:

(available from the U.S. or internationally)

IV.C.1. Structures for Government-Private Sector

Collaboration (IV.B.1., IV.B.2., IV.B.3., IV.B.4.,

IV.B.5.)

United States Information Sharing and Analysis Centers

(ISACs) & Coordinating Councils:

Financial Services ISAC <http://www.fsisisac.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://nric.org/>

National Security Telecommunications Advisory Committee

(NSTAC) <http://www.ncs.gov/nstac/nstac.html>

United States Sector Specific Plans:

http://www.dhs.gov/xprepr/programs/ge_1179866197607.stm

ITAA White Paper on Information Security:

<http://www.itaa.org/eweb/upload/ITAA%20Infosec%20Wbite%20Paper.pdf>

Government-Industry 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

National Telecommunications and Information

Administration: <http://www.ntia.doc.gov/>

InfraGard: www.infragard.net

IV.C.2. Cybersecurity Information Sharing (IV.B.1.,

IV.B.2., IV.B.3., IV.B.4., IV.B.5.)

National Information Assurance Council (NIAC) report on

sector partnership model working group:

http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf

US-CERT alerts: <http://www.us-cert.gov/cas/>

National Institute of Standards and Technology, Computer

Security and Research Center, <http://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

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 and www.OnGuardOnline.gov

U.S. CERT posters and information sheets:

http://www.uscert.gov/reading_room/distributable.html

OECD's Anti-Spam Toolkit: <http://www.oecd-antisipam.org>

3 – Reference Material and Training Resources:

(available from the U.S. or internationally)

V.C.1. Government systems and networks

(V.B.1., V.B.2.)

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_264934255_15582250_1_1_1_1.00.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_264934255_15589524_1_1_1_1.00.html

OECD Ministerial Declaration on the Protection of

Privacy on Global Networks (1998)

Multi State Information Sharing and Analysis

Center : Main Page: <http://www.msiscac.org/>

The U.S. Federal Information Security Management

Act of 2002 (FISMA)

<http://csrc.nist.gov/policies/FISMA-final.pdf>

U.S. HSPD-7, "Critical Infrastructure Identification,

Prioritization and Protection"

<http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>

U.S. Federal Acquisition Regulations (FAR), parts

1.2,7,11, and 39. <http://www.acqnet.gov/FAR/>

The [U.S.] National Strategy to Secure Cyberspace:

http://www.dhs.gov/interweb/assetlibrary/nationalCyberspace_Strategy.pdf

U.S. CERT : <http://www.us-cert.gov/>

NIST site: <http://csrc.nist.gov/> 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

U.S. CERT: <http://www.us-cert.gov/>

U.S. DHS/Industry "Cyber Storm" exercises:

http://www.dhs.gov/xnews/releases/pr_1158340980371.stm

U.S. DHS R&D Plan:

<http://www.dhs.gov/xres/programs/>

U.S. Federal Plan for R&D:

http://www.nitrd.gov/pubs/csia/FederalPlan_CSIARnD.pdf

U.S. President's Information Technology Advisory

Committee report on Cyber Security research

priorities:

http://www.nitrd.gov/pitac/reports/20050301_cybsecurityresearch.pdf

The Self-Assessment Tool

- Objective: assist nations *organize* and *manage* national efforts to
 - *Prevent*
 - *Prepare for*
 - *Protect against*
 - *Respond to, and*
 - *Recover from*cybersecurity incidents.

Management Framework for Organizing National Cybersecurity Efforts: Self-Assessment Tool

Prepared by
Joseph P. Richardson
Joseph.richardson@ties.itu.int
202-258-9278