Helping the world communicate

International Telecommunication Union

Management Framework for Organizing National Cybersecurity/CIIP Efforts

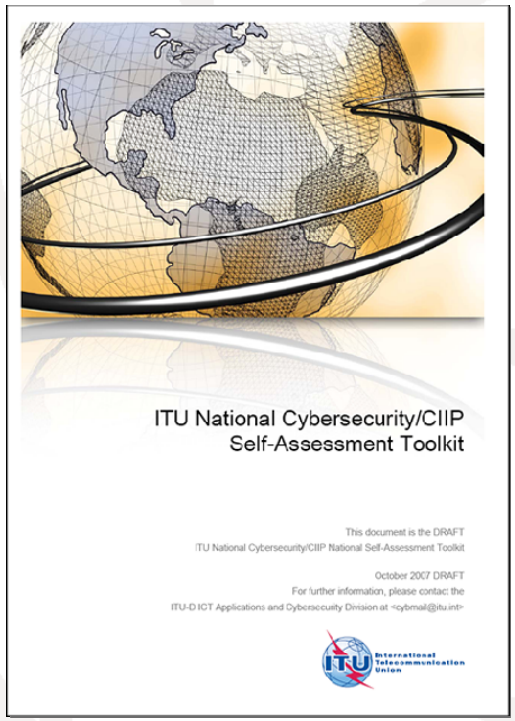
ITU Regional Workshop on Frameworks for Cybersecurity and CIIP
Doha, Qatar
18-21 February 2008

Joseph P. Richardson
<joseph.richardson@ties.itu.int>

ICT Applications and Cybersecurity Division
Telecommunication Development Sector (ITU-D)
International Telecommunication Union

The Framework is based on:

Work underway in ITU-D:



- Framework for National Cybersecurity/CIIP Efforts
- Report on Best Practices for Achieving Cybersecurity
- ITU National Cybersecurity Self-Assessment Toolkit

Why a Framework?
Why a National Strategy?

- Cybersecurity/CIIP is a SHARED responsibility

- All “participants” must be involved
  - Appropriate to their roles

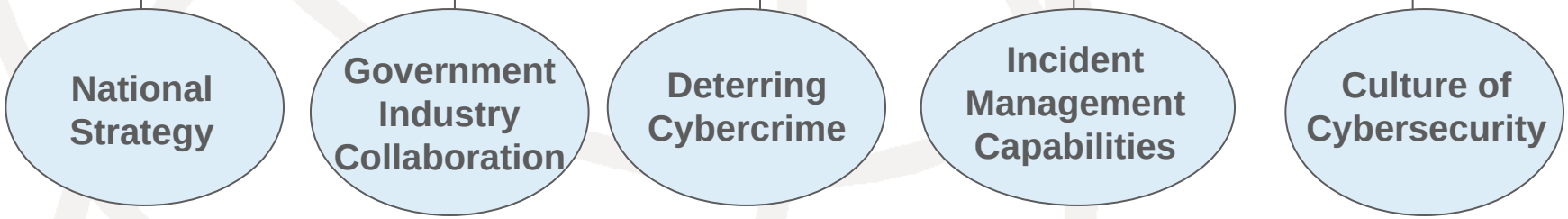
Participants

- "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"

Framework for National Cybersecurity/CIIP



Framework for National Cybersecurity/CIIP

For each of these five (5) elements, the Framework recommends:

- **POLICY** to guide national efforts
- **GOALS** to implement the policy
- **SPECIFIC STEPS** to achieve goals

ITU support for Framework and National implementation efforts:

- Best Practices for Achieving Cybersecurity
- Reference Material & Training Resources
- ITU National Cybersecurity/CIIP Self-Assessment Toolkit

Policy

- **National Strategy**:
  - *Protection of cyberspace is essential to national security and economic well-being.*
- **Government-Industry Collaboration**:
  - *Protection of cyberspace is a shared responsibility requiring collaboration between government and the private sector.*
- **Deterring Cybercrime**:
  - *Protection of cyberspace requires updating criminal laws, procedures and policy to address and respond to cybercrime.*

Policy

- **Incident Management Capabilities**:
  - *Protection of cyberspace requires a national focal point with mission of watch, warning, response and recovery; and collaboration with government entities, the private sector; and the international community.*
- **Culture of Cybersecurity**:
  - *Protection of cyberspace requires all participants who develop, own, provide, manage, service and use information networks to understand cybersecurity and take action appropriate to their roles.*

National Strategy

Policy: *Protection of cyberspace is essential to national security and economic well-being.*

Goals:

- **1.1.** Create awareness of need for national action and international cooperation.
- **1.2.** Develop national strategy.
- **1.3.** Participate in international efforts.

National Strategy

Specific Steps:

- **1.1.** Persuade leaders of need for action.
- **1.2.** Identify lead person and institution.
- **1.3.** Identify home for Computer Security Incident Response Team with national responsibility (N-CSIRT).
- **1.4.** Identify lead institutions for each element of the national strategy.
- **1.5.** Identify experts and policymakers and their roles.
- **1.6.** Identify and formalize cooperative arrangements.
- **1.7.** Establish mechanisms for government - private sector cooperation.
- **1.8.** Identify international counterparts; foster information sharing and assistance.
- **1.9.** Establish an integrated risk management process.
- **1.10.** Establish assessment/reassessment program.
- **1.11.** Identify training requirements.

Government-Industry Collaboration

Policy:

- *Protection of cyberspace is a shared responsibility requiring collaboration between government and the private sector.*

Goals:

- **2.1.** Develop government-industry collaboration.
- **2.2.** Use industry perspectives, equities and knowledge to enhance cybersecurity.

Specific Steps:

- **2.1.** Include industry.
- **2.2.** Encourage private sector groups to address common security interests and collaborate with government.
- **2.3.** Bring private sector and government together in trusted forums.
- **2.4.** Encourage cooperation among groups from interdependent industries.
- **2.5.** Establish government/ private sector arrangements for incident management and cooperation.

Deterring Cybercrime:

Policy:

- *Protection of cyberspace requires updating criminal laws, procedures and policy to address and respond to cybercrime.*

Goals:

- **3.1.** Enact and enforce a set of comprehensive laws relating to cybersecurity and cybercrime consistent with the provisions of the Convention on Cybercrime (2001).

Specific Steps:

- **3.1.** Assess the current legal authorities for adequacy.
- **3.2.** Draft and adopt substantive, procedural and mutual assistance laws and policies.
- **3.3.** Establish or identify national cybercrime units.
- **3.4.** Develop cooperative relationships with national cybersecurity infrastructure and private sector.
- **3.5.** Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.
- **3.6.** Participate in the 24/7 Cybercrime Point of Contact Network.

Incident Management Capabilities

Policy:

- *Protection of cyberspace requires a national focal point with mission of watch, warning, response and recovery; and collaboration with government entities, the private sector; and the international community.*

Goals:

- **4.1.** Develop coordinated national cyberspace security response system.
- **4.2.** Establish focal point for managing cyber incidents.
- **4.3.** Participate in information sharing mechanisms.
- **4.4.** Develop, test and exercise emergency response plans.

Incident Management Capabilities

Specific Steps:

- **4.1.** Identify or establish a national Computer Security Incident Response Team (N-CSIRT).
- **4.2.** Establish mechanism for coordination among all government agencies.
- **4.3.** Establish collaborative relationships with industry.
- **4.4.** Establish points of contact to facilitate information exchange with N-CSIRT.
- **4.5.** Participate in international cooperative activities.
- **4.6.** Develop tools and procedures for the protection of the cyber resources.
- **4.7.** Develop capability to respond to and recover from cyber incidents.
- **4.8.** Promote responsible disclosure practices.

Culture of Cybersecurity

Policy:

- *Protection of cyberspace requires all participants who develop, own, provide, manage, service and use information networks to understand cybersecurity and take action appropriate to their roles.*

Goals:

- **5.1.** Promote a national Culture of Cybersecurity.

Culture of Cybersecurity

Specific Steps:

- **5.1.** Implement a cybersecurity plan for government systems.
- **5.2.** Implement security awareness programs for government users.
- **5.3.** Encourage business to develop a Culture of Cybersecurity.
- **5.4.** Support outreach to civil society, children and individual users.
- **5.5.** Promote a comprehensive national awareness program.
- **5.6.** Enhance Science and Technology (S&T) and Research and Development (R&D).
- **5.7.** Review and update existing privacy regime.
- **5.8.** Develop awareness of cyber risks and available solutions.

Framework for National Cybersecurity Efforts	National Strategy	Government-Industry Collaboration	Deterring Cybercrime	Incident Management Capabilities	Culture of Cybersecurity
Policies	Developing and implementing a national cybersecurity plan requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, industry, and citizens) in the process.	Protecting critical information infrastructure and cyberspace is a shared responsibility that can best be accomplished through collaboration between government at all levels and the private sector, which owns and operates much of the infrastructure. It is important to recognize that although the world's information security systems have largely become an interoperable and interconnected whole, the structure of this network can vary greatly from country to country. Therefore, an effective and sustainable system of security will be enhanced by collaboration among owners and operators of these systems.	Cybersecurity can be greatly improved through the establishment and modernization of criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime.	It is important to maintain a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, whose national mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, industry, academia, and the international community.	Considering that personal computers are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and use information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Government must take a leadership role in bringing about this Culture of Cybersecurity and in supporting the efforts of other participants.
Goals	I.A.1. Create awareness at a national policy level about cybersecurity issues 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 both cyber and physical disruptions. I.A.3. Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents.	II.A.1. Develop government-industry collaborative relationships that work to effectively manage cyber risk and to protect cyberspace. II.A.2. Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.	III.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).	IV.A.1. Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to, and recover from cyber incidents. IV.A.2. Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents. IV.A.3. Participate in watch, warning, and incident response information sharing mechanisms. IV.A.4. Develop, test, and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.	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.
Steps	I.B.1. Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy-level discussions. 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 should be established; and identify lead institutions for each aspect 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 cybersecurity issues, including information sharing and assistance efforts. I.B.7. Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity. I.B.8. Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities. I.B.9. Identify training requirements and how to achieve them.	II.B.1. Include industry perspectives in the earliest stages of development and implementation of security policy and related efforts. II.B.2. Encourage development of private sector groups from different critical infrastructure industries to address common security interests collaboratively with government. II.B.3. Bring private sector groups and government together in trusted forums to address common cybersecurity challenges. II.B.4. Encourage cooperation among groups from interdependent industries. II.B.5. Establish cooperative arrangements between government and the private sector for incident management.	III.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. III.B.2. Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime. III.B.3. Establish or identify national cybercrime units. III.B.4. Develop cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector. III.B.5. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues. III.B.6. Participate in the 24/7 Cybercrime Point of Contact Network.	IV.B.1. Identify or establish a national CSIRT (N-CSIRT) capability. IV.B.2. Establish mechanism(s) within government for coordination among civilian and government agencies. IV.B.3. Establish collaborative relationships with industry to prepare for, detect, respond to, and recover from national cyber incidents. IV.B.4. Establish point(s) of contact within government agencies, industry and international partners to facilitate consultation, cooperation, and information exchange with the N-CSIRT. IV.B.5. Participate in international cooperative and information sharing activities. IV.B.6. Develop tools and procedures for the protection of the cyber resources of government entities. IV.B.7. Develop a capability through the N-CSIRT for coordination of governmental operations to respond to and recover from large-scale cyber attacks. IV.B.8. Promote responsible disclosure practices to protect operations and the integrity of the cyber infrastructure.	V.B.1. Implement a cybersecurity plan for government-operated systems. V.B.2. Implement security awareness programs and initiatives for users of systems and networks. V.B.3. Encourage the development of a culture of security in business enterprises. 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.

International Telecommunication Union

Framework for National Cybersecurity Efforts

Resources

National Strategy

I.C.1. Awareness raising (I.B.1, I.B.2)
- UN World Summit on the Information Society Declaration of Principles and Plan of Action: www.itu.int/WSIS/index.html
- ITU Development Sector Cybersecurity: www.itu.int/ITU-D/cyb/
- ITU Cybersecurity Gateway: www.itu.int/cybersecurity/gateway/
- OECD Guidelines and Culture of Security: www.oecd.org/sti/cultureofsecurity
- UNGA Resolutions 55/63, 56/121, 57/239, 58/199: www.un.org/Depts/dhl/resguide/gares1.htm
- The (U.S.) National Strategy to Secure Cyberspace: www.dhs.gov/interweb/assetlibrary/national_Cyberspace_Strategy.pdf
- United States Sector Specific Plans: www.dhs.gov/xprevprot/programs/gc_1179866197607.sthm
- Information Technology Association of America White Paper on Information Security: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- "Information Society in an Enlarged Europe," Budapest, 2/26/04: http://ec.europa.eu/archives/commission_1999_2004/liikanen/media/speeches/index_en.htm
- "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
- European Network and Information Security Agency: www.enisa.europa.eu/
- The Meridian Conference: www.meridian2007.org/

I.C.2. National Strategy (I.B.2, I.B.3, I.B.4, I.B.5, I.B.7)
- U.S. National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb/
- National Implementation Strategies of 11 OECD members: www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- UK Centre for the Protection of National Infrastructure (CPNI): www.cpni.gov.uk/
- UK Critical Information Infrastructure Protection Directory (government only) - to participate or obtain information email: ciip-directory@niscc.gov.uk
- New Zealand: www.digitalstrategy.govt.nz
- Canada: www.psepc-sppcc.gc.ca

I.C.3. Assessment and program development (I.B.5, I.B.7, I.B.8)
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003
- NIST SP 800-30 Risk Management Guide for Information Technology Systems, July 2002
- Control Objectives for Information and Related Technology (COBIT) 3.0/4.0

Government-Industry Collaboration

II.C.1. Structures for Government-Industry Collaboration
- United States Information Sharing and Analysis Centers (ISACs) & Coordinating Councils
  - Financial Services ISAC: www.fsisac.com
  - Electric Sector ISAC : www.esisac.com/
  - Information Technology ISAC: www.it-isac.org
  - Telecommunications ISAC: www.ncs.gov/ncc/
  - Network Reliability and Interoperability Council (NRIC): www.nric.org/
  - National Security and Telecommunications Advisory Committee (NSTAC): www.ncs.gov/nstac/nstac.html
- IT Sector Specific Plan: www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- United States Sector Specific Plans: www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- Information Technology Association of America White Paper on Information Security: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- Industry-Government Cooperation on Standards: American National Standards Institute-Homeland Security Standards Panel: www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3
- National Telecommunications and Information Administration: www.ntia.doc.gov
- IT Sector Coordinating Council (SCC): www.it-scc.org
- U.S. National Infrastructure Protection Plan: www.dhs.gov/xprevprot/programs/editorial_0827.shtm

II.C.2. Cybersecurity information sharing
- National Information Assurance Council (NIAC) report on sector partnership model working group: http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- US-CERT alerts: www.us-cert.gov/cas/
- Network Reliability and Interoperability Council: www.nric.org
- National Institute of Standards and Technology, Computer Security and Research Center: 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

II.C.3. Awareness raising and outreach: Tools for business and home use
- Information for technical and non-technical users: www.us-cert.gov/
- StaySafeOnLine: www.staysafeonline.org/

Deterring Cybercrime

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

Incident Management Capabilities

IV.C.1. National Response Plan
- National Response Plan: www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- StaySafeOnline: www.staysafeonline.info/
- Information Security and Privacy Advisory Board: http://csrc.nist.gov/ispab/
- NIST: http://csrc.nist.gov/

IV.C.2 National CSIRT
- US CERT: www.us-cert.gov/
- NIATEC training courses: http://niatec.info
- Carnegie Mellon University/CERT Coordination Center: www.cert.org/csirts/
- European Network and Information Security Agency document: A Step-by-Step Approach on How to Set Up a CSIRT: www.enisa.europa.eu/pages/05_01.htm
- India: www.cert-in.org.in
- Australia: www.auscert.org.au

IV.C.3 Cooperation and Information Sharing
- OECD's Anti-Spam toolkit: www.oecd-antispam.org
- IT-ISAC: www.it-isac.org/
- IT Sector Coordinating Council: www.it-scc.org/
- ISO, Joint Technical Committee 1, Subcommittee 27 (ISO/JTC1/SC27): www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopelist=CATALOGUE
- Forum of International Response Security Teams: www.first.org

IV.C.4 Vulnerability Information/Tools and Techniques
- National Vulnerability Database (NVD): 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: http://buildsecurityin.us-cert.gov/daisy/bsi/home.html
- Common Vulnerabilities and Exposures List (CVE): www.cve.mitre.org/about/

Culture of Cybersecurity

V.C.1. Government systems and networks (V.B.1, V.B.2, V.B.7)
- UNGA RES 57/239 Annexes a and b: www.un.org/Depts/dhl/resguide/r57.htm
- OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" [2002]: www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (Adopted Sept. 23, 1980): www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998) The Promotion of A Culture of Security for Information Systems and Networks in OECD Countries (DSTI/ICCP/REG(2005)1/Final.
- Multi State Information Sharing and Analysis Center: Main Page: www.msisac.org/
- The U.S. Federal Information Security Management Act of 2002 (FISMA): http://csrc.nist.gov/policies/FISMA-final.pdf
- U.S. HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection": www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- U.S. Federal Acquisition Regulation (FAR), parts 1,2,7,11, and 39: www.acqnet.gov/FAR/
- The [U.S.] National Strategy to Secure Cyberspace: www.whitehouse.gov/pcipb/
- U.S. CERT: www.us-cert.gov/
- U.S. NIST: 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
- U.S. CERT: www.us-cert.gov
- U.S. DHS/Industry "Cyber Storm" exercises: www.dhs.gov/xnews/releases/pr_1158340980371.shtm
- U.S. DHS R&D Plan: www.dhs.gov/xres/programs/
- U.S. Federal Plan for R&D: www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- U.S. President's Information Technology Advisory Committee report on Cyber Security research priorities: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

International Telecommunication Union

Framework for National Cybersecurity Efforts	National Strategy	Government-Industry Collaboration	Deterring Cybercrime	Incident Management Capabilities	Culture of Cybersecurity
Resources	• Disaster Recovery Institute International (DRII) • International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 Series, Information technology—Security techniques—Information security management systems • ISO/IEC 13335, Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management • ISO/IEC 17799, 2005 Information technology—Security techniques—Code of practice for information security management • ISO/IEC 21827, Systems Security Engineering—Capability Maturity Model (SSE-CMM®) • Information Technology Infrastructure Library (ITIL) Security Management • NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook • NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems • NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems • NIST Draft Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems • Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) I.C.4. International assistance points of contact (I.B.6) • Forum of Incident Response Security Teams (FIRST): www.first.org • Anti-Phishing Working Group: www.antiphishing.org • World Information Technology Services Alliance: www.witsa.org • Internet Engineering Task Force: www.ietf.org • World Wide Web Consortium: www.w3c.org • Institute of Electrical and Electronics Engineers: www.ieee.org • Messaging Anti-Abuse Working Group: www.maawg.org	• Federal Trade Commission, Onguard Online: www.ftc.gov/infosecurity and www.OnGuardOnline.gov • U.S. CERT posters and information sheets: www.uscert.gov/reading_room/distributable.html • OECD's Anti-Spam Toolkit: www.oecd-antispam.org • London Action Plan Spam Enforcement Cooperation Network: www.londonactionplan.org			V.C.3. Individuals and civil society (V.B.4., V.B.6, V.B.7.) • Stay Safe Online: www.staysafeonline.info/ • OnGuard Online: http://onguardonline.gov • U.S. CERT: www.us-cert.gov/nav/nt01/ • OECD's Anti-Spam toolkit: www.oecd-antispam.org • See also: The OECD questionnaire on implementation of a Culture of Security (which is found at DSTI/ICCP/REG(2004)4/Final) and the U.S. response to the questionnaire (which is found at http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase). The U.S. response to the questionnaire provides a comprehensive outline of U.S. efforts in this area. • New Zealand: www.netsafe.org.nz • Canada: www.psepc-sppcc.gc.ca

* Parenthetical references in each column, e.g., (I.B.1., I.B.2.), identify associated Specific Steps.

Government Actions

- Provide leadership, guidance and coordination for national effort and international cooperation
  - Identify lead person and institution for developing national strategy
  - Identify lead persons and institutions for operation of each element of national strategy
  - Develop computer security incident response team with national responsibility (N-CSIRT)
  - Identify cooperative arrangements and mechanisms for cooperation among all participants

Government Actions

- Provide leadership, guidance and coordination for national effort and international cooperation *(continued)*
  - Identify international counterparts and relationships
  - Identify experts
  - Establish integrated risk management process
  - Assess and periodically reassess cybersecurity
  - Identify training requirements

International Telecommunication Union

Getting Started on a National Strategy

ITU National Cybersecurity/CIIP Self–Assessment Toolkit

Self – Assessment Toolkit

- Based on *Best Practices* document
- Focus: national *management* and *policy* level
- Intended to assist national governments:
  - Understand existing national approach
  - Develop "baseline" re *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

The Self-Assessment Toolkit

- Examines each element of Framework at management and policy level:
  - National Strategy
  - Government - Industry Collaboration
  - Deterring Cybercrime
  - National Incident Management Capabilities
  - Culture of Cybersecurity

The Self-Assessment Toolkit

- Looks at organizational issues for each element of Framework:
  - The people
  - The institutions
  - The relationships
  - The policies
  - The procedures
  - The budget and resources

The Self-Assessment Toolkit

- Identifies issues and poses questions:
  - What Actions have been taken?
  - What Actions are planned?
  - What Actions are to be considered?
  - What is the Status of these actions?

The Self-Assessment Toolkit

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

National Pilot Tests

- ITU-D pilot tests of self-assessment tool
  - Vietnam (August 2007)
  - Argentina (2007)
  - 2008 – to be determined

- For information on ITU-D pilot test program
  - contact cybmail@itu.int

ITU National Cybersecurity/CIIP Self-Assessment Toolkit

- Additional and updated information at

  http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

International Telecommunication Union

Helping the World Communicate