Committed to Connecting the World

International Telecommunication Union

ITU-D Cybersecurity Activities

Overview of Activities to support the Americas Region April 2008

Joseph Richardson
Joseph.Richardson@ties.itu.int
for
ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

This Presentation

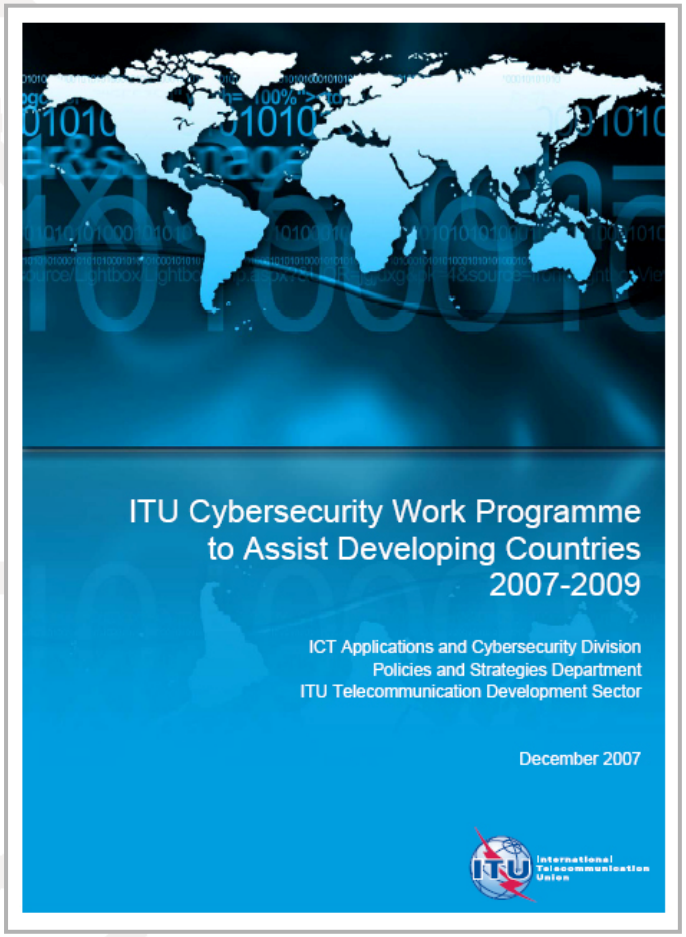
- ITU-D and Cybersecurity
- ITU Cybersecurity Framework
- Implementing the Framework Nationally
- Getting started with the ITU Self–Assessment Toolkit
- References related to the Americas

ITU Development Sector Role

- From ITU Plenipotentiary Conference (Antalya, 2006):
  - Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies;
- From World Telecommunication Development Conference (Doha, 2006):
  - ITU-D Study Group 1 Question 22/1
  - Cybersecurity part of Programme 3 managed by ITU–D ICT Applications and Cybersecurity Division

Key Activities Underway

- ITU-D Study Group 1 Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*
  - Developing *Framework for Organizing a National Approach to Cybersecurity*
- ITU-D Programme 3 *ITU Cybersecurity Work Programme to Assist Developing Countries*
- Synergies between these two activities



Cybersecurity Framework Origins

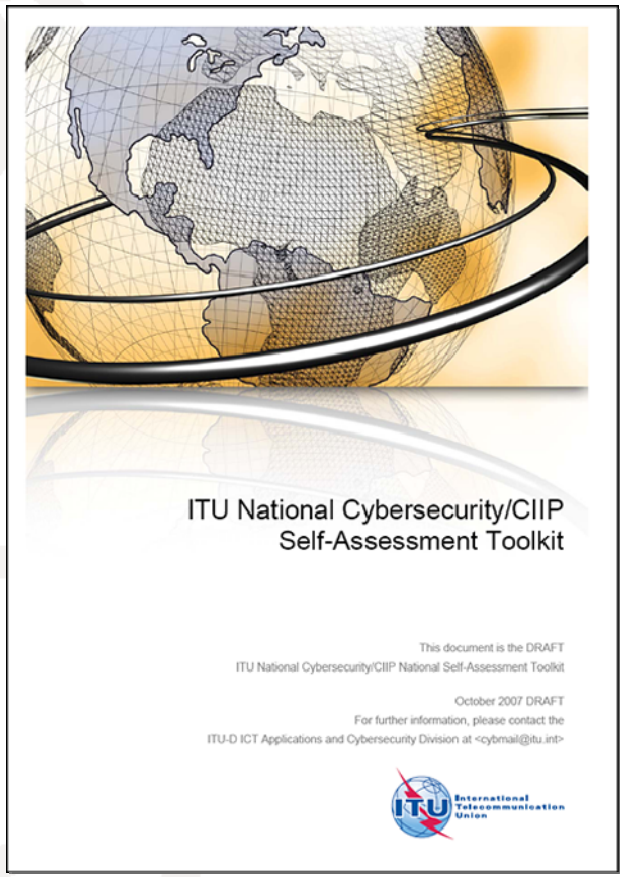
- International and Regional Efforts:
  - United Nations General Assembly (UNGA)
    - Resolutions (57/239 & 58/199)
  - Organization for Economic Cooperation and Development (OECD)
  - G8
  - Council of Europe (CoE)
  - Asia Pacific Economic Cooperation (APEC)
  - Organization of American States (OAS)
  - League of Arab States
  - Gulf Cooperation Council (GCC)
  - World Summit on the Information Society (WSIS)
  - ITU Global Cybersecurity Agenda
  - ITU-D Study Group 22/1

Cybersecurity Framework Origins

- In Organization of American States:
  - OAS General Assembly Resolution 1939 of 2003 called for the development of a draft cybersecurity strategy for Member States, in coordination and collaboration with CITEL, CICTE, REMJA, and other bodies of the OAS
- CITEL: Inter-American Telecommunication Commission
  - http://www.citel.oas.org
- CICTE: Inter-American Committee Against Terrorism
  - http://www.cicte.oas.org
- REMJA: Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA)
  - http://www.oas.org/juridico/english/cyber.htm

ITU Cybersecurity Framework

- Work in ITU-D:
  - Framework for National Cybersecurity/CIIP Efforts
- Q22.1 Report on Best Practices for Achieving Cybersecurity
- ITU National Cybersecurity Self-Assessment Toolkit



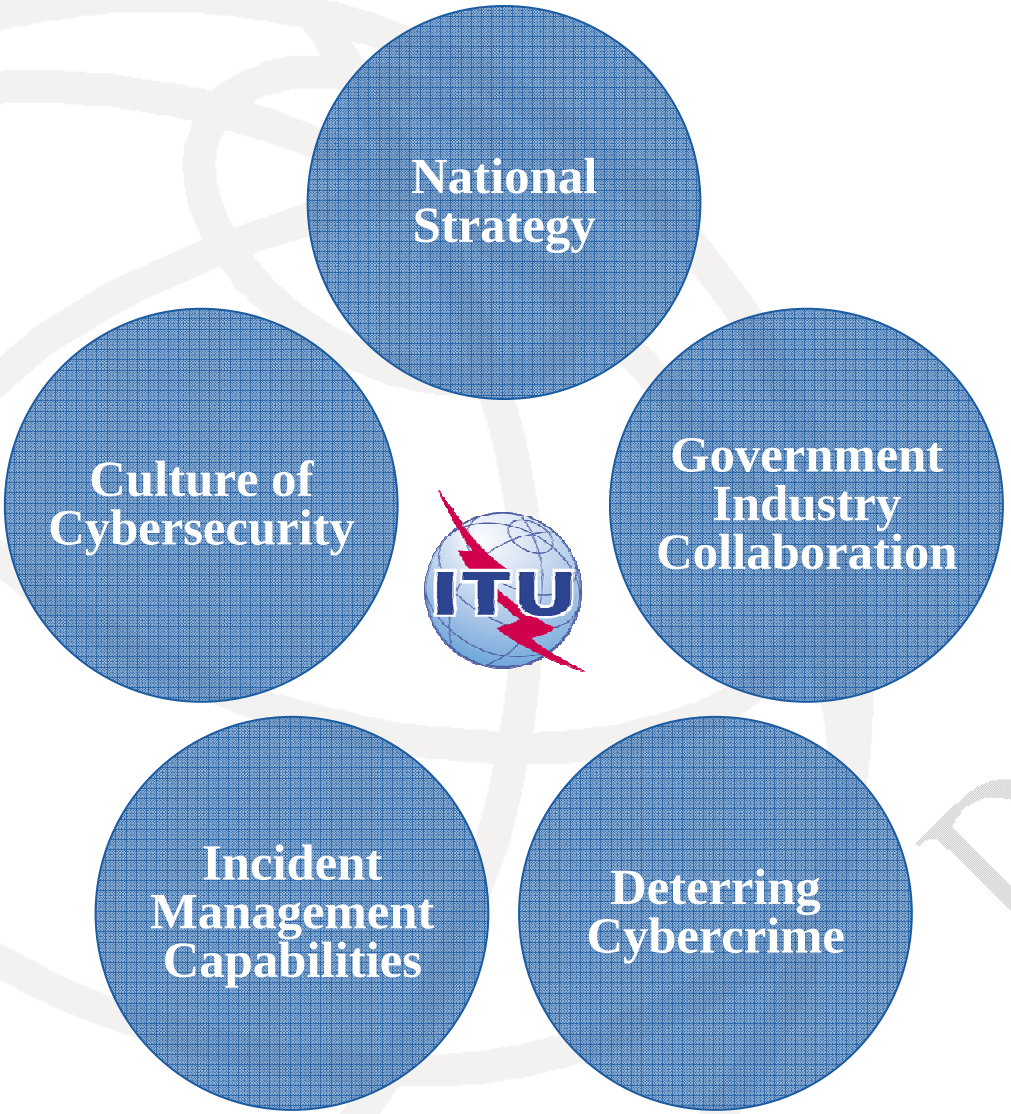
Why a Framework?

- Why is a National Strategy needed?
- Cybersecurity/Critical Information Infrastructure Protection (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"*
    - From "UNGA Resolution 57/239 Creation of a global culture of cybersecurity"

ITU Framework for National Action



Framework for Action

- For each of these five elements: ITU support includes:
  - Best Practices for Achieving Cybersecurity
  - Reference Material & Training Resources
  - Self-Assessment Toolkit
  - Cybersecurity Forums with capacity-building in Member States

Framework for Action

- For each of these five elements, the Framework recommends:
  - POLICY: to guide national efforts
  - GOALS: to implement the policy
  - SPECIFIC STEPS: to achieve goals

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.

Goals

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

Goals

- Government-Industry Collaboration:
  - 2.1. Develop government-industry collaboration.
  - 2.2. Use industry perspectives, equities and knowledge to enhance cybersecurity.

Goals

- Deterring Cybercrime:
  - 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).

Goals

- Incident Management Capabilities:
  - 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.

Goals

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

Specific Steps

- National Strategy:
  - 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.

Specific Steps

- National Strategy cont'd:
  - 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.

Specific Steps

- National Strategy cont'd:
  - 1.9. Establish an integrated risk management process.
  - 1.10. Establish assessment/reassessment program.
  - 1.11. Identify training requirements.

Specific Steps

- Government-Industry Collaboration:
  - 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.

Specific Steps

- Deterring Cybercrime:
  - 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.

Specific Steps

- Incident Management Capabilities:
  - 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.

Specific Steps

- Culture of Cybersecurity:
  - 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.

ITU International Telecommunication Union

Implementing the Framework Nationally

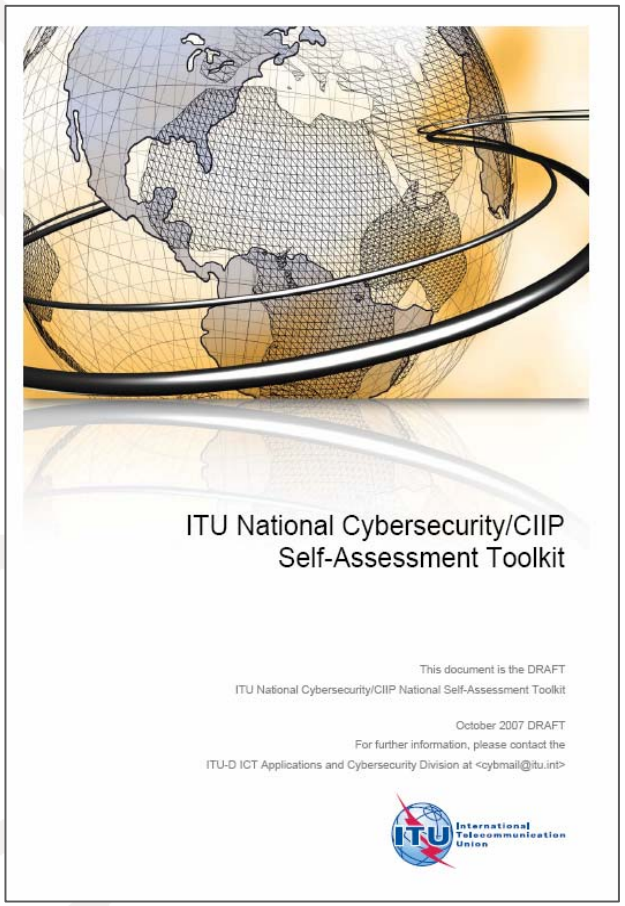
- Actions by Government
- Collaboration by other participants

Government Actions

- Provide leadership, guidance and coordination
  - Identify lead persons and institutions
  - Develop CSIRT with national responsibility
  - Identify cooperative arrangements and mechanisms among all participants
  - Identify international counterparts and relationships
  - Identify experts
  - Establish integrated risk management process
  - Assess and periodically reassess cybersecurity
  - Identify training requirements

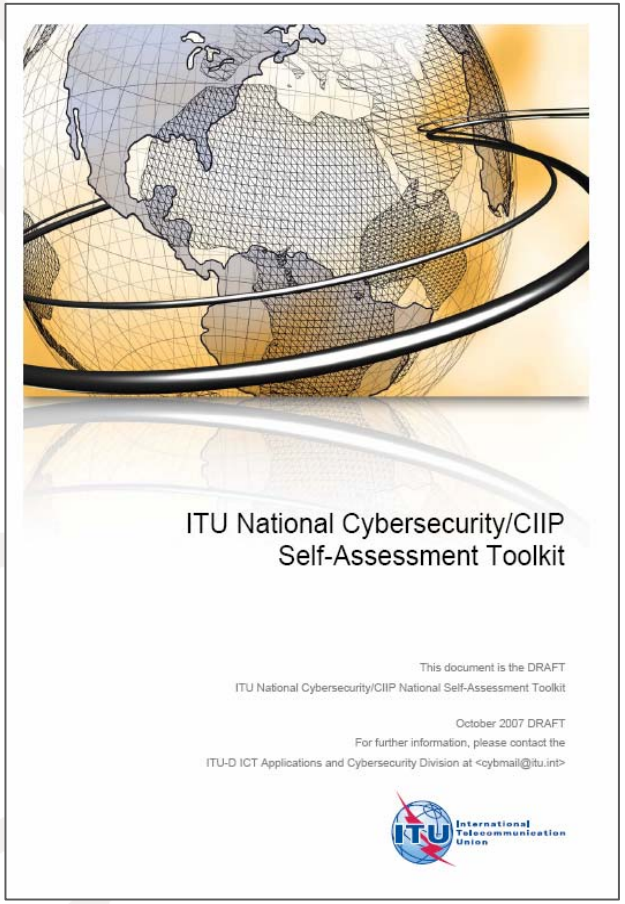
ITU National Cybersecurity/CIIP Self–Assessment Toolkit

- Based on Q.22/1 Framework
- Focused on national management and policy level
- Intended to assist national administrations to:
  - understand existing approach
  - compare to best practices
  - identify areas for attention
  - prioritize national efforts



ITU National Cybersecurity/CIIP Self–Assessment Toolkit

- Includes Annex on Deterring Cybercrime: Substantive, Procedural and Mutual Assistance Law Baseline Survey
- Intended to assist national authorities to review their domestic situation related to goals and actions identified in:
  - UN Resolutions 55/63 (2000) and 56/121 (2001): Combating the Criminal Misuse of Information Technologies
  - Council of Europe's Convention on Cybercrime (2001)
- Adapted from work in APEC-TEL



ITU National Cybersecurity/CIIP Self-Assessment Toolkit

- Additional & updated information at:
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- Including:
  - Powerpoint Project Overview (October 2007)
  - ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts (January 2008)
  - Draft ITU National Cybersecurity/CIIP Self-Assessment Toolkit (January 2008)
  - Draft Background Information for National Pilot Tests (December 2007)
  - Draft Implementation Matrix Work Booklet (Word, PDF) (October 2007)

ITU 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.

Country Self-Assessment Exercises

- ITU-D country self-assessments
  - Vietnam (August 2007)
  - Argentina (October 2007)
  - Qatar (February 2008)
  - 2008: More planned
- To request a country self-assessment exercise, contact:
  - cybmail@itu.int

Regional Cybersecurity Forums

- August 2007: Vietnam
- October 2007: Argentina
- November 2007: Cape Verde
- February 2008: Qatar
- July 2008: Australia
- August 2008: Zambia
- October 2008: Bulgaria
- November 2008: Tunisia
- December 2008: OAS (Miami) (TBC)

Next Steps

- What are the next steps
  - for your nation?
  - for your region?

Special References for Americas

- Recent Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection, Buenos Aires, Argentina, October 2007
  - www.itu.int/ITU-D/cyb/events/2007/buenos-aires/
  - Final Meeting Report (English Rev 1.0, Español)
  - Meeting Presentations
- OAS/CITEL/REMJA/CICTE/ITU-D holding discussions on joint activities for regional cybersecurity strategy
  - December 2007 joint event being discussed
  - Toolkit materials to be made available in Spanish
- Mailing list for cybersecurity discussion just created for cybersecurity discussions in the Americas:
  - cybersecurity-americas@itu.int
    - contact cybmail@itu.int to join

More Information

- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/itu-d/cyb/
- ITU-D Cybersecurity Overview
  - www.itu.int/itu-d/cyb/cybersecurity/
- Study Group Q.22/1: Report On Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
- National Cybersecurity/CIIP Self-Assessment Toolkit
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- ITU-D Cybersecurity Work Programme to Assist Developing Countries:
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf
- Regional Cybersecurity Forums
  - www.itu.int/ITU-D/cyb/events/
- Botnet Mitigation Toolkit
  - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

International Telecommunication Union

Committed to connecting the world