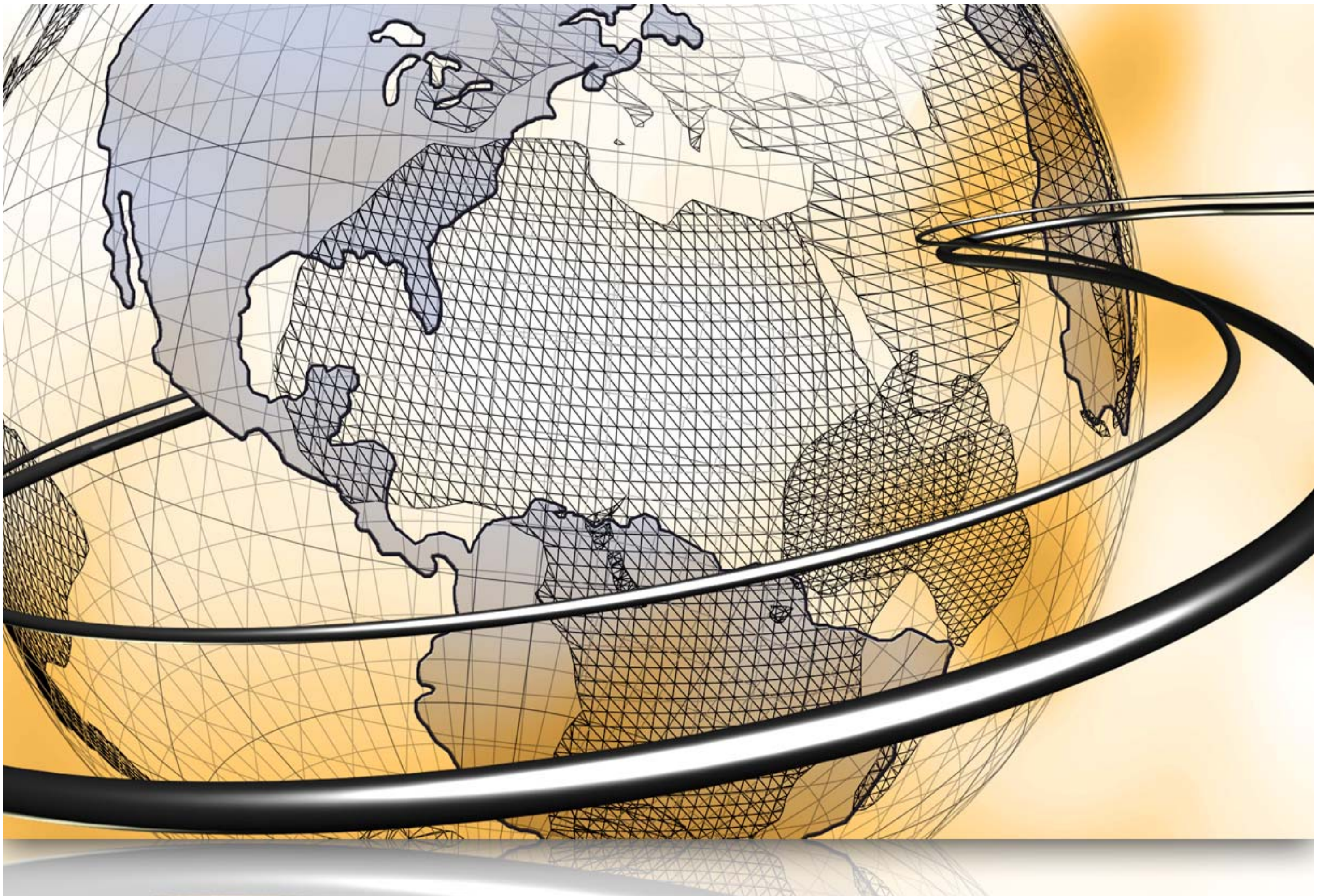

ITU National Cybersecurity/CIIP Self-Assessment Toolkit

Background Information for National Pilot Tests

This document provides background information for pilot tests of the ITU National Cybersecurity/CIIP National Self-Assessment Toolkit

December 2007 DRAFT

For further information, please contact the ITU-D ICT Applications and Cybersecurity Division at <cybmail@itu.int>

International
Telecommunication
Union

The **ITU National Cybersecurity/CIIP Self Assessment Toolkit** is based on studies underway in the ITU Telecommunication Development Sector's Study Group 1, Question 22/1: *Securing information and communication networks: best practices for developing a culture of cybersecurity*. This activity calls for ITU Member States and Sector Members to create a report on national best practices in the field of cybersecurity. More information on Question 22/1 activities can be found at the website www.itu.int/ITU-D/cyb/cybersecurity/.

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

In particular, the current version of the toolkit is based on the October 2007 draft of the *Report on Best Practices for a National Approach to Cybersecurity: A Basic Management Framework for Organizing National Cybersecurity Efforts*. This document provides background information for national authorities considering pilot tests of the toolkit. The toolkit, developed by Joseph Richardson, is intended to assist national government officials in examining their related existing national cybersecurity/CIIP policies, procedures, norms, institutions, and relationships.

The latest version of this document is available at:

www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit-info.pdf

For further information on participating in the toolkit pilot tests, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Table of Contents

Background 4

Objectives of the Toolkit 4

Actors Involved 5

Actors Involved in Development of a National Strategy 5

Actors Involved in National Coordination Efforts 6

Actors Involved in Government-Industry Collaboration 6

Actors Involved in Deterring Cybercrime 6

Actors Involved in Incident Management.. 7

Actors Involved in Promoting a Culture of Security 7

Background

The ITU National Cybersecurity/CIIP Self-Assessment Toolkit is derived from work underway in the ITU Telecommunication Development Sector's Study Group 1, Question 22/1: *Securing information and communication networks: best practices for developing a culture of cybersecurity*.

This activity calls for ITU Member States and Sector Members to create a report on national best practices in the field of cybersecurity.

The toolkit is based on the October 2007 draft of the *Report on Best Practices for a National Approach to Cybersecurity: A Basic Management Framework for Organizing National Cybersecurity Efforts* (hereafter the *Report*). More information on Question 22/1 activities can be found at the website:

- www.itu.int/ITU-D/cyb/cybersecurity/

Objectives of the Toolkit

The toolkit is intended to assist national government officials at the management level in examining their existing national policies, procedures, norms, institutions, and relationships in light of *the Report.* It assists in identifying:

- major players involved in cybersecurity/critical information infrastructure protection (CIIP) in a country; and
- their roles and their means of coordination, interaction, and cooperation.

The toolkit assists policy makers and managers from relevant agencies and institutions to discuss among themselves their nation's cybersecurity efforts and arrangements.

During initial discussions among relevant agencies and institutions to consider the toolkit, ideally national relevant agencies and institutions should be represented at similar levels in order to facilitate dialogue among peers. Experience to date has demonstrated that as a target level, ideally this should be at the Director General or Deputy Director General. However, additional representatives at lower levels would of course be welcome to attend the session.

These actors would ideally participate in the self-assessment efforts. In addition, consideration should be given to including relevant private sector players and associations in the self-assessment dialogue.

Actors Involved

The suggested governmental roles and agencies that would normally be involved in the elaboration, development and operation of a national cybersecurity effort are discussed below.

Actors Involved in **Development of a National Strategy**

Some countries may have already designated an agency to coordinate and lead interagency efforts and a specific national strategy. Other countries may have taken only initial steps and thus may need to identify a person and institution that will lead development of a national cybersecurity/CIIP framework. This role is typically under the head of government and could include a national security council or a cabinet level coordination mechanism.

Actors Involved in **National Coordination Efforts**

The agency that will provide operational guidance and likely head the interagency coordination effort on cybersecurity/CIIP. Most likely, this would be different from the agency that originally developed the national strategy. For example, in the United States of America, this role is partially handled by the National Cyber Response Coordination Group (NCRCG), a forum of 13 principal agencies that coordinate intra-governmental and public/private preparedness operations to respond to and recover from cyber attacks.

Actors Involved in **Government-Industry Collaboration**

The agencies that have significant interaction with the private sector in regard to cybersecurity whether for cybercrime, incident management, or technical and/or policy development. For example, in the United States, a number of agencies are involved in these areas. They include the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) and police related to cybercrime; the Department of Homeland Security (DHS) and USCERT and the Department of Defense (DOD) related to incident management; and the Departments of Homeland Security (DHS) and Commerce (DOC) related to technical and policy development.

Actors Involved in **Deterring Cybercrime**

These are the agencies and institutions that develop and enforce laws related to cybersecurity. For example, in the United States, this includes the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) and police related to investigating and prosecuting cybercrime.

Consideration should also be given to including the Courts and the legislature in a self-assessment effort.

Actors Involved in **Incident Management**

These are the principal agencies and institutions responsible for preparedness operations to respond to and recover from cyber incidents. The private sector is also a key player in this area. For example, in the Unites States, the lead players are the Department of Homeland Security (DHS) and USCERT. In addition, many other agencies, individually or through the United States' GOVCERT, are involved. Among these are the principal agencies of the National Cyber Response Coordination Group (NCRCG) which also includes the Department of Defense (DOD). Private sector CSIRTS and industry associations are also involved.

Actors Involved in **Promoting a Culture of Security**

Much of the effort in this area involves awareness raising among individuals, small businesses and other users. This area also includes specific issues such as privacy, and research and development (R&D). In the United States, much of this work is carried out by agencies involved in other areas of cybersecurity noted above. One principal addition is the Federal Trade Commission (FTC) in matters related to privacy.