ITU National Cybersecurity/CIIP Self-Assessment Tool

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

April 2009 Revised 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 Tool** is a practical initiative by the ITU-D ICT Applications and Cybersecurity Division to assist ITU Member States who wish to elaborate on their national approach for cybersecurity and critical information infrastructure protection (CIIP). The National Cybersecurity/CIIP Self-Assessment Tool is one of the complementary cybersecurity resources that the ITU is currently developing as part of a Cybersecurity Toolkit for Member States.

The National Cybersecurity/CIIP Self-Assessment Tool, initially 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 tool is built on work currently being undertaken in ITU in the area of cybersecurity. It is a work in progress and will be further integrated with other ongoing ITU initiatives and activities as these evolve.

The latest version of this document is available at:

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

For further information on the National Cybersecurity/CIIP Self-Assessment Tool and related resources of the ITU Cybersecurity Toolkit, 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

INTRODUCTION

Modern societies have a large and growing dependency on information and communication technologies (ICTs) that have become essential to national security, economic well-being and social cohesion for all nations. At the same time, these technologies are globally interconnected producing global interdependencies and they contain vulnerabilities and introduce threats to the national systems and to the nation. In order to maximize societies' benefits from these ICTs, the risks resulting from interdependences, vulnerabilities and threats must be managed. Enhancing cybersecurity and improving critical information infrastructure protection (CIIP) have become the watchwords for efforts by all nations to address and manage these risks.

Cybersecurity/CIIP is a shared responsibility of government, business, other organizations, and individual users who develop, own, provide, manage, service and use these information systems and networks (the "participants"[1]). Managing the inherent risks requires that the participants act cooperatively and in coordination with one other, and that each participant take action to address security appropriate to its role. The collective goal of participants is to prevent, prepare for, respond to, and recover from incidents. In this interconnected system, the roles and responsibilities of participants for cybersecurity/CIIP are shared and often overlap. Only when all participants share a common vision and understanding of the security objectives and how to achieve them, as well as their individual roles in the effort, can the collective goal be achieved.

[1] See OECD, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002, available at: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html; UN Resolution 57/239: Creation of a Global Culture of Cybersecurity, 2002, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf; UN Resolution 58/199: Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 2004, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

Only national governments are in a position to lead national efforts involving all relevant national participants to enhance cybersecurity and improve CIIP. The preparation of a national strategy has proven to be a valuable tool for effective, coordinated national action. By establishing a common vision and delineating participant roles and responsibilities, the national strategy provides a guide for managing risks inherent in ICT use and addressing cybersecurity/CIIP. Such a national strategy statement can also provide valuable support for regional and international cooperation. Only when a nation has organized itself to address cybersecurity/CIIP can it gain requisite experience and capability that will allow it to participate meaningfully in regional and international cooperative security efforts.

The ***ITU National Cybersecurity/CIIP Self-Assessment Tool*** is intended to assist ITU Member States in developing a national strategy for cybersecurity/CIIP by examining their existing national policies, procedures, norms, institutions, and relationships for addressing the cybersecurity/CIIP challenge, by identifying their own national requirements to enhance cybersecurity and address CIIP, and by outlining a national response plan. The tool is directed to national leadership at the policy and management level of government. It addresses the policies, institutional frameworks and relationships required to enhance cybersecurity/CIIP. It seeks to produce a snapshot of the current state of national cybersecurity/CIIP efforts, identify goals, and delineate the roles, responsibilities and relationships among the key institutions and participants whose coordinated efforts will be required by the national effort. It aims towards the production of a statement that will delineate roles and responsibilities, set priorities, establish timeframes and provide metrics for addressing cybersecurity/CIIP. The authors hope that upon completion of a national self-assessment using this ITU tool, users will have a draft national cybersecurity/CIIP strategy statement that could be circulated to participants for review, discussion and finalization.

BACKGROUND

A fundamental role of ITU, following the World Summit on the Information Society (WSIS)[2], and the 2006 ITU Plenipotentiary Conference, is to continue to build confidence and security in the use of information and communication technologies (ICTs). The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent global strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. In this regard, the World Summit on the Information Society recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime. Paragraphs 108-110 of the *WSIS Tunis Agenda for the Information Society*[3], including the Annex, set out a plan for multi-stakeholder implementation at the international level of the *WSIS Geneva Plan of Action*[4] describing the multi-stakeholder implementation process according to eleven action lines and allocating responsibilities for facilitating implementation of the different action lines. At the WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, dedicated to building confidence and security in the use of ICTs.[5]

In this regard, the International Telecommunication Union Secretary-General launched the ***ITU Global Cybersecurity Agenda (GCA)***[6] on 17 May 2007, on the occasion of the 2007 World Telecommunication and Information Society Day, alongside partners from governments, industry, regional and international organizations, academic and research institutions.

[2] For more information on the World Summit on the Information Society (WSIS), which was conducted in two phases, in Geneva, Switzerland (2003) and Tunis, Tunisia (2005), see: http://www.itu.int/wsis/.
[3] The WSIS Tunis Agenda for the Information Society available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.
[4] The WSIS Geneva Plan of Action available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.
[5] For more information on WSIS action line C5: Building confidence and security in the use of ICTs see: http://www.itu.int/wsis/c5/.
[6] For more information on the Global Cybersecurity Agenda (GCA) see: http://www.itu.int/cybersecurity/gca/.

As such the GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the Information Society. It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Within ITU, the Global Cybersecurity Agenda complements existing ITU work programmes by facilitating the implementation of the three ITU Sectors' cybersecurity activities, within a framework of international cooperation.

The GCA is now moving into its operational phase and ITU is undertaking a number of efforts across its full range of activities to address cybersecurity. The ***ITU National Cybersecurity/CIIP Self-Assessment Tool*** is part of that effort. It is a practical initiative that grew out of the work 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[7], where ITU Member States and Sector Members are developing a best practices document that elaborates issues of cybersecurity.

The ***ITU National Cybersecurity/CIIP Self-Assessment Tool***[8] is intended to assist ITU Member States in examining their existing national policies, procedures, norms, institutions, and relationships in light of these international best practices. The self-assessment tool is intended to assist Member States to identify and respond to their own national requirements to enhance cybersecurity and address CIIP and thereby to participate more effectively in regional and international efforts. The tool is directed to national leadership at the policy and management level of government. It addresses the policies, institutional frameworks and relationships required,

[7] Overview of ITU-D Study Group 1, Question 22/1: Securing information and communication networks – Best practices for developing a culture of cybersecurity, available at: http://www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf.

[8] ITU National Cybersecurity/CIIP Self-Assessment Tool website at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

and seeks to produce a snapshot of the current state of national policy development, authorities, and relationships, as well as to identify the key institutions, players and actions required to address cybersecurity/CIIP.

Just as the interconnection of information infrastructures creates a weakest link problem in the global network, the elements of a national strategy are interlinked and require concerted effort from all national participants. Using this ITU National Cybersecurity Self-Assessment Tool will require input from various government ministries, agencies and persons responsible for and knowledgeable about the issues of cybersecurity/CIIP. The target ministries and agencies would include but not be limited to the agency or organization designated as the national lead, Ministries of Justice, Commerce, Trade, Defense, Intelligence, Telecommunications, ministries responsible for critical industries and infrastructures, and relevant computer incident response teams (CIRTs), computer security incident response teams (CSIRTs), and/or computer emergency response teams (CERTs). Using this tool will also require input from other government organizations with a significant role in the national effort, including state and local government, and input from other participants including industry and civil society.

The tool is divided into three parts. **Part One** looks at the case for national action and examines the participants who will be required to address the issues, their roles and the organizational structure needed to achieve the necessary cooperation. **Part Two** examines key elements that must be considered in addressing cybersecurity/CIIP and included in a statement of national strategy. **Part Three** is a review and reassessment of information developed in the previous parts with a view to drafting a national strategy for cybersecurity/CIIP. In each part, an "**Action Item**" follows a brief discussion of an issue. Users of the tool are invited to provide a response based on their own national experience and objectives to each point in the action item. The information thus developed in parts 1 and 2 will provide the basis for the development of the draft strategy statement of the action item in part 3.

PART 1: CYBERSECURITY/CIIP IN THE NATIONAL AGENDA

SECTION 1: A CASE FOR NATIONAL ACTION

Security literature and even the popular press regularly provide anecdotal evidence of the risks and consequences of our increasing dependence on ICTs. For most participants, these are stories of how problems of cybersecurity/CIIP have affected some other participant, often in some other country. Little is available in the way of definitive analysis of the magnitude, frequency and consequences of cyber incidents in any country. Moreover, because the roles of participants in cybersecurity/CIIP differ and overlap, no participant is likely to have a clear, full picture of the problem, how to address it, and what responsibilities each participant should shoulder.

Cybersecurity/CIIP is a shared responsibility of participants: the government, business, other organizations, and individual users who develop, own, provide, manage, service and use these information systems and networks. If the full range of security responsibilities is to be addressed, all participants must have a common understanding of the problem and each participant must have an appropriate understanding of its role in responding to the security challenge.

Raising awareness of the issues of cybersecurity/CIIP and coordinating action at the national level by and among all participants to prevent, prepare for, respond to, and recover from incidents is the responsibility of government. A coordinated national effort has proven valuable for effective national action and is an essential building block for regional and international cooperation. The preparation of a national strategy for

responding to cybersecurity/CIIP has proven an effective first step in addressing these security challenges. Such a strategy statement would make the case for coordinated national action, establish national objectives and identify actions to be taken to achieving those national objectives.

The case for national action is a function of the role of ICTs in the nation, the threats and vulnerabilities (risks) of ICT utilization to the nation, the place of cybersecurity/CIIP in overall national objectives, and the impact of ICTs on other national concerns. The national strategy should be promulgated at a sufficiently high level so as to command attention among all national participants. Of particular note is the need to promulgate the national strategy at a level to ensure cooperation and participation by competing, often stove piped, government ministries. The national strategy must also be relevant to all participants in their different roles. It must speak to political leaders to command their attention and action. It must address the concerns of industry that owns and operates much of the ICT and relevant critical information infrastructures and it must also speak to individual users and small businesses to ensure they will support the chosen national approach.

The national strategy statement can set the stage by providing information on the roll of ICTs in national life. Information, such as the level of ICT penetration and the types of commercial, industrial and governmental processes dependent on ICTs, provides evidence of the national dependence on ICTs. By highlighting the role of ICTs in the economy, national security, critical infrastructures and social interaction the national strategy addresses interest relevant to all participants and brings all participants to a common understanding of the importance to ICTs to the nation.

The risks to the nation that arise from the use of ICTs are the reason for the call to action. This portion of the statement should provide a realistic, but not alarmist, presentation of the security challenge faced by the nation and its ICT participants.

A national policy on cybersecurity/CIIP is but one of many policies confronting a government. Placing cybersecurity/CIIP effort into context with other national objectives and concerns is important to make it real and relevant. Government initiatives such as increasing ICT penetration, e-Government deployment, online tax filing, and putting national databases online, provide a context for action on cybersecurity/CIIP. Other national concerns such as the fight against organized crime and terrorism provide context for a statement of national policy on cybersecurity/CIIP.

A national policy on cybersecurity/CIIP should establish a set of goals and broadly identify how these goals will be implemented, including through collaboration with industry and other participants. It should establish timeframes to stimulate rapid action and metrics to provide benchmarks for progress. Additionally, it may place the national efforts in the context of other regional and international activities.

ACTION ITEM: Prepare a brief statement of each of these points:

1. The role of ICTs in the nation:
    a. In the economy
    b. In the national security
    c. In the critical infrastructures
    d. In the social interaction (civil society and social discourse)
2. Risks and ICTs in the nation:
    a. Identify threats from and vulnerabilities of ICT use
    b. Identify risks
        i. To the economy
        ii. To the national security
        iii. To the critical infrastructures
        iv. To the social interaction (civil society and social discourse)
3. The place of cybersecurity/CIIP in overall national objectives and concerns
4. Policy on cybersecurity/CIIP
    a. Goals
    b. How will it be implemented

c. Timeframes
d. Metrics
e. Relationship to regional and international activities

SECTION 2: PARTICIPANTS IN THE NATIONAL RESPONSE

Cybersecurity and CIIP are a shared responsibility of government, business, other organizations, and individual users who develop, own, provide, manage, service and use these information systems and networks (the participants). Each participant must be involved in cybersecurity/CIIP in a manner appropriate to its role. Yet, the roles and responsibilities are not only shared, in many cases they overlap. The challenge is to delineate and differentiate the roles and responsibilities of participants to ensure that all responsibilities are covered and that cooperative arrangements are in place to address shared responsibilities.

For some participants, for example individuals and small businesses, the role may be limited to managing their personal computer in a secure fashion. Yet these participants must be able to cooperate with other participants who can provide the necessary security solutions and procedures; and, these individual and small business participants need to be represented in the national cybersecurity/CIIP discussion through associations or groups that represent their class of participants. For other participants, such as operators of critical infrastructures, the role will be more involved and would include not only participation in general policy discussions but also direct cooperation with government authorities and participation in trust based forums with government and other key participants.

An important first step in developing a national response to cybersecurity/CIIP is to identify the key institutions and persons from government and from other participants and their roles and responsibilities for cybersecurity/CIIP. Government participants would include ministries and agencies with key roles in the development of policy and in operations related to cybersecurity/CIIP in the economy, national security, critical information infrastructure (CII) and social interaction. Other participants would include industry, civil society, academia and others. It would also

include key individual firms, critical sector groupings, relevant associations, and other key entities and groupings within the nation with a role in cybersecurity/CIIP.

The tradition of stove piped responsibilities within government, the rapid deployment of ICT infrastructures within the economy, and the widespread utilization of the Internet have highlighted the existence of overlapping roles and responsibilities within government for cybersecurity/CIIP. Thus, for each entity identified, it would be useful to identify their roles in cybersecurity/CIIP and to distinguish between their roles in policy discussions and policy formulation and their roles in carrying out cybersecurity/CIIP operations. Because of the importance of building trust among participants, the identification of a point of contact (with contact information) for each entity and for each significant role of that entity is a necessary step.

ACTION ITEM: Identify national participants in cybersecurity/CIIP:

1. **Government**: For each government ministry/agency with a role in cybersecurity/CIIP:
    a. Identify the ministry/agency.
    b. Describe its role(s) in the development of policy and in operations of cybersecurity/CIIP related to the economy, national security, CII and social interaction.
    c. Identify a point of contact for each entity and for each significant role.
2. **Other participants**: For each non-government participant with a role in cybersecurity/CIIP including industry, civil society, academia and others, identify key individual firms and institutions, critical sector groupings, associations, and other key entities and groupings within the nation with a role in cybersecurity/CIIP.
    a. Identify the participant.
    b. Describe its role(s) in the development of policy and in operations of cybersecurity/CIIP related to the economy, national security, CII and social interaction.
    c. Identify a point of contact for each entity and for each significant role.

SECTION 3: ORGANIZING FOR CYBERSECURITY/CIIP

Enhancing cybersecurity/CIIP will require government to lead a national effort involving all participants to review and develop policy related to cybersecurity/CIIP and to conduct ongoing operations to prevent, prepare for, respond to, and recover from incidents related to cybersecurity/CIIP. These efforts require the identification of a lead government agency (and a lead person), and the establishment of forums and mechanisms within which to develop policy and to facilitate the conduct cooperative operational efforts among key participants.

The identification of the lead government institution for a national cybersecurity/CIIP effort is dependent on local conditions. The approach taken could provide a lead institution for developing policy and a separate institution for the conduct of ongoing operations. Alternately, the same institution may be used for both functions.

The lead government institution will need to have a mechanism available for the development of policy that includes outreach to other national participants, as well as regional and international participants, for purposes of receiving input and advice on proposed policy actions. Available national policy development structures should be identified, reviewed for adequacy and modified as appropriate, or established.

The lead government institution for the conduct of operational efforts will likewise need mechanisms and structures to facilitate cooperation among participants. Recognizing that because of their roles some participants are uniquely placed to support national cybersecurity/CIIP operational efforts, the mechanisms and structures chosen should include opportunities for the development of trusted relationships among participants. Attention should also be paid to the need for operational forums among government entities since government agencies may have overlapping responsibilities and/or the

need share some of the same or similar types of information. However, not all entities will participate in all cooperative arrangements and no single arrangement is likely to serve all purposes. Operational forums and structures suitable to address the cybersecurity/CIIP challenge should be identified, reviewed for adequacy and modified as appropriate. Where none exists, they should be established.

ACTION ITEM: Policy and operational forum/structures.

1. Identify the government institution(s) designated to lead the national cybersecurity/CIIP effort for policy development and operations.
2. Policy development: Identify relevant forum/structure for use by the lead agency for the development of cybersecurity/CIIP policy.
    a. Name of forum/structure.
    b. Participants.
    c. Role and objective of forum/structure.
    d. How is input from other participants obtained and addressed?
    e. Evaluate forum/structure for adequacy and identify required modifications.
3. Operations: Identify relevant forum/structures available to enhance operational cybersecurity/CIIP. Include government and non-government forums and structures.
    a. Name of forum/structure.
    b. Who leads and convenes the forum/structure?
    c. Participants.
    d. Role and objective of forum/structure.
    e. Is forum/structure trusted? If yes, how is trust addressed?
    f. Evaluate forum/structures for adequacy and identify required modifications.

PART 2: KEY ELEMENTS TO BE ADDRESSED BY A NATIONAL CYBERSECURITY/CIIP STRATEGY

SECTION 4: GOVERNMENT-PRIVATE SECTOR COLLABORATION

Cybersecurity/CIIP is a shared responsibility that can best be accomplished through collaboration between government and the private sector, which owns and operates much of the infrastructure in many countries. Both the government and the private sector have an enduring interest in assuring the resilience of the infrastructure. Their collaboration is fundamental to enhancing cybersecurity/CIIP. Successful public-private partnerships and collaboration will be mutually beneficial, involve clearly delineated roles and responsibilities, and require the development of trust. The objectives of public-private collaboration are to develop relationships that work to effectively manage cyber risk and protect the CII. Achieving this objective for collaboration requires a mechanism and procedures for bringing a variety of industry perspectives, equities and knowledge together with those of government and other participants to reach consensus and move forward together to enhance cybersecurity/CIIP.

While the exact approach taken to achieve government/private sector collaboration will vary based on local conditions, several key factors for effective government/private sector collaboration can be identified. Private sector input must be obtained early in the process of developing a national approach to cybersecurity/CIIP. Collaboration early in the process, and throughout the development stages and implementation, helps to ensure a workable effective national cybersecurity/CIIP system. As owners and

operators of the relevant infrastructures, the private sector must support any national approach to cybersecurity/CIIP for it to be effective. Only by learning of the cybersecurity/CIIP challenges facing firms and industries of the private sector and addressing them as part of the national effort can a national strategy be developed and implemented effectively. Collaboration between government and the private sector will provide for private sector input on matters of policy as well as information sharing between government and the private sector in ongoing operational matters. To maximize effectiveness of government/private sector collaboration, trust among participants is essential to encourage information sharing. Trust addresses issues such as what information is to be shared, how it will be shared, how it will be used and how the information is linked to its source.

Collaboration among government/private sector participants is also essential in the response and recovery phases of an incident. Throughout the process of government/private sector collaboration, but especially during times of incident response and recovery, knowing whom to call is a must. Identifying points of contact addresses this issue and is made more effective by the use of periodic exercises that bring key players together and encourages cooperation and the development of trust.

Where firms and industries face common security challenges, collaboration amongst these firms and industries can be an effective tool. Because critical industries are interlinked and face the potential for cascading failures, collaboration across critical industry lines is also important. While cooperation within an industry sector or across industry sectors may not require government as a participant, some government involvement is usually required to address issues such as antitrust.

ACTION ITEM: Describe actions taken and requirements for future action to develop government/private sector collaboration that will;

1. Include private sector perspectives in all stages of the development and

implementation of cybersecurity/CIIP policy.

2. Establish cooperative arrangements between government and the private sector for information sharing and incident management.
3. Bring private sector groups and government together in trusted forums to address common cybersecurity/CIIP challenges.
4. Encourage cooperation among participants in each critical infrastructure to address common cybersecurity/CIIP interests.
    a. How is government involved in this collaboration?
5. Encourage cooperation among participants from interdependent critical infrastructures to address shared cybersecurity/CIIP interests.
    a. How is government involved in this collaboration?

SECTION 5: INCIDENT MANAGEMENT CAPABILITIES

It is an important role of government to identify and maintain an incident management capability to prevent, prepare for, respond to, and recover from cybersecurity/CIIP incidents. This national cybersecurity/CIIP function is a corollary of the role of government in preparing for and responding to natural and other disasters. The entity providing this incident management capability function may also be the government institution(s) designated to lead the national cybersecurity/CIIP effort identified in Section 3.

The development of an incident management capability is sometimes subsumed in efforts to establish a computer incident response team (CIRT)/computer security incident response team (CSIRT). However, while the incident management capability and the CIRT may be housed in the same government entity, there are different functions involved. CIRT functions are often technical in nature and may be provided to government by non-government entities. In contrast, the incident management capability is a government function responsible for coordinating national efforts related to cybersecurity/CIIP. The incident management capability would lead national efforts on collaboration related to cybersecurity/CIIP among government entities the private sector and all other participants. The incident management capability may obtain CIRT services from an in-house CIRT or from other CIRTs.

The goals of the incident management capability would include:

1. Develop and implement coordinated national cyberspace security response system to prevent, detect, deter, respond to, and recover from cybersecurity/CIIP incidents.

2. Establish a focal point for managing cyber incidents that brings together critical elements from government (including law enforcement) and

essential elements from industry to reduce both the risk and severity of incidents.

3. Ensure the availability of CIRT services.
4. Maintain watch, warning, and incident response information sharing mechanisms.
5. Ensure availability of tools and procedures for the protection of cyber resources of government entities.
6. Develop, test, and exercise cybersecurity/CIIP response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.
7. Develop an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity/CIIP. Only if participants have a common understanding of risks and risk management can the interconnected systems and networks be appropriately protected.
8. Assess and periodically reassess the state of cybersecurity/CIIP efforts and develop program priorities.
9. Identify training requirements and how to achieve them.
10. Ensure availability of adequate funding, human resources, and training for addressing the cybersecurity/CIIP challenge.

ACTION ITEM: Describe actions taken and requirements for future action in regard to the incident management capability function to prevent, prepare for, respond to, and recover from cybersecurity/CIIP incidents:

1. Identify agency to provide the incident management capability function for watch, warning, response and recovery.
2. Identify cooperating government agencies and points of contact for each.
3. Identify cooperating participants (industry, CII, and civil society partners) and points of contact for each.
4. Identify arrangements for cooperation and information sharing between the incident management capability and its cooperating partners.

5. Identify international cooperating partners, points of contact and arrangements for cooperation.
6. Ensure availability of CIRT services by:
    a. Identifying available and/or contracting with existing CIRTs.
    b. Establishing a CIRT with national responsibility.
7. Develop tools and procedures for the protection of the cyber resources of government entities.
8. Develop procedures and tools for the dissemination of incident management information.
9. Develop an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity/CIIP.
10. Assess and periodically reassess the current state of cybersecurity/CIIP efforts and develop program priorities.
11. How will incident management capability and cybersecurity/CIIP effort be funded and staffed?

SECTION 6: LEGAL INFRASTRUCTURE

Cybersecurity/CIIP requires the review, establishment and modernization of relevant legal infrastructures that support modern information and communication technologies. The primary of these is that related to cybercrime where criminal law, procedures and policy should be reviewed to ensure the capability exist to prevent, deter, respond to, and prosecute cybercrime. Because the CII is globally interconnected and cybercrime crosses national boundaries, every country needs laws that address cybercrime per se, the procedures for electronic investigations, and assistance to other countries. These laws must not only be enacted, they must be enforced. An effective cybercrime effort will require updating legal authorities, establishing dedicated cybercrime units, and training and outreach for all who have a role in deterring cybercrime, including the judiciary and the private sector.

Other legal infrastructures may also require review and updating. Examples of legal infrastructures that may need review and updating include those related to data protection, privacy, digital signatures, commercial law and encryption.

Considerable work has been done at regional and international levels related to these cybersecurity/CIIP legal infrastructures. Such regional and international work should be utilized in national review efforts in order to assist in developing international norms and thereby facilitating international and regional cooperation.[9] Among those recommended for consideration are the Budapest Convention on Cybercrime (2001), the UNCITRAL Model Laws on Electronic Commerce and on Electronic Signatures (2001) and the

[9] Some additional background information and reference material for Member States in this regard can be found in the ITU publication *Understanding Cybercrime: A Guide for Developing Countries*, 2009, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html; and the *ITU Toolkit for Cybercrime Legislation*, 2009, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), to name some examples.

ACTION ITEM: Describe actions taken and requirements for future action in regard to the review and update of the national legal infrastructure:

1. Cybercrime authorities and procedures.
    a. Review and update legal authorities.
    b. Establish or identify national cybercrime units.
    c. Participate in international efforts, such as the 24/7 Cybercrime Point of Contact Network.
    d. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.
2. Other legal infrastructures.
    a. Which ones have been addressed?
    b. Which ones require review?

SECTION 7: CULTURE OF CYBERSECURITY

The concept of a Culture of Cybersecurity refers to the necessity of all participants to review their approach to ICTs and make adjustments to help ensure cybersecurity/CIIP. This culture is referenced in UNGA Resolutions 57/239, Creation of a global culture of cybersecurity[10], and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures[11]. A national culture of cybersecurity 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, civil society and individuals.

Similarly, this culture calls for training of users of government and private systems, improvements in security, and efforts to address other significant issues including privacy, spam, and malware. Developing such a culture requires nations to adopt a multidisciplinary and multi-stakeholder approach to implement cybersecurity/CIIP. Awareness raising and education initiatives are very important to this effort, as are the sharing of best practices, collaboration among participants, the use of international standards and international and regional cooperation.

ACTION ITEM: Describe actions taken and requirements for future action to develop a national culture of cybersecurity: including, for example;

1. To implement a cybersecurity plan for government-operated systems.
2. To promote a comprehensive national awareness program so that all participants – businesses, the general workforce, and the general population – secure their own parts of cyberspace and participate effectively in a new culture of cybersecurity.

[10] UN Resolution 57/239: Creation of a Global Culture of Cybersecurity, 2002, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.
[11] UN Resolution 58/199: Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 2004, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

3. To support outreach with special attention to the needs of children and individual users.
4. To enhance Science and Technology (S&T) and Research and Development (R&D) activities.
5. To identify national cybersecurity/CIIP training requirements and how to achieve them.

PART 3: DRAFTING A NATIONAL CYBERSECURITY/CIIP STRATEGY

SECTION 8: THE NATIONAL STRATEGY FOR CYBERSECURITY/CIIP

For a nation seeking to manage the risks arising from ICT use, a first step is to promulgate a national cybersecurity/CIIP strategy. In general, a national cybersecurity/CIIP strategy: **(1)** recognizes the importance of CII to the nation; **(2)** identifies the risks associated with the CII (usually an all-hazards approach[12]); **(3)** establishes a cybersecurity/CIIP policy; and, **(4)** broadly identifies how that policy will be implemented, including through collaboration with the private sector.

Such a cybersecurity/CIIP national strategy amplifies and delineates roles and responsibilities, identifies priorities, and establishes timeframes and metrics for implementation. The national cybersecurity/CIIP strategy can also place national efforts into the context of other national efforts, as well as regional and international cybersecurity/CIIP activities. In order to be successful a cybersecurity/CIIP strategy will need to raise awareness of the issues among political leaders and key decision makers and ensure they understand the magnitude of the challenge and recognize that it may take a long period of time to fully implement the proposed strategy. Indeed, cybersecurity/CIIP is a process, not a destination. No country starts from zero, and no country has completed the process.

A national cybersecurity/CIIP strategy should not be comprised of immutable policies. Instead, the strategy should be flexible and able to respond to the

[12] An *all-hazards* or *multi-hazards* approach to risk management includes consideration of all potential natural and technological hazards; this includes natural and manmade (accidental or intentional) emergencies and disasters.

dynamic risk environment. The strategy should establish policy goals by which government agencies and non-government entities can work together to achieve the stated policy in the most efficient and effective manner.

The cybersecurity/CIIP strategy should be developed cooperatively through consultation with representatives of all relevant participant groups, including government agencies, industry, academia, and civil society. It should be adaptive and integrate state, local, and community-based approaches consistent on national needs and contexts. The cybersecurity/CIIP strategy should be promulgated at the national level preferably by the head of government.

The main elements and considerations of a national strategy have been addressed in the previous seven sections of this paper. The responses provided in the "**Action Item**" sections of these sections should provide the basic material from which a national strategy can be crafted. Any final national strategy would of course need to be reviewed to ensure it confirms to national considerations.

In completing the action item below, participants should note that continual review, reassessment and reprioritization are essential to any strategy. Risks are constantly changing and the cybersecurity/CIIP strategy will require constant review and reassessment, which should be built into the strategy statement.

ACTION ITEM: Review responses in Sections 1-7 and prepare statements that respond to the following points. When combined these statements should represent a draft national strategy on cybersecurity/CIIP for your country:

1. **From Section 1 (A Case for National Action):**
    a. Identify a national policy on cybersecurity/CIIP.
    b. Identify a case for national action on cybersecurity/CIIP.
2. **From Section 2 (Participants in the National Response):**
    a. Identify key government ministries and agencies with leadership responsibilities in cybersecurity/CIIP and describe their roles.

b. Identify key other participants with responsibilities in cybersecurity/CIIP and describe their role(s).

3. **From Section 3 (Organizing for Cybersecurity/CIIP):**
    a. Identify organizational structures to be used for the development of cybersecurity/CIIP policy.
        i. Describe the workings of these structures and the involvement of other participants.
    b. Identify organizational structures to be used for ongoing cybersecurity/CIIP operations.
        i. Describe the workings of these structures and the involvement of other participants.
4. **From Section 4 (Government-Private Sector Collaboration):**
    a. Identify objectives and structures for government/private sector collaboration.
    b. Identify objectives and structures for trusted government/private sector collaboration.
5. **From Section 5 (Incident Management Capabilities):**
    a. Identify location within government of the incident management capability function.
    b. Identify and prioritize objectives of the incident management capability function.
6. **From Section 6 (Legal Infrastructures):**
    a. Identify objectives for updating the legal infrastructure related to cybercrime.
    b. Identify objectives for updating other elements of the legal infrastructure.
7. **From Section 7 (Culture of Cybersecurity):**
    a. Identify and prioritize objectives for building a national culture of cybersecurity.
8. **Additional Requirements:**
    a. Identify how the national strategy will be finalized and promulgated.
    b. Review funding requirements and sources for each element of the national strategy.
    c. Identify implementation timeframes.
    d. Identify metrics and reassessment objectives.