SECRETARIA DE COMUNICACIONES

REPUBLICA ARGENTINA

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection

16-18 October 2007
Buenos Aires, Argentina

Draft Meeting Agenda

Description: At the start of the 21st century, modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected. However, this interconnectivity also creates interdependencies and risks that need to be managed at national, regional and international levels. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this necessitates cooperation and coordination with relevant partners. The formulation and implementation of a framework for cybersecurity and critical information infrastructure protection (CIIP) requires a comprehensive approach.

This workshop, one in a series of regional events jointly organised by the ITU Telecommunication Development Sector and ITU Telecommunication Standardization Sector, in collaboration with Secretaría de Comunicaciones, Argentina. The workshop aims to identify the main challenges faced by countries in the Americas region in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on technical standards and development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity.

TUESDAY 16 OCTOBER 2007	
08:00–09:00	**Meeting Registration**
09:00–09:30	**Meeting Opening and Welcome**
	Welcoming Address: Secretarío de Comunicaciones, Secretaría de Comunicaciones, Argentina ***Opening remarks:*** ITU-D Representative ***Opening remarks:*** ITU-T Representative
09:30–10:45	**Session 1: What is a Framework for Cybersecurity and Critical Information Infrastructure Protection?**
	Session Description: The necessity of building confidence and security in the use of ICTs, promoting cybersecurity and protecting critical infrastructures at national levels is generally acknowledged. As national public and private actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established cybersecurity/CIIP institutional framework structures while others have used a light-weight and non-institutional approach. This session will review different approaches to such frameworks and their often similar components in order to provide meeting participants with a broad overview of the issues and challenges involved.
10:45–11:00	**Coffee/Tea Break**

11:00–12:30	**Session 2: Development of a National Strategy**
	Session Description: Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks that can be adopted? This session seeks to explore in more detail various approaches, best practices, and identify key building blocks that could assist countries in the Americas region in establishing national strategies for cybersecurity and CIIP.
12:30–14:00	**Lunch**
14:00–15:30	**Session 3: Technical Standards for Cybersecurity**
	Session Description: Standards-development bodies are an important player in addressing security vulnerabilities in ICTs. This session presents some of the main activities of standards development organizations (SDOs), focusing on ITU-T and considering topics such as security architecture, cybersecurity, security management, identity management, security baseline for network operators, and the ICT Security Standards Roadmap initiated by ITU-T Study Group 17.
15:30–15:45	**Coffee/Tea Break**
15:45–17:00	**Round Table Information Exchanges on a Framework for Cybersecurity and Critical Information Infrastructure Protection, the Development of a National Strategy, and Technical Standards**
	• Moderator for Information Exchanges • Rapporteur for Information Exchange on Frameworks for Cybersecurity and CIIP • Rapporteur for Information Exchange on National Strategies • Rapporteur for Technical Standards
17:00–17:15	**Daily Wrap-Up and Announcements**
	Meeting moderator to provide wrap-up of discussions and announcements

WEDNESDAY 17 OCTOBER 2007	
09:00–10:15	**Session 4: Watch, Warning and Incident Response**
	Session Description: A key activity for addressing cybersecurity at the national level requires preparing for, detecting, managing, and responding to cyber incidents through establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. This session discusses best practices and related standards in the technical, managerial and financial aspects of establishing national or regional watch, warning, and incident response capabilities.
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 5: Countering Spam and Related Threats**
	Session Description: One of the more prominent risks to Internet security is spam, which has mutated from a general annoyance to a broader cybersecurity threat. Spam is now the primary mechanism for delivering viruses that can hijack millions of computers (through zombie botnets) or launching phishing attacks to capture private or corporate financial information. Phishing refers to spam sent with a fraudulent motive - for instance, to gather credit card or personal banking information. Spam also acts as a platform for many other types of scams. A number of counter-measures against spammers – technical, legal, financial, user training - can be used against spammers, but there is a general lack of overall coordination at the international level. This session

	looks at some of the standards, best practices and initiatives that have been launched to counter spam.
12:00–13:30	**Lunch**
13:30–15:00	**Session 6: Government/Industry/Standardization Development Organizations Collaboration**
	Session Description: Industry/government partnerships are founded upon three pillars of trust, mutual benefit, and a clear understanding of roles and responsibilities. A fundamental element of successful industry-government partnerships is trust which is necessary for establishing, developing and maintaining sharing relationships between the private sector and government. The success of industry-government partnerships is dependent on all participants deriving value from the particular partnership. By providing an understanding of each party's roles and responsibilities in cybersecurity and participating in reciprocal information sharing, industry-government partnerships can mitigate and reduce risk and implement a more comprehensive approach to cybersecurity. This session discusses industry/government partnerships and considers the specific example of how standards development organizations play an important role.
15:00–15:15	**Coffee/Tea Break**
15:15–17:00	**Round Table Information Exchanges on Watch, Warning and Incident Response, Countering Spam and Related Threats, and Government/ Industry/ SDO Collaboration**
	• Moderator for Information Exchanges • Rapporteur for Watch, Warning and Incident Response • Rapporteur for Countering Spam and Related Threats • Rapporteur for Government/ Industry/ SDO Collaboration
17:00–17:15	**Daily Wrap-Up and Announcements**
	Meeting moderator to provide wrap-up of discussions and announcements

THURSDAY 18 OCTOBER 2007	
09:00–11:00	**Session 7: Legal Foundation, Regulatory Development and Enforcement**
	Session Description: Appropriate legislation, international legal coordination and enforcement are all important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. This requires updating of criminal law, procedures and policy to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments in their penal codes, or are in the process of adopting amendments, in accordance with international conventions and recommendations. This session reviews some various national legal approaches and potential areas for international legal coordination and enforcement efforts.
11:00–11:15	**Coffee/Tea Break**
10:30–12:00	**Session 8: Promoting a Culture of Cybersecurity**
	Session Description: Considering that personal computers and mobile phones 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 maintain information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Governments can take a leadership role in promoting a culture of cybersecurity and in supporting the efforts of others. This session will explore the concept of promoting a culture of cybersecurity, offers examples of specific initiatives and elaborate on possible best practices.
12:00–13:30	**Lunch**
13:30–15:00	**Session 9: Regional and International Cooperation**
	Session Description: Regional and international cooperation is extremely important in fostering a

	culture of security, along with the role of regional fora to facilitate interactions and exchanges. This session will review some of the ongoing regional and international cooperation initiatives in order to encourage meeting participants to participate in further concrete actions that could be implemented in the Americas region and internationally.
15:00–15:15	**Coffee/Tea Break**
15:15–17:00	**Session 10: Wrap-Up, Recommendations and the Way Forward**
	Session Description: The final session of the meeting reports some of the main findings from the event, and aims to elaborate recommendations for future activities in order to enhance cybersecurity and increase protection of critical information infrastructures in the region.
17:00–17:15	**Meeting Closing**
	Closing remarks: Secretarío de Comunicaciones, Secretaría de Comunicaciones, Argentina ***Closing remarks:*** Representative from ITU-D to close the meeting