APPENDIX A

A COMPREHENSIVE INTER-AMERICAN CYBERSECURITY STRATEGY: A MULTIDIMENSIONAL AND MULTIDISCIPLINARY APPROACH TO CREATING A CULTURE OF CYBERSECURITY

INTRODUCTION

The Internet and related networks and technologies have become indispensable tools for OAS member states. The Internet has spurred tremendous growth in the global economy and prompted gains in efficiency, productivity, and creativity across the Hemisphere. Individuals, businesses, and governments increasingly use the information networks that comprise the Internet to, *inter alia*, conduct business; manage personal, industrial, and governmental activities; transmit communications; and perform research. Moreover, at the Third Summit of the Americas, held in Quebec City, Canada, in 2001, our leaders committed to further increasing connectivity in the Americas.

Unfortunately, the Internet has also spawned new threats that endanger the entire global community of Internet users. Information that transits the Internet can be misappropriated and manipulated to invade users' privacy and defraud businesses. The destruction of data that reside on computers linked by the Internet can stymie government functions and disrupt public telecommunications service and other critical infrastructures. Such threats to our citizens, economies, and essential services, such as electricity networks, airports, or water supplies, cannot be addressed by a single government or combated using a solitary discipline or practice.

As recognized by the General Assembly in resolution AG/RES. 1939 (XXXIII-O/03), "Development of an Inter-American Strategy to Combat Threats to Cybersecurity," a comprehensive strategy for protecting information infrastructures that adopts an integral, international, and multidisciplinary approach is needed. The OAS is committed to the development and implementation of such a cybersecurity strategy and, in furtherance of this, held a Conference on Cybersecurity (Buenos Aires, Argentina, July 28-29, 2003) that demonstrated the gravity of cybersecurity threats to the security of critical information systems, critical infrastructures, and economies throughout the world, and underscored that effective action to deal with this issue must involve intersectoral cooperation and coordination among a broad range of governmental and nongovernmental entities.[1/]

Similarly, at the Special Conference on Security (Mexico City, Mexico, October 28-29, 2003) the member states considered the cybersecurity issue and agreed as follows:

> "*We will develop* a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyberattacks, whatever their origin, fighting against cyber threats and cybercrime, criminalizing attacks against cyberspace, protecting critical infrastructure and securing networked systems. We reaffirm our commitment to develop and implement an integral OAS cybersecurity strategy, utilizing the contributions and recommendations developed jointly by member state experts and the REMJA Governmental Experts Group on Cybercrime, CICTE, the Inter-American Telecommunication Commission (CITEL), and other appropriate organs,

---

[1]. Report on the Conference on Cybersecurity, document OEA/Ser.L/X.5, CICTE/CS/doc.2/03.

taking into consideration the existing work developed by member states, coordinated with the Committee on Hemispheric Security."[2/]

The states of the Hemisphere meeting at the Fourth Regular Session of the Inter-American Committee against Terrorism (CICTE) (Montevideo, Uruguay, January 28-30, 2004), once again declared their commitment to fight terrorism, including threats to cybersecurity, which they identified as one of the emerging terrorist threats[3/] and considered the document "Framework for Establishing an Inter-American CSIRT Watch and Warning Network."[4/] On that occasion, CICTE also decided to hold in Ottawa, Canada, in March 2004, a meeting of government experts or practitioners to consider that framework document and to produce recommendations as CICTE's contribution to the Comprehensive Inter-American Cybersecurity Strategy.

The Comprehensive Inter-American Cybersecurity Strategy pools the efforts and expertise of CICTE, CITEL, and REMJA. The Strategy recognizes the necessity for all participants in networks and information systems to become aware of their roles and responsibilities in regard to security in order to build a culture of cybersecurity.

The Strategy further recognizes that an effective framework for protecting the networks and information systems that constitute the Internet, and for responding to and recovering from incidents, is dependent in equal measure upon:

- Furnishing users and operators of the Internet with information to help them secure their computers and networks against threats and vulnerabilities, and respond to and recover from incidents;

- Fostering public-private partnerships with the goal of increasing education and awareness and working with the private sector–which owns and operates most of the information infrastructures on which nations depend–to secure those infrastructures;

- Identifying, evaluating, and stimulating the adoption of technical standards and best practices that ensure the security of information transmitted over the Internet and other communication networks; and

- Fostering the adoption of cyber-crime policies and legislation that will protect Internet users and prevent and deter criminal misuse of computers and computer networks, while respecting the privacy and individual rights of Internet users.

The member states of the OAS are committed, within the framework of this Comprehensive Inter-American Cybersecurity Strategy, to fostering a culture of cybersecurity that deters misuse of the Internet and related information systems and encourages the development of trustworthy and reliable information networks. This commitment will be effectuated through actions of the member states and the initiatives that will be undertaken by CICTE, CITEL, and REMJA's Group of Governmental Experts on Cyber-crime described below.

---

2. Declaration on Security in the Americas, document CES/DEC. 1/04 rev. 1.
3. Declaration of Montevideo, OEA/Ser.L/X.2.4, CICTE/DEC. 1/04 rev. 3.
4. Appendix V, document OEA/Ser.L/X.2.4, CICTE/INF.4/04.

CICTE: The Formation of an Inter-American Alert, Watch, and Warning Network to Rapidly Disseminate Cybersecurity Information and Respond to Crises, Incidents, and Threats to Computer Security

Because of the rapidly evolving nature of technology, the daily discovery of new vulnerabilities in software and hardware, and the increasing number of security incidents, cybersecurity is impossible without a constant, reliable supply of information about threats, vulnerabilities, and how to respond to and recover from incidents. Therefore, in support of the Comprehensive Inter-American Cybersecurity Strategy, CICTE will develop plans for the creation of a hemisphere-wide 24-hour per day, seven-day per week network and Computer Security Incident Response Teams (CSIRTs) capable of and charged with appropriately and rapidly disseminating cybersecurity information and providing technical guidance and support in the event of a cyber incident. These teams could begin simply as official points of contact located in each state and charged with receiving computer security information to be transformed into CSIRTs in the future.

The essential characteristics of the effort to create this hemispheric network are summarized below and fully described in the document "Recommendations of the CICTE Cybersecurity Practitioners' Workshop on the OAS Integral Cybersecurity Strategy: Framework for Establishing the Inter-American CSIRT Watch and Warning Network" (CICTE/REGVAC/doc.2/04). CICTE shall, along with the member states, create this hemispheric network using the Plan of Action provided in that document (CICTE/REGVAC/doc.2/04, Section IV).

Principles

The CSIRTs that will participate in CICTE's initiative will share common principles. They will be:

- Indigenous – The hemispheric network should be operated and controlled by national points of contact in each participating nation appointed by the governments.

- Systemic – The hemispheric network requires a trained workforce, regular information sharing regarding threats and vulnerabilities, constant reevaluation, the implementation of best practices, and appropriate interaction with policymakers.

- Ongoing – Due to the daily evolution of the Internet, the program must be regularly updated and maintained and the staff trained on a periodic basis.

- Accountable – Rules with respect to issues such as the handling of information must be understood and adhered to or users will lose confidence and efforts to make the system more secure will be undermined.

- Built upon existing arrangements – There are a number of preexisting entities in the Hemisphere that provide cybersecurity services to a greater or lesser extent. Any new system must build upon these preexisting institutions to avoid duplication and encourage active participation.

Building the Hemispheric Network

The creation of the hemispheric network of CSIRTs will require a series of progressive steps that will depend upon the active participation of the member states:

- Identification of Existing CSIRT Organizations – A survey of CSIRTs must be conducted within the Hemisphere to identify gaps in the coverage of CSIRTs that currently exist in the Hemisphere and to prevent redundant efforts.

- Establishment of a Service Model – National CSIRTs should be so designated by their respective governments and certified and accredited in accordance with international norms in the computer security community. They should also establish a minimum set of standards for cooperation and information-sharing among CSIRTs, as enumerated in CICTE/REGVAC/doc.2/04.

- Addressing Trust Issues – Since much of the information that CSIRTs need to exchange is proprietary or otherwise sensitive, trust must be developed among the participants as an essential element of the hemispheric network. To build such trusted relationships, CSIRTs should be created to possess the attributes and capabilities identified in CICTE/REGVAC/doc.2/04, which include a secure infrastructure for managing sensitive information; the ability to communicate securely with stakeholders; and procedures to guard against inappropriate disclosure of information. Member states will always maintain the right to decide on the type of information that will be exchanged through their designated CSIRTs.

- Building Public Awareness – National CSIRTs should ensure the public knows how to report a cyber incident and to whom.

- Extending the Network – Member states will consider, when appropriate, extending the capability of the hemispheric network, with a view to assisting states that so request in the development of specific plans, obtaining funding, and developing capacity-building projects.

- Maintaining the Network – The Group of Government Cybersecurity Practitioners would meet periodically as necessary and as convened by CICTE, within available resources.

CITEL: The Identification and Adoption of Technical Standards for a Secure Internet Architecture

The IV Meeting of Permanent Consultative Committee I: Telecommunication Standardization, held in Quito, Ecuador, from March 16 to 19, 2004, adopted the attached resolution, CCP.I/RES.49 (IV-04), [5/] "Cybersecurity," after conducting a joint workshop with the International Telecommunication Union (ITU) that addressed key issues of cybersecurity as related to CITEL. The said resolution, which encompasses the contribution of CITEL to the Comprehensive Inter-American Cybersecurity Strategy, provides guidance for the future work to be developed by CITEL in that area.

---

[5]. Appendix II.

An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry. Both the telecommunications and information technology industries and the governments of OAS member states are seeking cost-effective comprehensive cybersecurity solutions. Security capabilities in computer products are crucial to the overall network security. However, as more technologies are produced and integrated into existing networks, their compatibility and interoperability--or the lack thereof--will determine their effectiveness. Security must be developed in a manner that promotes the integration of acceptable security capabilities into the overall network architecture. To achieve such integrated, technology-based cybersecurity solutions, network security should be designed around international standards developed in an open process.

The development of standards for Internet security architecture will require a multi-step process to ensure that adequate agreement, planning, and acceptance are achieved among the various governmental and private entities that must play a role in the promulgation of such standards. Drawing upon the work of such standards development organizations as the Standardization Sector of the International Telecommunication Union (ITU-T), CITEL is identifying and evaluating technical standards to recommend their applicability to the Americas region, bearing in mind that the development of networks in some of the OAS member states has suffered some delays, which implies that for those countries, the achievement of a certain degree of quality for their networks will be important to fully realize adequately secure information exchange systems. CITEL is also establishing liaisons with other standards bodies and industry forums to obtain the participation and feedback of those parties.

The identification of cybersecurity standards will also be a multi-step process. Once CITEL's evaluation of existing technical standards is completed, it will recommend the adoption of standards of particular importance to the region. It will also, on a timely and ongoing basis, identify obstacles to the implementation of those security standards in the networks of the region, and possible appropriate action that may be considered by member states.

The development of technical standards is not a “one-size-fits-all” endeavor. CITEL will evaluate regional approaches to network security, deployment strategies, information exchange, and outreach to the public and the private sector. As part of this effort, CITEL will identify resources for best practices for network communication and technology-based infrastructure protection. This process will require that CITEL review the objectives, scope, expertise, technical frameworks, and guidelines associated with available resources, in order to determine their applicability within the Americas region to determine which ones are most appropriate. CITEL will continue to work with member states to assist them in the most appropriate and effective implementation.

CITEL’s contribution to the Comprehensive Inter-American Cybersecurity Strategy will take a prospective approach and seek to foster information-sharing among member states to promote secure networks. It will identify and evaluate technical issues relating to standards required for the security of future communications networks across the region, as well as existing ones. This task will draw primarily on the work of ITU-T. Through CITEL, other existing standards-setting bodies will also be considered, as appropriate. Ultimately, CITEL will highlight security standards of particular importance and recommend that member states endorse those standards. It is also important to highlight the crucial role of CITEL in promoting capacity-building and training programs so as to advance the process of spreading technical and practical information related to cybersecurity issues.

CITEL recognizes that, although the first priority must focus on public policies which will bring the benefits of telecommunications and information technologies to all citizens of the OAS member states, strengthening the private-public partnership that will result in the wide-scale adoption of a framework of technical standards that help secure the Internet, will require communication and cooperation among and within the communities that are stakeholders in this partnership. CITEL will foster cooperation among member states on aspects related to network security by helping administrations adopt policies and practices that encourage network and service providers to implement technical standards for secure networks. The new edition of *The Blue Book: Telecommunication Policies for the Americas*, a joint publication of CITEL and ITU, will include a chapter on cybersecurity. CITEL will also foster dialogue within the relevant technical and governmental communities regarding work on network security and cybersecurity through joint seminars with the ITU on security standards. The actions of CITEL may also include matters relating to telecommunications policies, practices, regulations, economic aspects, and the responsibilities of users, all within the legal framework within which the telecommunications service operates, and within the duties and responsibilities of CITEL.

REMJA: Ensuring That OAS Member States Have the Legal Tools Necessary to Protect Internet Users and Information Networks

Criminals such as "hackers," organized crime groups, and terrorists are increasingly exploiting the Internet for illicit purposes and engineering new methods of using the Internet to commit and facilitate crime. These illegal activities, commonly referred to as "cyber-crimes," hinder the growth and development of the Internet by fostering the fear that the Internet is neither a secure nor a trustworthy medium for conducting personal, government, or business transactions. Accordingly, REMJA's contribution to the Comprehensive Inter-American Cybersecurity Strategy, through the initiatives of the Group of Governmental Experts on Cyber-crime (the Experts Group), will focus upon assisting member states to combat cyber-crime by ensuring that law enforcement and judicial officials have the legal tools necessary to investigate and prosecute such offenses. This decision was adopted by REMJA at its meeting held from April 28 to 30, 2004, in Washington D.C.[6/]

Drafting and Enacting Effective Cybercrime Legislation and Improving International Handling of Cybercrime Matters

Without appropriate laws and regulations, member states are unable to protect their citizens from cyber-crime. Furthermore, member states lacking adequate cyber-crime laws and mechanisms for international cooperation run the risk of becoming safe havens for criminals who commit such offenses. Consequently, the Experts Group will provide technical assistance to member states in drafting and enacting laws that punish cyber-crime, protect information systems, and prevent the use of computers to facilitate illegal activity. The Experts Group will also promote legal mechanisms that encourage cooperation in cyber-crime matters among investigators and law enforcement authorities who investigate and prosecute cyber-crime. These efforts in support of the Comprehensive Inter-American Cybersecurity Strategy will be undertaken within the framework of the recommendations of the Experts Group (Third Meeting of the Group of Governmental Experts on Cyber-Crime, OEA/Ser.K/XXXIV, CIBER-III/doc.4/03).[7/]

---

6. Appendix IV, document OEA/Ser.K/XXXIV.5, REMJA-V/doc.7/04 rev. 4.
7. Appendix III.

In pursuing this initiative, the Experts Group will create training materials, provide technical assistance, and conduct regional workshops to assist in the development of government policies and legislation that will help engender trust and confidence in information systems and the Internet by criminalizing misuse of computers and computer networks. The Experts Group's collaborative training for member states will focus on the modernization of laws and regulations to respond to the challenge of combating cyber-crime. A major objective of these technical training sessions will be to outline the criminal laws and privacy protections necessary to help secure information systems and foster confidence among users of those systems. Specifically, the workshops will focus on the enactment of the following categories of legislation:

- Substantive Computer Crime Laws - Every member state should develop criminal and legal prohibitions against attacks on the confidentiality, integrity, and security of computer systems. Conduct, such as accessing computers without authorization, illegal interception of data, interference with the availability of computer systems, and theft and sabotage of data, should be deemed illegal under the law of each member state.

- Procedural Laws for Gathering Electronic Evidence - Each nation must also have clear procedures meeting international standards for government access to communications and stored data when needed for the investigation of crimes. Equally important, businesses and consumers must be assured that the government will not unjustifiably monitor their communications, and consumers must be sure that the data they provide to merchants will not be misused.

The workshops will focus on the need to draft such laws in a manner that is "technology neutral" (i.e., such laws should address types of crime or types of behavior rather than being drafted only to address a particular type of technology) to prevent newly enacted laws from quickly becoming outdated or irrelevant.

The borderless nature of global networks means that a single criminal act involving a computer may affect or target computers in multiple countries. During its regional workshops, the Experts Group will also provide training on how to respond to such challenges in international cooperation and facilitate the exchange of investigative information in cyber-crime cases. Additional emphasis will be placed upon building relationships among the cyber-crime experts within the Hemisphere to facilitate international cooperation and provide ready access to expertise and resources within the region for battling cyber-crime.

Following the workshops, the Experts Group will further assist member states by providing legal consultation to support government ministries and legislatures in drafting legislation, regulations, and policies. Expert assistance on a bilateral basis may be required to support governments in the preparation of legislation and policies embodying the core concepts of cyber-crime laws, investigative authorities, and privacy.

CONCLUSIONS AND FOLLOW-UP TO THE STRATEGY

The initiatives of CICTE, CITEL, and REMJA described above each represent a pillar of this Comprehensive Inter-American Cybersecurity Strategy. Together, the concerted multidisciplinary

efforts of these bodies will support the growth, development, and protection of the Internet and related information systems and protect users of those information networks. These efforts may evolve over time, requiring new approaches, but their objective will remain the same: creating and supporting a culture of cybersecurity.

Considering that the Strategy is dynamic, periodic review must be undertaken to ensure its continued applicability and effectiveness. This can be achieved through the following actions:

1. Ongoing coordination and cooperation among the secretariats of CICTE, CITEL, and the REMJA Group of Governmental Experts on Cyber-crime.

2. Strengthening coordination among the national authorities and entities, including the national CSIRTs, involved in addressing cybersecurity issues.

3. Establishment of a joint Web site on which pertinent cybersecurity information generated by CICTE, CITEL, and the REMJA Group of Governmental Experts on Cyber-crime can be posted, in order to allow for a cross-fertilization of ideas and to facilitate the exchange of information.

4. The member states and their national CSIRTs should undertake, with CICTE, CITEL, and the REMJA Group of Governmental Experts on Cyber-crime, an inter-American public awareness program regarding cybersecurity and cyber-ethics that emphasizes: the benefits and responsibilities of using information networks; safety and security best practices; the potential negative consequences resulting from the misuse of networks; how to report a cyber incident and to whom; and technical and practical information related to cybersecurity.

5. Periodic review of the cybersecurity initiatives and programs of CICTE, CITEL, and the REMJA Group of Governmental Experts on Cyber-crime, and on the implementation of the Strategy, to be conducted by these three bodies, with a joint progress report to the General Assembly.