AG/RES. 2004 (XXXIV-O/04)

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

(Adopted at the fourth plenary session held on June 8, 2004)

THE GENERAL ASSEMBLY,

HAVING SEEN the Annual Report of the Permanent Council to the General Assembly in particular the section on the matters entrusted to the Committee on Hemispheric Security, and specifically the recommendations on a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity;

RECALLING its resolution AG/RES. 1939 (XXXIII-O/03) "Development of an Inter-American Strategy to Combat Threats to Cybersecurity";

BEARING IN MIND that the Inter-American Committee against Terrorism (CICTE), at its fourth regular session, held in Montevideo, Uruguay, January 28-30, 2004, adopted the Declaration of Montevideo (CICTE/DEC. 1/04 rev. 3) in which it declared its commitment to identifying and fighting emerging terrorist threats, regardless of their origins or motivation, such as threats to cybersecurity;

NOTING WITH SATISFACTION:

That the OAS Conference on Cybersecurity, held in Buenos Aires, Argentina from July 28 to 29, 2003, in compliance with the abovementioned resolution AG/RES. 1939 (XXXIII-O/03), which demonstrated the gravity of cybersecurity threats to the security of critical information systems, critical information structures and economies throughout the world, and underscored that effective action to deal with this issue must involve inter-sectoral cooperation and coordination among a broad range of governmental and non-governmental entities;

That CICTE, at its Fourth Regular Session, held in Montevideo, Uruguay, from January 28 to 30, 2004, considered the document "Framework for Establishng an Inter-American CSIRT Watch and Warning Network" (CICTE/INF.4/04) and decided to hold a meeting of government cybersecurity experts, in March 2004 in Ottawa, Canada, to prepare its recommendations for the draft Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity, in compliance with the abovementioned resolution AG/RES. 1939 (XXXIII-O/03); and

The recommendations formulated by CICTE (CICTE/REGVAC/doc.2/04), CITEL (CPP.I-TEL/doc.427/04 rev. 2) and the Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) and its Group of Government Experts in Cybercrime (CIBER-III/doc.4/03) ;

WELCOMING the Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, recommended to this General Assembly by the Permanent Council as the joint effort of member states and their experts with the technical expertise of the CICTE, CITEL and REMJA Group of Government Experts in Cybercrime (CP/doc…/04);

RECOGNIZING:

The urgency of increasing the security of information networks and systems commonly referred to as the Internet, in order to address vulnerabilities and protect users, national security and critical infrastructures from the serious and damaging threats posed by those who would carry out attacks in cyberspace for malicious or criminal purposes;

The need to create an inter-American alert, watch and warning network to rapidly disseminate cybersecurity information and to respond to and recover from crises, incidents and threats to computer security;

The need to develop trustworthy and reliable Internet information networks and systems thereby enhancing user confidence in such networks and systems;

REITERATING the importance of developing a comprehensive strategy for protecting information infrastructures that adopts an integral, international, and multi-disciplinary approach; and

CONSIDERING:

The United Nations General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies; resolution 57/239 concerning the creation of a global culture of cybersecurity ; and resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information systems; and

That at its XII Meeting, the Permanent Executive Committee of the Inter-American Telecommunications Commission (COM/CITEL) pointed out that “building a culture of cyber security to protect telecommunication infrastructures by raising awareness among all participants in the Americas in information systems and networks concerning the risk to those systems and by developing necessary measures to address security risks to respond quickly to cyber incidents” is within CITEL’s mandates,

RESOLVES:

1. To adopt the Comprehensive Inter-American Cybersecurity Strategy, attached hereto as Appendix A.

2. To urge member states to implement the said Strategy.

3. To urge member states to establish or identify national "alert, watch, and warning" groups, also known as "Computer Security Incident Response Teams" (CSIRTs).

4. To place renewed emphasis on the importance of achieving secure Internet information systems throughout the Hemisphere.

5. To request that the Permanent Council, through the Committee on Hemispheric Security, continue to address this issue and continue to facilitate the coordination efforts to implement the said Strategy, in particular the efforts of government experts, the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), the Group of Government Experts on Cybercrime of the Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA), and other appropriate organs of the OAS.

6. To urge Member States and the organs, agencies and entities of the OAS to coordinate their efforts to enhance cybersecurity.

7. To request that the Secretariats of CICTE and CITEL, and the Group of Government Experts on Cybercrime of REMJA assist member states, when so requested, in the implementation of the respective portions of the said Strategy, and to submit a joint report to the Permanent Council, through the Committee on Hemispheric Security, on their compliance with this resolution, prior to the thirty-fifth regular session of the General Assembly.

8. To support the holding of a second Meeting of Government Cybersecurity Practitioners to be convened by CICTE for appropriate follow-up on the recommendations on the Establishment of the Inter-American Alert, Watch and Warning Network, contained in the document CICTE/REGVAC/doc.2/04, and which form part of the said Strategy.

9. To stipulate that the abovementioned Meeting of Government Cybersecurity Practitioners be held within the resources allocated in the Program-Budget of the Organization and other resources, and to request that the General Secretariat and the CICTE Secretariat provide the necessary administrative and technical support for this Meeting.

10. To urge member states to implement, as appropriate, the recommendations of the Initial Meeting of the Group of Government Experts in Cybercrime of REMJA (document REMJA-V/doc.5/04) and the recommendations regarding cybercrime of the Fifth

Meeting of REMJA (document REMJA-V/doc.7/04 rev. 4) as a means of creating a framework for enacting laws that protect information systems, prevent the use of computers to facilitate illegal activity, and punish cybercrime.

11. To request the Permanent Council to report to the General Assembly at its thirty-fifth regular session on the implementation of this resolution.

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 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 multi-disciplinary 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 that effective action to deal with this issue must involve inter-sectoral cooperation and coordination among a broad range of governmental and non-governmental 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:

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

> "*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, 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 this 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 the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), and the Meeting of Justice Ministers or Ministers or Attorneys General of the Americas (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 toward 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.

---

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.

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 cybercrime 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 Government Experts on Cybercrime described below.

CICTE: The Formation of an Inter-American Alert, Watch, and Warning Network to Rapidly Disseminate Cyber Security 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 and security of 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).[5/] 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, pp. 4-6).

Principles

5. Appendix I.

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 re-evaluation, the implementation of best practices and appropriate interaction with policy-makers.

- Ongoing – Due to the daily evolution of the Internet, the program must regularly be 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 pre-existing entities in the hemisphere that provide cyber-security services to a greater or lesser extent. Any new system must build upon these pre-existing 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 in 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 the Permanent Consultative Committee I: Telecommunication Standardization held in Quito, Ecuador, from 16-19 March 2004 adopted the attached Resolution CCP.I/RES.49 (IV-04)[6/] "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, is replicated below and provides guidance for the future work to be developed by CITEL in that area.

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 is 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

6. Appendix II.

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 fora to obtain the participation and feedback of those parties.

The identification of cybersecurity standards will 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 for 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 – "Telecommunications 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 "cybercrimes," hinder the growth and development of the Internet by fostering the fear that the Internet is neither a secure nor 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 Government Experts on Cybercrime (the Experts Group), will focus upon assisting Member States to combat cybercrime by ensuring that law enforcement and judicial officials have the legal tools necessary to investigate and prosecute such offenses. This decision was adopted by the REMJA at its meeting held April 28-30, 2004 in Washington D.C., United States.[7/]

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 cybercrime. Furthermore, Member States lacking adequate cybercrime 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 cybercrime, 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 cybercrime matters among investigators and law enforcement authorities who investigate and prosecute cybercrime. 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 Group of Governmental Experts on Cyber-Crime, OEA/Ser.K/XXXIV, CIBER-III/doc.4/03).[8/]

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 cybercrime. 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:

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

- 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 cybercrime cases. Additional emphasis will be placed upon building relationships among the cybercrime experts within the Hemisphere to facilitate international cooperation and provide ready access to expertise and resources within the region for battling cybercrime.

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 cybercrime 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 Government Experts in Cybercrime.

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

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

4. The Member States and their national CSIRTs should undertake, with CICTE, CITEL and the REMJA Group of Government Experts in Cybercrime, 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 Government Experts in Cybercrime, and on the implementation of the Strategy, to be conducted by these three bodies, with a joint progress report to the General Assembly.

APPENDIX I

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

CYBERSECURITY PRACTITIONERS' WORKSHOP
March 29-30, 2004
Ottawa, Canada

OEA/Ser.L/X.5
CICTE/REGVAC/doc.2/04
8 April 2004
Original: English

RECOMMENDATIONS OF THE CICTE CYBERSECURITY PRACTITIONERS'WORKSHOP ON THE OAS INTEGRAL CYBERSECURITY STRATEGY: FRAMEWORK FOR ESTABLISHING THE INTER-AMERICAN CSIRT WATCH AND WARNING NETWORK

RECOMMENDATIONS OF THE CICTE CYBERSECURITY PRACTITIONERS' WORKSHOP ON THE OAS INTEGRAL CYBERSECURITY STRATEGY: FRAMEWORK FOR ESTABLISHING THE INTER-AMERICAN CSIRT WATCH AND WARNING NETWORK

I. OBJECTIVE

To create a hemisphere-wide network that will operate 24 hours a day, 7 days a week, to be made up of national contact points among *Computer Security Incident Response Teams* (CSIRTs) in Member States of the OAS, with a mandate and the capacity to respond rapidly and in an appropriate manner to crises, incidents and threats to computer security.

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.

Since intruders now have more sophisticated means to launch highly automated attacks that spread rapidly over the Internet, while at the same time employing methods intended to disguise and make it difficult to understand or trace the origin of such attacks, worldwide cooperation and ability of teams to respond in real time is of growing importance. Such cooperation must make it possible to:

1. Establish CSIRTs in each of the Member States;
2. Strengthen the hemisphere's CSIRTs;
3. Identify national points of contact in each State;
4. Identify those services deemed most critical;
5. Quickly detect and diagnose problems;
6. Establish protocols and procedures for the exchange of information;
7. Rapidly disseminate notice of such attacks throughout the region;
8. Provide rapid regional notice of general vulnerabilities in the system;
9. Provide regional warning of suspicious activities, and develop the cooperation needed for analysis and diagnosis of such activities;
10. Provide information on measures for remedying or mitigating attacks and threats;
11. Reduce the amount of duplication in the analysis carried out by each team;
12. Strengthen technical cooperation and training in computer security aimed at establishing national CSIRTs;
13. Make use of existing subregional mechanisms.

This cooperation will reinforce existing technical expertise among the teams so that they can better limit the damage and ensure the continuing operation of critical services.

II. PRINCIPLES

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

2. Systemic – The hemispheric network must be a multi-faceted operation requiring an aware and trained workforce, regular sharing of information regarding current threats and vulnerabilities, constant re-evaluating and implementing of best practices and appropriate interaction with public policy makers.

3. On-going – due to the inherent daily evolution of the Internet, any successful program must regularly be updated and maintained, and the staff trained on a periodic basis. Internet security will not be achieved with a one-time fix.

4. Accountable – The "security" in "cyber security". Established rules with respect to issues such as the handling and provision of information must be understood and adhered to, or users will lose confidence and efforts to make the system more secure will be undermined and become counter-productive.

5. Built upon existing arrangements – There are a number of pre-existing entities in the hemisphere, including CSIRTs, consulting companies, and contact networks, among others, that provide cyber-security services to a greater or lesser extent. Any new system should build upon these pre-existing institutions and the trust relationships that have already been established intra- and inter-regionally, to avoid duplication and encourage active participation.

III. IDENTIFICATION OF EXISTING ORGANIZATIONS, ESTABLISHING A SERVICE MODEL, TRUST ISSUES, FINANCING, PUBLIC AWARENESS, AND EXTENDING THE NETWORK

1. Identification of Existing Organizations

There are well over a hundred organizations that use the name CERT (Computer Emergency Response Team), or CSIRT (the generic term of equivalent meaning), world-wide. The Forum of Incident Response and Security Teams (FIRST), a world-wide, voluntary association of CSIRTs, lists 80 members within the OAS Member States, however the vast majority of these currently exist in one member state only. Given the information gaps, conducting a CSIRT census is the essential first step towards developing a cyber-security network.

2. Establishing a Service Model

While there are no international standards agreed upon for what constitutes a CSIRT, there are a number of documents and efforts that can assist the process of defining a CSIRT team and on certification and accreditation of CSIRTs.

The CERT/CC has published a variety of documents that can assist in the creation of a CSIRT, including:

- *Handbook for Computer Security Incident Response Teams (CSIRTs)* provides updated guidance on generic issues to consider when forming a CSIRT;
- *State of the Practice of Computer Security Incident Response Teams*. This report includes information collected through a pilot survey of computer security incident response teams (CSIRTs), CERT/CC's own experience, discussions with and observations of other CSIRTs, and research and reviews of the current literature on incident response; and
- *Creating a Computer Security Incident Response Team: A Process for Getting Started* is a document that describes the basic requirements for creating a CSIRT.

There should be certification and accreditation of national CSIRTs. Member states should consider whether affiliation of their national CSIRTs with FIRST would satisfy the certification and accreditation requirements.

In establishing a regional network of cooperating National CSIRTs, a minimum set of standards for cooperation and information-sharing among the CSIRTs would be expected. These would include:

i. Designation of the national CSIRT by the respective government;

ii. Agreement on principles of information sharing among the cooperating teams;

iii. Responsibility for receiving information from other national CSIRTs and disseminating that information to appropriate entities within the country;

iv. Participation in information-sharing among the other national CSIRTs in the hemispheric network;

v. Authorization to disseminate information to other national CSIRTs; and

vi. Provision of assistance to other national CSIRTs for incidents and threats.

3. Trust Issues

Much of the information which CSIRTs need to exchange is proprietary or otherwise sensitive and there are few good models that promote the consistent sharing of information among CSIRTs. Trust –the essential ingredient in information sharing– when it exists, has developed in practice among individuals who know and have worked with each other, rather than institutionally, among organizations. To establish trust, clear expectations on how information exchanged will be used or disseminated must be understood and followed by all parties. Rules on information-sharing, stating how information can be used or disseminated, must be agreed to among all of the cooperating national CSIRTs.

Some of the CSIRT attributes that are required to promote trust in communication and cooperation about sensitive security issues include:

i. a secure infrastructure for managing sensitive information;

ii. the ability to communicate securely with stakeholders;
iii. the ability to marshal experts and decision-makers;

iv. an infrastructure to support advance notification to select audiences;

v. procedures to guard against information leakage;

vi. a well-known public interface for dissemination of critical information; and

vii. the ability to reach a large audience quickly.

Developing a regional CSIRT capability will require the development of a consensus on rules on information-sharing including what information to share, with whom, and when.

4. Financing

The member states will consider the financial mechanisms for establishing and maintaining a national CSIRT in each country and of participating in the hemispheric network.

5. Public Awareness

The Member States should undertake, with CITEL and the REMJA Working Group, an inter-American public awareness program regarding cyber-security and cyber-ethics that emphasizes:

i. the benefits and responsibilities of using information networks;

ii. safety and security best practices;

iii. the potential negative consequences resulting from the misuse of networks;

iv. how to report a cyber incident and to whom; and

v. technical and practical information related to cybersecurity.

The public includes member states, government entities at all levels, the private sector, academia, and the general population.

6. 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 in developing capacity-building projects.

IV. PLAN OF ACTION

A. Census

Conduct a census to identify existing CSIRTS, their membership range, and the services they provide. This will allow us to identify coverage gaps, both geographically and sectorally, and will lay the groundwork for establishing a consensus set of services which member CSIRTs will offer.

B. Rules on information-sharing

Establish rules on information-sharing among CSIRTs, including how shared information should be protected and disseminated.

C. Establishment of national CSIRTs

Each member state will establish or designate national CSIRTs. Among their responsibilities will be the implementation of the pertinent proposals contained 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).

D. National point of contact

Designate a national point of contact with the capacity to exchange information on threats, weaknesses and incidents, report on the cybersecurity status in their jurisdiction, and provide timely information to authorities within their jurisdiction.

E. Best practices compendium

Produce a Best Practices compendium based on international CSIRT norms and practices. These could include standards and protocols to undertake real-time monitoring and subsequent exchange of information throughout the network, and could become the basis of subsequent technical assistance and testing protocols.

F. Assistance for building and maintaining CSIRTs in Member States

Identify resources and capabilities that can be used to help member states build and maintain CSIRT capacity or improve existing CSIRT infrastructures in order to effectively participate in the hemispheric network and meet information-sharing rules. Necessary technical assistance and staff training will be included.

G. Public awarness

CICTE, CITEL, and the REMJA Working Group of Government Experts in Cybercrime will work together to develop an awareness campaign to alert the public in member states to cybersecurity issues and the need to protect their cyber-networks.

H. Follow-up

It is recommended that CICTE reconvene the Meeting of Government Experts on Cybersecurity (Cybersecurity Practitioner's Workshop) to develop and implement the recommendations formulated 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).

It is also recommended that the Working Group to Develop a Draft Cybersecurity Strategy for OAS Member States, of the OAS Committee on Hemispheric Security, transmit this Framework document to the General Assembly for adoption.

APPENDIX II

PCC.I/RES. 49 (IV-04)[9/]
CYBERSECURITY

The IV Meeting of the Permanent Consultative Committee I: Telecommunication Standardization,

RECOGNIZING:

a) That ensuring the safety and security of networked information systems (cybersecurity) is a priority item for our hemisphere;

b) That ubiquitous and secure information networks play an important role for the critical infrastructure of all OAS Member States, their economies and their societies; and

c) That the next generation networks (NGNs) presently being designed and standardized can take into account technologies and techniques to ensure their robustness and harden their resilience to cyber attacks,

TAKING INTO CONSIDERATION:

a) That secure and efficient operation of the global telecommunications infrastructure is crucial to the welfare and development of all sectors of the economy and therefore is of vital interest to both governments and the private sector; and

b) The increasingly frequent and insidious number of cyber attacks on networks, institutions and users, which is causing all kinds of harm, especially those moral, economic and financial,

CONSIDERING:

a) That CITEL, CICTE (the Inter-American Committee Against Terrorism of the OAS) and REMJA (the Meeting of Justice Ministers or Attorneys General of the Americas) are working towards the development of a hemispheric-wide strategy for cybersecurity, as determined by the OAS General Assembly in Resolution AG/RES.1939(XXXIII-O/03);

b) The workshop held jointly by the Working Group on Advanced Network Technologies and Services and the Working Group on Standards Coordination on cybersecurity at the IV PCC.I Meeting in Quito, Ecuador, addressed the key issues of cybersecurity as related to CITEL; and

9. CCP.I-TEL/doc.427/04 rev. 2.

c) The important commitments undertaken by the Heads of State and Government of the Region, as expressed in the Nuevo Leon Declaration, including the encouragement of affordable access to information and communications technologies for all,

FURTHER CONSIDERING:

That CITEL, through its partnering with the private sector on issues in its areas of responsibility, and through its Work Plan for advanced network issues, and in particular cybersecurity and NGNs, can make an important contribution to both raising awareness of critical issues potentially impacting the Region and refining its work plans in these areas through facilitation of focused discussion and information sharing.

RESOLVES:

1. To approve the attached contribution of CITEL to the OAS Cybersecurity Strategy and forward it to the OAS Committee on Hemispheric Security for review and submission to the OAS General Assembly in June 2004.

2. To request the CITEL's Rapporteur on Cybersecurity and Critical Infrastructure matters to convey a copy of this Resolution to the CICTE/CITEL/REMJA Joint Working Group on Cybersecurity.

INVITES:

a) The Working Group on Advanced Network Technologies and Services and the Working Group on Standards Coordination to continue working on the issue of cybersecurity and to report back to PCC.I on their findings on this particular matter.

b) The Chairman of PCC.I to send a letter to the Chairman of the OAS Committee on Hemispheric Security attaching a copy of this Resolution.

ANNEX TO RESOLUTION PCC.I/RES.49 (IV-04)

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

An effective cyber security 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 interweaving of acceptable security capabilities with 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 is 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. To expedite its work, CITEL and the ITU-T organized a joint workshop on Cybersecurity in March 2004. CITEL is also establishing liaisons with other standards bodies and industry fora to obtain the participation and feedback of those parties.

The identification of cyber security standards will be a multi-stepped 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 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, scopes, 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 for the most appropriate and effective implementation.

CITEL's contribution to the cyber security 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 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 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 – "Telecommunications 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 and cyber security 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 the users, all within the legal framework within which the telecommunications services operates, and within the duties and responsibilities of CITEL.

APPENDIX III

MEETINGS OF
MINISTERS OF JUSTICE OR OF MINISTERS
OR ATTORNEYS GENERAL OF THE AMERICAS
III/doc.4/03
(REMJA)

OEA/Ser.K/XXXIV
CIBER-

June 24, 2003
Original: Spanish

Third Meeting of Group of Governmental Experts
On Cyber-Crime
June 23 and 24, 2003
Washington, D.C.

RECOMMENDATIONS
INITIAL MEETING OF GROUP OF
GOVERNMENTAL EXPERTS ON CYBER-CRIME*

Governmental experts on Cyber-Crime of the OAS Member States met in Washington D.C, during the days of June 23 and 24, 2003, in accordance with the recommendations adopted at the Fourth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA-IV) and with OAS General Assembly resolution AG/RES. 1849 (XXXII-O/02).

Taking into account the mandate that was assigned to this Group by REMJA-IV, in concluding its deliberations within the framework of this initial meeting, the Group of Governmental Experts agreed to the following recommendations in relation to the areas in which major developments are required in order to strengthen and consolidate hemispheric cooperation in the fight against cyber-crime:

1. That, in accordance with the recommendation prepared by this Group and adopted by REMJA-III, States that have yet not done so, as soon as possible, identify or, when necessary create or establish, the specific units or bodies charged with the direction and development of the investigation and prosecution of the different modalities of cyber-crimes and that they be assigned the necessary human, financial and technical resources in order to comply with their responsibilities in an efficient, effective and expeditious manner.

---

* The present document was approved in its entirety by the Group of Governmental Experts on Cyber-Crime, in the session that took place on the 24th of June, 2003.

2. That States that have yet not done so, as soon as possible, examine their legal systems to determine whether it adequately applies to combat cyber-crime and collect and keep in safe custody electronic indicia and/or evidence.

3. That the States that have yet not done so adopt legislation that is specifically required for criminalizing the different modalities of cyber-crimes and to set the procedural measures which ensure the collection and preservation in safe custody of electronic indicia and/or evidence, as well as the efficient, effective and expeditious investigation and prosecution of cyber-crimes.

4. That, in order to assist the States in the preparation or improvement and adoption of legislation on cyber-crime, technical meetings be held, within the OAS framework, on legislative drafting in this field, in which specific actions that must be undertaken be considered, among others, in substantive, procedural and mutual legal assistance areas to write or improve national legislation and provide a legal framework that allows and ensures efficient, effective and expeditious hemispheric cooperation in the handling of electronic evidence and of the fight against the different modalities of cyber-crimes.

5. That, based on the information provided by the States, the OAS General Secretariat prepare and maintain an updated directory of points of contact for each one of the countries that make up the Governmental Group of Experts on Cyber-crime, as well as a directory of authorities responsible for the investigation and prosecution of cyber-crimes.

6. That the States that have yet not done so, adopt the necessary decisions for membership, as soon as possible, to the "24 hours/7 days Emergency Network," having first taken the steps in item 1, if necessary.

7. That taking into account progress made through the OAS website, information regarding developments in the fight against cyber-crime be consolidated into a comprehensive information system that provides both public access to information and restricted access to sensitive information for government officials with responsibilities in this field. Likewise that, based on the information provided by the States, the General Secretariat compile and post on the OAS website the applicable national laws and identify the common thematic areas.

8. That the States incorporate specific materials on cyber-crime and the handling of electronic evidence in general into their training programs, directed to judges, prosecutors and law enforcement officials and that the Member States of the OAS and Permanent Observers to this Organization provide the broadest mutual technical assistance and cooperation among themselves.

9. That information exchange and cooperation continue to be strengthened with other international organizations and agencies on cyber-crime like the United Nations, the Council of Europe, the European Union, Asian Pacific Economic Cooperation forum, the OECD, the G-8 and the Commonwealth, giving the OAS Member States the opportunity to know and use the developments in said organizations and agencies.

10. That the Group of Governmental Experts on Cyber-Crime meet at least once a year, within the OAS framework, and that in its following meetings:

a) Examine the results of the technical meetings mentioned in paragraph 4 and that, taking into account their results, consider what adjustments, if any, should be adopted for future meetings of this nature, and further actions that should be taken to facilitate the adoption and application of legislation described above.

b) Prepare recommendations to identify and describe the various types of cyber-crimes.

c) Prepare recommendations to identify and describe the legal investigative powers that States shall possess to investigate cyber-crimes. These legal investigative powers shall:

i) Apply not only to investigation of cyber-crimes, but also to the collection and safe custody of indicia and/or evidence in electronic form of any other criminal offense.

ii) Ensure an adequately balance between the funded and motivated exercise of these powers and the need to guarantee the rules of due process, in the framework of the respect of fundamental human rights and freedoms.

iii) Apply, as permitted by national law, to respond to requests for international cooperation and domestic investigations.

iv) Be able to trace the communications of criminals suspects, through computer networks involving multiple service providers in order to determine the path, origin or destination of the communication.

d) Recommend measures to prevent the creation of cyber-crime heavens in accordance with laws of the States and international treaties.

e) The States report on the measures that they have taken between one meeting and the other.

Washington D.C., United States of America, June 24, 2003.

APPENDIX IV

FIFTH MEETING OF MINISTERS OF JUSTICE OR OF MINISTERS OR ATTORNEYS GENERAL OF THE AMERICAS
April 28-30, 2004
Washington, D.C.

OEA/Ser.K/XXXIV.5
REMJA-V/doc.7/04 rev. 4
30 April 2004
Original: Spanish

CONCLUSIONS AND RECOMMENDATIONS OF REMJA-V*

* The "Conclusions and Recommendations of REMJA-V" were approved by consensus during the plenary session held on April 30, 2004, in the framework of the Fifth Meeting of Minister of Justice or of Ministers or Attorneys General of the Americas (REMJA-V) held at OAS Headquarters in Washington, D.C., United States.

CONCLUSIONS AND RECOMMENDATIONS OF REMJA-V

Having concluded its deliberations on the various items on its agenda, the Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA-V), convened under the auspices of the OAS, approved the following conclusions and recommendations for transmission, through the Permanent Council, to the General Assembly of the OAS at its thirty-fourth regular session.

I. HEMISPHERIC COOPERATION AGAINST TRANSNATIONAL ORGANIZE3D CRIME AND AGAINST TERRORISM

REMJA-V reaffirms that the damage caused and the threat posed by the different types of transnational organized crime and terrorism, to our citizens and to our democracies and to the economic and social development of our states, make it necessary and urgent to continue to strengthen and enhance mutual legal and judicial cooperation at the hemispheric level, as well as to enact laws, procedures, and new mechanisms, if they have not done so, to enable them to combat these crimes effectively.

In this connection, it underscores that the Declaration on Security in the Americas, adopted in Mexico City on October 28, 2003, states that terrorism and transnational organized crime are part of the new threats, concerns, and other diverse challenges affecting the security of the states of the Hemisphere and reaffirms that "the Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA) and other meetings of criminal justice authorities are important and effective fora for promoting and strengthening mutual understanding, confidence, dialogue, and cooperation in developing criminal justice policies and responses to address new threats to security."

Considering that, although the international community has made progress in drawing up regulations to combat these forms of crime, differences persist in the way States criminalize this conduct, which can create obstacles for more effective international cooperation.

REMJA-V recognizes that it is advisable that the subject of transnational organized crime continue to be dealt with by the many bodies of the OAS as they have been doing in the framework of their respective competence, such as CICAD, the Consultative Committee of CIFTA, the CIM, the Inter-American Children's Institute, REMJA, and MESICIC.

REMJA-V reaffirms that the measures carried out by the States Parties in combating terrorism shall take place with full respect for the rule of law, human rights, and fundamental freedoms, without undermining the rights and obligations of States and individuals in keeping with International Law, International Law on Human Rights and International law on Refugees.

REMJA-V expresses satisfaction that in the period following REMJA-IV, OAS Member States have taken significant steps to strengthen hemispheric implementation of United Nations counter-terrorism and transnational organized crime instruments in effectively addressing these crimes. In particular, during the interval between REMJA-IV and REMJA-V, numerous OAS Member States became Party to the 1999 Convention for the Suppression of the Financing of Terrorism, as well as earlier universal counter-terrorism instruments. Similarly, numerous OAS Member States became Party to the 2000 United Nations Convention Against Transnational Organized Crime and its three Complementary Protocols or took substantial steps towards reaching this status. REMJA-V recognizes this notable progress to combat terrorism and transnational organized crime.

REMJA-V also notes with satisfaction that adherence to regional instruments addressing terrorism and organized crime has rapidly accelerated. The 2002 Inter-American Convention Against Terrorism has entered into force on July 10, 2003 and has been ratified by eight (8) Member States of the OAS; and the Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Material (CIFTA) has been ratified by twenty-two (22) Member States of the OAS.

REMJA-V also expresses satisfaction at the progress made in strengthening and consolidating cooperation between the States of the Americas to combat terrorism, through the work of the Inter-American Committee against Terrorism (CICTE) and its national contact points.

At the same time, more work remains in crafting effective implementation of hemispheric and global counter-terrorism and organized crime standards, and we note with alarm the increase in terrorist attacks throughout the world and activities of other criminal organizations. Accordingly, we recommend that:

A. HEMISPHERIC COOPERATION AGAINST TRANSNATIONAL ORGANIZED CRIME

1. With respect to combating organized crime, Member States that have not yet done so sign and ratify, ratify, or accede to, as appropriate, and implement the following as quickly as possible:

   a. The United Nations Convention Against Transnational Organized Crime, the Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children, and the Protocol Against the Smuggling of Migrants by Land, Sea, and Air. We encourage Member States to complete their internal processes for determining whether to sign and ratify the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition.

   b. The Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other

Related Material (CIFTA), which, inter alia, sets forth an effective regime for criminalizing illicit arms trafficking that can aid the fight against organized crime and terrorist groups, as well as creating a mechanism for tracing illicitly trafficked weapons to their source.

2. Member States who are Party or signatory to the Transnational Organized Crime Convention and its two protocols in force, work together at the First Conference of the Parties, June 28 to July 9, 2003, to facilitate the successful application of these important international instruments.

3. To recommend to the General Assembly of the OAS that it convene a group of experts to consider the possibility of drawing up a Hemispheric Plan of Action against Transnational Organized Crime as an integrated plan that brings together the efforts that each area of the OAS has been making to address the problem's different aspects, in accordance with the Declaration on Security in the Americas.

4. That the Member States consider, when appropriate, harmonization of their respective legal frameworks with the obligations taken on in this matter. To this end, it is recommended that the General Assembly of the OAS instruct the Inter-American Juridical Committee to conduct a study on the afore-mentioned issue and that it report to the body that the General Assembly has assigned responsibility to consider the possibility of drafting the Hemispheric Plan of Action against Transnational Organized Crime.

5. That the Member States promote greater inter-relations between law enforcement authorities so they can decide on common lines of action in investigating and prosecuting these crimes.

6. Urge States to hold regional and national training seminars and workshops that refer to the different modalities of transnational organizes crime.

B. HEMISPHERIC COOPERATION AGAINST TERRORISM

1. With respect to combating terrorism, Member States that have not yet done so sign and ratify, ratify, or accede to, as appropriate, and implement the following as quickly as possible:

   a. the twelve United Nations counter-terrorism conventions.

   b. the Inter-American Convention Against Terrorism.

2. Member States have sufficient ability to take law enforcement action with respect to situations in which a terrorist attack has not yet been carried out, and timely investigation and prosecution may prevent the carrying out of such attacks, and take immediate steps to provide for a sufficient ability to pursue and cooperate with each other in respect of such conduct.

3. Each Member State enhances its abilities to facilitate the sharing of information among security services and law enforcement agencies in order to prevent attacks and successfully prosecute terrorists in conformity with applicable national laws and international instruments.

4. In applying Article 7 of the Inter-American Convention against Terrorism, the Member States promote the broadest measures of cooperation, particularly measures to ensure effective cooperation among law enforcement agencies, immigration services, and related agencies, and improve their controls on travel and identity documents.

5. To take note of the work of the Inter-American Commission on Human Rights in the area of terrorism and human rights. It recommends that officials responsible for the development of anti-terrorism legislation continue to meet and exchange best practices and national experiences between them on this issue.

6. To recommend that Hemispheric Information Exchange Network for Mutual Legal Assistance in Criminal Matters include information on legislation, as appropriate, and anti-terrorist policies in force in the Member States.

7. To recommend that, in order to help in the prevention of acts of terrorism, measures must be taken to avoid discrimination against members of society.

II. MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS AND EXTRADITION

A. MEETING OF CENTRAL AUTHORITIES AND OTHER EXPERTS ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS

REMJA-V recommends as follows:

1. To express its satisfaction at the Meeting of Central Authorities and Other Experts in Mutual Legal Assistance in Criminal Matters, held pursuant to the recommendations of REMJA-IV in Ottawa, Canada, from April 30 to May 2 2003, and to adopt in their entirety its recommendations, published in document OEA/Ser.K/XXXIV.5 REMJA-V/doc.4.

2. To support, in accordance with recommendation 6 of that meeting, the continued holding of meetings of the Central Authorities and other Experts on mutual legal assistance in criminal matters in the Hemisphere at least once between REMJAs, with the support and coordination of the Working Group on Mutual Legal Assistance, as well as consideration, at their next meeting, of both progress made in implementing the recommendation of the Ottawa meeting and, *inter alia*, the topics referred to in the aforementioned recommendation 6, according to an order of priorities that they define.

3. To decide that the next Meeting of Central Authorities and Other Experts start considering actions to build up hemispheric legal cooperation in the matter of extradition, including temporary extradition when appropriate in keeping with national legislation and to proceed with organizing the sections on mutual legal and judicial cooperation of a hemispheric plan of action to fight against transnational organized crime and terrorism, including measures of administration of cases by the requesting State so as not to overburden the requested State.

4. To decide that the next Meeting of Central Authorities and Other Experts shall continue building up and rendering more effective the mechanisms of mutual legal assistance in criminal matters, and hemispheric cooperation in the matter of extradition. To this end, the Meeting of Central Authorities and Other Experts will be able to request input from the following bodies regarding the areas of their competence: CICTE, CICAD, Consultative Committee of CIFTA, CIM, MESICIC, Inter-American Children's Institute, and the Inter-American Juridical Committee.

B. HEMISPHERIC INFORMATION EXCHANGE NETWORK FOR MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS

In view of the usefulness and importance of the *Hemispheric Information Exchange Network for Mutual Legal Assistance in Criminal Matters*, REMJA-V recommends as follows:

1. To decide to adopt the Hemispheric Information Exchange Network for Mutual Legal Assistance in Criminal Matters and urge all Member States to implement its public component and disseminate among the most interested users.

2. That, since the network, under the leadership of a group consisting of Argentina, Bahamas (The), Canada, and El Salvador, and administered by the OAS General Secretariat, comprises data on all OAS Member States, information related to mutual legal assistance in criminal matters and extradition should continue to be posted on the public website.

3. That States that have not yet done so identify a contact person to provide and update the information made available via the network.

4. To express satisfaction towards the development of the MLA secure e-mail pilot project and recommends that all States take the appropriate measures to evaluate it and that it continue to operate and be expanded to cover other States.

5. To examine the possibility of exchanging information, in mutually interesting areas and methodologies, with the Virtual Prosecution Office of Latin America.

III. PENITENTIARY AND PRISON POLICIES

Given the importance and advisability of continuing and reinforcing the exchange of information and experiences as well as mutual cooperation with regard to penitentiary and prison policies, REMJA-V recommends as follows:

1. To express its satisfaction with the results and adopt the report of the First Meeting of the Group of Officials Responsible for the Penitentiary and Prison Policies of the OAS Member States (document OEA/Ser.K/XXXIV.5 REMJA-V/doc.6/04), OEA/Ser.K/XXXIV.5 REMJA-V/doc.6/04), held at OAS headquarters on October 16 and 17, 2003, in keeping with a REMJA-IV decision.
2. To support periodic meetings of officials responsible for the penitentiary and prison policies of the OAS member states and the establishment of an Internet information system on such policies, as recommended at the first meeting of the officials.

3. That the States, through their participation in the meetings of penitentiary and prison authorities, promote penitentiary strategies and policies, based on respect for human rights, and that contribute to reducing overcrowding in prisons. To this end, the States will promote modernization of prison infrastructure and extend the functions of rehabilitation and social integration of the individual, by improving conditions of detention and studying new penitentiary standards.

IV. CYBER-CRIME

Under this topic, REMJA-V recommends as follows:

1. To express its satisfaction with the results of the Initial Meeting of the Group of Governmental Experts on Cyber-Crime, held at OAS headquarters on June 23 and 24, 2003, in keeping with a REMJA-IV decision.

2. To adopt the recommendations of the Group of Governmental Experts (document OEA/Ser.K/XXXIV.5 REMJA-V/doc.5/04) and to ask it, through its Chair, to report to the next meeting of REMJA on the progress made regarding said recommendations.

3. To support consideration of the recommendations made by the Group of Governmental Experts at its initial meeting as the REMJA contribution to the development of the Inter-American Strategy to Combat Threats to Cybersecurity, referred to in OAS General Assembly resolution AG/RES. 1939 /XXXIII-O/03), and to ask the Group, through its Chair, to continue to support the preparation of the Strategy.

4. That international training on cybercrime be provided to the States of the OAS that request it and that the States of the OAS in general consider the possibility of allocating resources to guarantee delivery of this training.

5. That the Member States participate in the technical meetings of the Group of Governmental Experts on Cyber-Crime so that future challenges can clearly be understood throughout the hemisphere.

6. That Member States, in the context of the expert group, review mechanisms to facilitate broad and efficient cooperation among themselves to combat cybercrime and study, when possible, the development of technical and legal capacity to join the 24/7 network established by the G8 to assist in cybercrime investigations.

7. To the extent possible, Member States ensure that differences in the definition of offenses do not impede the efficiency of cooperation through mutual legal and judicial assistance and extradition.

8. That Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercime (2001); and consider the possibility of acceding to that convention.

9. That Member states review and, if appropriate, update the structure and work of domestic bodies, or agencies in charge of enforcing the laws so as to adapt to the shifting nature of cybercime, including by reviewing the relationship between agencies that combat cybercrime and those that provide traditional police or mutual legal assistance.

V. CORRUPTION: FOLLOW-UP ON THE COMMITMENTS UNDERTAKEN IN THE DECLARATION OF NUEVO LEÓN

The Declarations of Nuevo Leon and Quebec City, as well as previous REMJA, recognize the severity of the problem of corruption in our societies.

We note with approval that, since REMJA-IV, most Member States have signed the United Nations Convention against Corruption and a number of additional Member States have become Party to the Inter-American Convention against Corruption, but we today undertake to strengthen our efforts to effectively pursue corruption.

Accordingly, REMJA-V recommends that Member States:

1. That have not yet done so take measures as soon as possible that are necessary to reach the following objectives:

   a. Sign and ratify, ratify, or accede to, as appropriate, and implement the 2003 United Nations Convention against Corruption.

   b. Sign and ratify, ratify, or accede to, as appropriate, and implement the 1996 Inter-American Convention against Corruption.

2. Cooperate to strengthen the Follow-up Mechanism for the Implementation of the Inter-American Convention against Corruption, through practical measures to enhance its effectiveness, including to increase economic resources and develop human resources and speed up the evaluation process of the First Round.

3. Prior to REMJA-VI, each Member State, in conformity with its national laws and applicable international regulations, shall adopt domestic legal measures that deny safe haven to corrupt officials, to those who corrupt them, and their assets and shall exchange information on the measures they have adopted.

4. In conformity with national legislation and any international juridical instruments that are applicable, review their legal regimes to extradite and provide mutual legal assistance with respect to corruption offenses, including their abilities to provide for confiscation of assets proceeding from criminal activities on behalf of other countries that may have different modalities for obtaining confiscation, with a view to enhancing them.

5. Adopt such legislative and other measures, in accordance with fundamental principles of its domestic law, as may be necessary to enable its competent authorities to return confiscated property to the requesting State, in the case of embezzlement of public funds or of laundering of embezzled public funds.

6. We shall support the work of the meeting of the States Parties to the Inter-American Convention against Corruption that will be held in Managua, Nicaragua in July 2004, which should consider “additional concrete measures to increase transparency and combat corruption.”

VI. TRAFFICKING IN PERSONS, ESPECIALLY WOMEN AND CHILDREN

Bearing in mind that the trafficking in persons is an offense against human dignity, which should be criminalized, prevented, and combated and whose victims are in a situation of vulnerability, which requires greater international attention and due assistance and protection to safeguard their human rights and for which, to reach these goals, integral cooperation of all the States is required.

Recognizing that there are many international instruments guaranteeing the protection of women, boys, girls and adolescents, such as the Convention on the Rights of the Child, the Convention on the Elimination of All Forms of Discrimination against Women, the Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women, ILO Convention 182 concerning the Worst Forms of Child Labor, the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, the Inter-American Convention on International Traffic in Minors, and the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children.

Bearing in mind that the Protocol to Prevent, Suppress and Punish the Trafficking in Persons, Especially Women and Children, complementary to the United Nations Convention against Transnational Organized Crime, specifies the actions that qualify trafficking in persons as a crime.

Determined to overcome obstacles in the fight against this transnational crime.

REMJA-V recommends the following:

1. That Member States that have not yet done so sign and ratify, ratify, or accede to, as appropriate, and implement the following as quickly as possible, the Protocol to Prevent, Suppress and Punish the Trafficking in Persons, Especially Women and Children, that complements the United Nations Convention against Transnational Organized Crime.

2. Encourage Member States to complete their internal processes for determining whether to sign and ratify:

   a. The Protocol against the Illicit Trafficking in Migrants by Land, Sea and Air

   b. The Inter-American Convention on International Traffic in Minors.

3. The holding of a meeting of national authorities in this matter, including the participation, *inter alia*, of the CIM, the IIN, the United Nations, the OIM, and other related international organizations for the purpose of studying integral cooperation mechanisms among the States to ensure protection of and assistance to the victims, the prevention of the crime, and the prosecution of

its perpetrators. Likewise, the meeting will facilitate the exchange of information and experiences, political dialogue and cooperation between the countries of origin, transit and destination of the trafficking in persons, as well as the establishment or improvement of statistics records in this area.

4. To keep the topic of the Trafficking in Persons as an item on the agenda in future debates of REMJA.

VII. VIOLENCE AGAINST WOMEN

REMJA-V:

1. Urges Member States to complete their internal processes for determining whether to sign and ratify the Inter-American Convention on the Prevention, Punishment and Eradication Violence against Women (Convention of Belén do Pará).

2. Encourages the States Parties to the Inter-American Convention on the Prevention, Punishment and Eradication Violence against Women (Convention of Belén do Pará) to study the most appropriate manner establish the Convention's Follow-up Mechanism.

VIII. GENDER AND JUSTICE

REMJA-V, after having heard the presentation by the Inter-American Commission of Women (CIM), took note of the recommendations on gender and justice formulated to the REMJA-V by the Second Meeting of Women Ministers or Ministers or Top Authorities Responsible for Women's Policies in the Member States and refers them to the Member States for greater consideration.

IX. JUSTICE STUDIES CENTER OF THE AMERICAS (JSCA)

Pursuant to the mandates of the Second and Third Summits of the Americas, OAS resolution AG/RES.1 (XXVI-E/99), and the conclusions and recommendations of REMJA II and III, which led to the establishment of a Studies Center to contribute to improving the policies and institutional capacity of the region's justice systems.

And having heard the report of the Justice Studies Center of the Americas, REMJA-V decides:

1. To express its appreciation to the Board of Directors and the Executive Director for the leadership and initiative they have shown in guiding and developing the Center's initial work plans in the criminal justice area and giving concrete form to the vision of a regional center of justice sector expertise set forth by the Heads of State and Government in Santiago of Chile.

2. To congratulate the Center on the successful launch of websites and publications that are being widely consulted in the region, as well as on the drafting of an important comparative study of criminal procedure norms and practices in the region that should help improve justice system performance.

3. To express satisfaction at the efforts made to ensure participation by Member States in Center programs and activities, notwithstanding the diversity of interests and institutions involved and the limitations of funding.

4. To request that the Center, consistent with the objectives set forth in its Statute, include in its working plans the conclusions and recommendations of REMJA, toward which end the Member States shall provide the necessary resources.

5. To request the Center to organize a working group or process, including both the Member States and other donors, to develop for consideration by REMJA-VI a plan for funding the Center consistent with the mandate of the Third Summit of the Americas. This process shall be without detriment to the voluntary contributions that for this purpose the Member States should make, in accordance with the provisions of the Center's Statute, approved by the General Assembly of the Organization of American States.

6. To approve renewal of the Executive Director's term of office as agreed by the Board of Directors of the Center, in accordance with its Statute, in a regular session held on January 5, 2004 in Santiago de Chile.

7. To request the Center to continue supporting national efforts to strengthen domestic systems, with a view toward improving the national frameworks for cooperation and mutual legal assistance.

X. NEXT MEETING

REMJA-V recommends that the Sixth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA-VI) take place in 2006 and that the OAS General Assembly charge the Permanent Council of the OAS to set a date and site for REMJA-VI.

APPENDIX V

INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)

FOURTH REGULAR SESSION
January 28-30, 2004
Montevideo, Uruguay

OEA/Ser.L/X.2.4
CICTE//INF.4/04/04
29 January 2004
Original: English

FRAMEWORK FOR ESTABLISHING AN INTER-AMERICAN CSIRT WATCH AND WARNING NETWORK

(Presented by Ambassador Margarita Escobar,
Chair of the Working Group of the OAS Committee on Hemispheric Security
of the OAS, held on January 29, 2004, during the Third Plenary Session)

FRAMEWORK FOR ESTABLISHING AN INTER-AMERICAN CSIRT WATCH & WARNING NETWORK

(Presented by Ambassador Margarita Escobar,
Chair of the Working Group of the OAS Committee on Hemispheric Security
of the OAS, held on January 29, 2004, during the Third Plenary Session)

Objective: To develop a hemisphere-wide 24-hour per day, seven day per week network of national points of contact among Computer Security Incident Response Teams (CSIRTs) with national responsibility (National CSIRTs), in OAS member states, capable of and charged with appropriately and rapidly responding to cyber-security related crises, incidents, and threats.

As intruders use increasingly sophisticated attack tools, launch highly automated attacks that travel at Internet speed, and intentionally use attack techniques that make it difficult to understand the nature and source of the attacks, global, real-time collaboration across response teams will become increasingly important. This collaboration would:

- support rapid and accurate diagnosis of a problem;
- rapidly disseminate warnings of actual attacks across the global community;
- rapidly disseminate warnings of generic vulnerabilities across the global community;
- alert the global community to suspicious activity and support collaborations that investigate and diagnose the activity;
- provide information on mitigation and remediation strategies to combat attacks and threats; and
- minimize duplication of analysis effort across teams.

Collaboration helps to leverage the technical knowledge that exists across the teams to limit damage and ensure continued operation of critical services.

Principles:

Indigenous – The program must be operated and controlled by entities rooted in each participating nation, designated by their government.

Systemic – The system must be a multi-faceted operation requiring an aware and trained workforce, regular sharing of information regarding current threats and vulnerabilities, constant re-evaluating and implementing of best practices and appropriate interaction with public policy makers.

On-going - due to the inherent daily evolution of the Internet, any successful program must regularly be updated and maintained. Internet security will not be achieved with a one-time fix.

Accountable – The "security" in "cyber security". Strict 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 and become counter-productive.

Built upon existing arrangements – There are a number of pre-existing entities in the hemisphere that provide cyber-security services to a greater or lesser extent. Any new system should build upon these pre-existing institutions to avoid duplication and encourage active participation.

Identification of Existing Organizations

There are well over a hundred organizations that use the name CERT (Computer Emergency Response Team), or CSIRT (the generic term of equivalent meaning), world-wide. Many, but not all, have some affiliation with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University where the first "CERT" was created. Even those CSIRTs associated with CERT/CC vary in their specific approaches to incident response based on a variety of factors such as consistency, geographical and technical issues, authority, services provided, and resources. In the United States, the Department of Homeland Security, National Cyber Security Division has created US-CERT, to be the "Computer Emergency Readiness Team" with national responsibility in the United States. In Canada, the Cyber Protection Division within the newly formed Public Safety and Emergency Preparedness Canada (PSEPC) fulfils a similar national responsibility role.

The Forum on Incident Response Teams (FIRST), a world-wide, voluntary association of CSIRTs, lists 79 members within the OAS Member States, of which 68 are in the US. Of the remainder, six are in Canada; two are in Brazil, and one each in Chile, Mexico, and Peru. In addition, some companies, such as ATT, Symantec, and Visa, offer CSIRT services to their customers throughout the world, and there may be other CSIRTs in the region, such as Ar-CERT in Argentina, that that are not part of the FIRST network.

Given the information gaps, conducting a CSIRT census is the essential first step towards developing a cyber-security network.

Establishing a Service Model

While there are no international agreed upon standards for what constitutes a CSIRT, there are a number of documents and efforts that can assist the process of defining a CSIRT team and on certification and accreditation of CSIRTs.

The CERT/CC has published a variety of documents that can assist in the creation of a CSIRT, including:

- *Handbook for Computer Security Incident Response Teams (CSIRTs)* provides updated guidance on generic issues to consider when forming a CSIRT;
- *State of the Practice of Computer Security Incident Response Teams*. This report includes information collected through a pilot survey of computer security incident response teams (CSIRTs), CERT/CC's own experience, discussions with and observations of other CSIRTs, and research and reviews of the current literature on incident response; and
- *Creating a Computer Security Incident Response Team: A Process for Getting Started* is a document that describes the basic requirements for creating a CSIRT.

In addition, the United States Department of Defense (US DoD) has created a program of certification and accreditation of computer network defense service providers within the US DoD. This program can be used as a starting point for establishing criteria for the accreditation of National CSIRTs.

In establishing a regional network of cooperating National CSIRTs, a minimum set of standards and services would be expected. These would include:

- designation of responsibility by the National CSIRT's government;
- agreement to principles of information sharing among the cooperating teams;
- responsibility for receiving information from other National CSIRTs and disseminating that information to appropriate entities within the country;
- authorization to disseminate information to other National CSIRTs; and
- provide coordination assistance to other National CSIRTs for incidents and threats.

Trust Issues

Much of the information which CSIRTs need to exchange is proprietary or otherwise sensitive and there are few good models that promote the consistent sharing of information among CSIRTs. Trust – the essential ingredient in information sharing – when it exists, has developed among individuals who know and have worked with each other, rather than institutionally, among organizations. To establish trust, clear expectations on how information exchanged will be used or disseminated must be understood and followed by all parties. Principles of information sharing stating how information can be used or disseminated must be agreed to among all of the cooperating National CSIRTs.

Vulnerability disclosure policies outline under what circumstances and to whom vulnerability information is disseminated. These policies must balance the need to disseminate actionable information to appropriate audiences with the need to minimize the potential that intruders will obtain the information before patches or workarounds are available.

Some of the CSIRT attributes that are required to promote trust in communication and cooperation about sensitive security issues include:

- a secure infrastructure for managing sensitive information;
- the ability to communicate securely with stakeholders;
- the ability to marshal experts and decision makers;
- an infrastructure to support advance notification to select audiences;
- procedures to guard against information leakage;
- a well-known public interface for dissemination of critical information; and
- the ability to reach a large audience quickly.

Developing a regional CSIRT capability will require the development of a consensus on principles of information sharing including what information to share, with whom, and when.

Financing

CSIRT financing is not inexpensive. In addition to providing equipment and trained staff on a permanent basis, CSIRT administrators need to provide periodic technical assistance and develop regular exercises to keep their operations sharp. Member States and the Organization will have to carefully consider CSIRT funding mechanisms and may have to prioritize their coverage, or seek stable sources of outside funding.

It should be noted that in October 2002, APEC leaders called for the development of a regional 24/7 CSIRT capability by October 2003. Both APEC and the Government of Australia agreed to fund CSIRT capacity-building projects in four member economies. In their most recent report on the project, APEC officials admitted difficulties in attracting acceptable applicants and in raising adequate funds to cover the cost of the project.

Public Awareness

Government and industry support for CSIRT programs (and financing) is closely linked to public awareness of the cyber-security problem and its potential impact on highly desirable development goals. If systems in one networked economy are not adequately protected, then the networks and infrastructures of all the interconnected economies are vulnerable. Participants in a network, whether as developer, owner, operator, or individual user, must be aware of the threats to and vulnerabilities of the network and assume responsibility for protecting that network according to their position and role. The Organization, working with Member States and CSIRTS, should undertake a public awareness program regarding cyber-security and cyber-ethics that emphasizes (1) the benefits and responsibilities of using information networks; (2) safety and security best practices; and (3) the potential negative consequences resulting from the misuse of networks. There are a number of organizations and on-line sites with useful information for this purpose; the Organization should take advantage of them.

Extending the Network

Although public awareness is an essential element of this proposal, establishing a regional CSIRT capability will require developing political commitments where they may not exist. The working group should propose a draft resolution on cyber-security for approval by the Committee on Hemispheric Security and transmission to the General Assembly for their approval, which commits Member States to establish CSIRTs in their territories and to implement such other recommendations the group may make and the Committee may approve. This will harness the Member States' political will to achieve regional CSIRT coverage and provide the Organization with the institutional framework necessary to proceed. With this resolution in hand, the working group can assist individual states to develop specific plans and, assuming adequate funding, to develop capacity-building projects in the Member States. As of this moment, no state has offered to fund this project.

Course of Action

Action Item 1: Conduct a census to identify existing CSIRTS, their membership range, and the services they provide. This will allow us to identify coverage gaps, both geographically and sectorially, and will lay the groundwork for establishing a consensus set of services which member CSIRTs will offer. A notional census questionnaire is attached.

Action Item 2:Establish a consensus for a minimum set of services that all member CSIRTs will offer. This will help shape a consistent, hemisphere-wide operating doctrine and provide the key for subsequent technical assistance activities.

Action Item 3:Draft a resolution for submission to the CHS and GA calling on Member States to create CSIRTs and implement the other proposals contained in the working group report. Of the 11 non-US CSIRTs that are members of the FIRST network, six are government-run, four are private sector, and one is run by a university.

Action Item 4:Produce a Best Practices compendium based on the consensus CSIRT services and standards, consistent with similar practices in Europe and Asia. These could include standards and protocols to undertake real-time monitoring and subsequent exchange of information throughout the network, and will become the basis of subsequent technical assistance and testing protocols.

Action Item 5:Establish a system of on-going technical assistance and information exchange for CSIRTs. Some countries will need capacity-building assistance or technical assistance to create an information protection coordination capacity or to improve existing capacities in order to meet the required standards. Financing will need to be secured.

Upon completion of Action Item 1, hold an Inter-American meeting of existing CSIRT representatives to move forward on the action items and on issues of information-sharing, identification of gaps in coverage and technical assistance, interoperability, and intercommunication. Representatives of the OAS Cyber-security Working Group would attend to provide policy input where necessary, and ensure that the issues outlined in this paper are addressed. Such a meeting would also be an important step in tackling the trust issue, and, as it would be at the technical level, would not be contingent upon GA action.