May 16, 2006

Framework for National Action
for
Cyber Security and Critical Information Infrastructure Protection (CIIP)

Introduction: In resolution 57/239 on the *Creation of a global culture of cybersecurity*, the United Nations General Assembly, recognized "that, in a manner appropriate to their roles, government, business, other organizations and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies." This view was reaffirmed by the World Summit on the Information Society (WSIS) in the Tunis Agenda for the Information Society and in the Geneva Declaration of Principles and Plan of Action.

The global interconnectivity of information networks and systems, and the necessity for this interconnectivity if we are to achieve the full promise of these new technologies, means that no single nation can successfully secure itself in isolation. Security is a problem common to all nations and each nation's security is limited by that of the weakest link in the global infrastructure.

The nine simple elements for creating a Culture of Cybersecurity promulgated by the OECD in its Guidelines for the Security of Information Systems and Networks" translate into the need for national action by all countries and action by all participants in the information society. Developing this new Culture will require review and modification of national institutions, laws, procedures, cooperative arrangements and attitudes towards the information society. To facilitate this task, the following *Framework for National Action (Framework) for Cyber Security and Critical Information Infrastructure Protection (CIIP)* was prepared as a guide for national policy makers. It outlines the breadth, depth and interrelations of institutions and functions involved in cyber security. The Framework is composed of five overarching areas for attention by policy makers. It provides the policy objective for each area together with goals for achieving the policy, actions that must be taken to achieve the goals, and information on where to find supporting dialogue and training resources. This Framework is based on the experience of the US both in the development of the US domestic structures and procedures, which continue to evolve, and on our observations from participation with other governments bilaterally and through international organizations in addressing these issues.

While the Framework calls for designation of national leadership to oversee the cyber security and CIIP, the plan also recognizes that each area of the plan will have its own leaders and persons in charge of various actions. The Framework thus serves as a template to allow all participants to see how their actions fit into the whole national effort. Because coordination across areas is essential, the plan has some duplication where different participants have complementary roles for achieving related goals, policies, and in turn, the national plan. It is also intended that the outline will be supplemented as new areas become evident and in particular that additional materials, especially training materials, will be added as they are identified.

In considering action covered by the Framework, it is important to recall the concluding documents of both sessions of the World Summit on the Information Society and keep in mind that security must be implemented in a manner consistent with other objectives of the information society. In addition, measures adopted to implement a Culture of Security will form part of the economic environment of a nation and impact the ability of the private sector, the primary owner, operator and builder of information systems and networks, to continue the development of the domestic infrastructure.

The Framework is outlined below. The outline is also reproduced on two power point slides to facilitate a visualization of the full scope of actions required.

Framework for National Action for Cyber Security and Critical Information Infrastructure Protection

Part 1:

National Strategy and Administration (NS)

POLICY: *Protection of critical national information infrastructures and cyberspace are essential to national security and a nation's economic well-being. Critical national information infrastructures and cyberspace are interconnected across industry sectors and national borders. The protection of these infrastructures and cyberspace requires coordinated national action related to the prevention, preparation, response, and recovery from an incident on the part of government authorities at the national, state/provincial and local levels; the private sector; and citizens/users; and cooperation and coordination with international partners.*

1 - Goals:

NS 1.1 Create awareness at policy level of cyber/Critical Information Infrastructure Protection (CIIP) issues and need for national action and international cooperation.

NS 1.2 Develop a national strategy to protect national critical information infrastructures and cyberspace from all-hazards (cyber and physical) incidents.

NS 1.3 Join international efforts to coordinate activities related to the prevention, preparation, response, and recovery from incidents.

2 - ACTIONS:

NS 2.1 Undertake policy level discussions with major players and key decision makers with regard to threats and vulnerabilities and the need for national action.

NS 2.2 Identify lead institution for national effort; determine government construct and requirements for placement and stand-up of a computer security incident response team with national responsibility; and identify lead institutions for each aspect of the national strategy.

NS 2.3 Identify stakeholders and points of contact within government ministries, state and local government, and the private sector.

NS 2.4 Identify roles, responsibilities and cooperative arrangements for and among all participants.

NS 2.5 Establish mechanisms for cooperation among government and private sector entities at the national level.

NS 2.6 Identify international stakeholders and partners, and join international information efforts to address cyber security and CIIP issues, including information sharing and assistance efforts.

NS 2.7 Assess and conduct periodic reassessments of the current state of cyber security and CIP, and develop program priorities.

NS 2.8 Identify training requirements and need for technical exchanges.

3 – Dialogue and Training Resources:(*available from the U.S. or internationally*)

NS 3.1 Awareness raising (Supports NS 2.1, 2.2)

- OECD Guidelines and Culture of Security: http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
- UNGA Resolutions 55/63, 56/121, 57/239, 58/199: http://www.un.org/Depts/dhl/resguide/gares1.htm
- EU Commissioner Erkki Liikanen on "Information Society in an Enlarged Europe," Budapest, 2/26/04, http://europa.eu.int/comm/commissioners/liikanen/index_en.htm
- EU Commissioner Viviane Reding on "i2010: How to Make Europe's Information Society Competitive," Brussels, 2/22/05, http://europa.eu.int/comm/commissioners_barroso/reding/index_en.htm
- European Network and Information Security Agency, http://www.enisa.eu.int/

NS 3.2 National Strategy (NS 2.2, 2.3, 2.4, 2.7)

- U.S. National Strategy to Secure Cyberspace: http://www.whitehouse.gov/pcipb/
- National Implementation Strategies of 11 OECD members: http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
- UK: www.niscc.gov.uk
- New Zealand: www.digitalstrategy.gov.nz
- Canada: www.psepc-sppcc.gc.ca

NS 3.3 Assessment and program development (NS 2.4, 2.5, 2.7, 2.8)

-

NS 3.4 International assistance points of contact (NS 2.6)

-

May 16, 2006

Legal Foundation and Regulatory Development (LR)

POLICY: *The protection of critical national information infrastructures and cyberspace requires the updating criminal law, procedures and policy to address and respond to cybersecurity and cybercrime.*

Goals:

LR 1.1 Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime in accordance with the provisions of international legal instruments and the Council of Europe's Cyber Crime Convention (2001).

Actions:

LR 2.1 Assess the current legal authorities for adequacy.
LR 2.2 Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime.
LR 2.3 Establish or identify national cybercrime units.
LR 2.4 Develop cooperative relationships with other elements of the national cyber security infrastructure and the private sector.
LR 2.5 Develop understanding of cyber crime issues in judiciary and legislative branches of government.
LR 2.6 Participate in the 24X7 Cybercrime Point of Contact Network.

3 – Dialogue and Training Resources:(*available from the U.S. or internationally*)

LR 3.1 Executive Branch (Supports LR 2.1, 2.6)

- Council of Europe: Convention on Cybercrime website: http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp
- UNGA Resolutions 55/63, 56/121: http://www.un.org/Depts/dhl/resguide/gares1.htm
- G-8 High-Tech Crime Principles and 24X7 information assistance mechanism: http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- DOJ CCIPS website: http://www.cybercrime.gov
- APEC TEL Working Group E-Security Task Group Documents: http://www.apectelwg.org/e-securityTG/index.htm
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials: http://www.apectelwg.org/e-securityTG/Resources.htm

LR 3.2 Legislative Branch (Supports LR 2.2, 2.5)

- Council of Europe: Convention on Cybercrime website: http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp
- UNGA Resolutions 55/63, 56/121: http://www.un.org/Depts/dhl/resguide/gares1.htm
- DOJ CCIPS website: http://www.cybercrime.gov

- APEC TEL Working Group E-Security Task Group Documents: http://www.apectelwg.org/e-securityTG/index.htm
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials: http://www.apectelwg.org/e-securityTG/Resources.htm

LR 3.3 Judicial Branch (Supports LR 2.2, 2.5)

- Council of Europe: Convention on Cybercrime website: http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp
- UNGA Resolutions 55/63, 56/121: http://www.un.org/Depts/dhl/resguide/gares1.htm
- DOJ CCIPS website: http://www.cybercrime.gov
- APEC TEL Working Group E-Security Task Group Documents: http://www.apectelwg.org/e-securityTG/index.htm
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials: http://www.apectelwg.org/e-securityTG/Resources.htm

Part 3:

Incident Response Watch and Warning (IR)

POLICY: *Maintain an organization to serve as a focal point for securing cyberspace and the protection of critical national information infrastructures, whose mission includes watch, warning, response and recovery efforts and the facilitation of interactions and collaboration between and among government entities at the national, state and local levels; the private sector; academia; and internationally.*

Goals:

IR 1.1 Develop a national cyberspace security response system with effective organizations to prevent, predict, detect, respond to and recover from cyber incidents.

IR 1.2 Develop national cyberspace threat and vulnerability reduction program in coordination with the intelligence and law enforcement communities.

IR 1.3 Develop national cyberspace security awareness and training program.

IR 1.4 Develop procedures and capabilities to secure government computer systems and networks.

IR 1.5 Participate in international watch, warning and incident response information sharing mechanisms.

Actions:

IR 2.1 Identify or establish a national computer security incident response team (CSIRT) capability. (Supports IR 1.1, 1.2, 1.5)

IR 2.2 Establish mechanism(s) for coordination within government among civilian agencies, law enforcement, the military and intelligence communities.

IR 2.3 Establish partnerships with the private sector for the prevention and response to cyber incidents.

IR 2.4 Establish point(s) of contact for consultation, cooperation, and information exchange among CSIRTs from government agencies, the military and intelligence communities, the private sector and international partners.

IR 2.5 Undertake international cooperative and information sharing activities.

IR 2.6 Develop tools and procedures for the protection of the cyber resources of government entities.

3 – Dialogue and Training Resources:(*available from the U.S. or internationally*)

IR 3.1 National Response Plan (Supports IR 2.1-2.6)

- http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf
- Industry: National Cyber Security Partnership: http://www.cyberpartnership.org/031804.html
- StaySafeOnline http://www.staysafeonline.info/
- Information Security and Privacy Advisory Board http://csrc.nist.gov/ispab/
- NIST: http://csrc.nist.gov/

IR 3.2 National CSIRT (Supports IR 2.1-2.5)

- US CERT: http://www.us-cert.gov/
- Homeland Security Operations Center http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0456.xml
- NIATEC training courses: http://niatec.info
- Carnegie Mellon University/CERT Coordination Center: http://www.cert.org/csirts/
- India: www.cert-in.org.in
- Australia: www.auscert.org.au

IR 3.3 Cooperation and Information Sharing (Supports IR 2.1-2.5)

- Industry: National Cyber Security Partnership, Early Warning Task Force: http://www.cyberpartnership.org/031804.html
- National Cyber Security Partnership, Public Awareness Task Force http://www.cyberpartnership.org/031804-3.html
- IT-ISAC: https://www.it-isac.org/
- National Cyber Response Coordinating Group: http://www.dhs.gov/dhspublic/display?content=4359
- http://www.house.gov/science/hearings/full05/sept15/Purdy%20Testimony%20Final.pdf
- Critical Infrastructure Protection Advisory Committee http://www.itaa.org/infosec/docs/CIPAC Fact Sheet2.pdf
- IT Sector Coordinating Council http://www.itaa.org/infosec/docs/ITSCCResponsestoGAO.pdf

Part 4:

Industry-Government Partnership (IG)

POLICY: *The protection of critical information infrastructure and cyberspace is a shared responsibility that requires a coordinated partnership between the government at all levels and the private sector, which owns and operates much of this information infrastructure.*

Goals:

IG 1.1 Develop public-private partnerships for the protection of cyberspace and globally interconnected information infrastructures.
IG 1.2 Develop cyber risk management program.

Actions:

IG 2.1 Include industry perspectives in the development and implementation of security policy and efforts.
IG 2.2 Encourage development of industry and non-government (sector) groups to address security around common interests.
IG 2.3 Encourage cooperation among sector groups of interdependent industries.
IG 2.4 Establish cooperation arrangements between government and industry for watch, warning and incident response systems. (See also IR.)
IG 2.5 Support industry awareness raising efforts.
IG 2.6 Promote a comprehensive national awareness program to empower all participants – businesses, the general workforce, and the general population – to secure their own parts of cyberspace.
IG 2.7 Develop a framework for public-private partnership to address cyber risk based on threats, vulnerabilities and consequences.

3 – Dialogue and Training Resources:(*available from the U.S. or internationally*)

IG 3.1 Structures for Industry-Government Partnership (IG 2.1, 2.2 and 2.7)
ISACs & Coordinating Councils

- Multi State Information Sharing and Analysis Center : Main Page http://www.cscic.state.ny.us/msisac/index.html; NY State http://www.cscic.state.ny.us
- ITAA White Paper on Information Security: http://www.itaa.org/infosec/doc/ITAANIPPComments1.doc
- ITAA Comments on DHS National Infrastructure Protection Plan: http://www.itaa.org/infosec/docs/ITAANIPPComments1.doc
- Industry-Government Cooperation on Standards: American National Standards Institute-Homeland Security Standards Panel: www.ansi.org/standards_activities/
- Network Reliability and Interoperability Council (NRIC): http://www.nric.org/

- National Security and Telecommunications Advisory Committee (NSTAC): http://www.ncs.gov/nstac/nstac.html
- National Telecommunications and Information Administration: http://www.ntia.doc.gov/

IG 3.2 Cyber security and CIIP information sharing (IG 2.3, 2.4 and 2.7)

- National Information Assurance Council (NIAC) report on cross sector interdependencies: http://www.itaa.org/infosec/docs/Cross%20Sector%20Interdependencies%20WG%20Final%20Report_Redacted%20(2003-10-06)pdf
- US-CERT alerts: http://www.us-cert/cas/
- National Cyber Alert System (NCAS): http://www.dhs.gov/dhspublic/display?content=3086
- Network Reliability and Interoperability Council, www.nric.org
- National Institute of Standards and Technology, Computer Security and Research Center, http://csrc.nist.gov/

IG 3.3 Awareness raising and outreach: Tools for business and home use (IG 2.5 and 2.6)

- Information for technical and non-technical users: http://www.us-cert.gov/
- StaySafeOnLine: http://www.staysafeonline.org/
- Federal Trade Commission: Onguard Online www.ftc.gov/infosecurity and www.OnGuardOnline.gov
- State of Virginia: http://www.interoperability.publicsafety.virginia.gov/index.cfm
- U.S. CERT posters and information sheets: http://www.uscert.gov/reading_room/distributable.html

Part 5:

Culture of Security (CS)

POLICY: *Ever more powerful personal computers, converging technologies, the widespread use of the Internet; increasing interconnectivity and connections cross national borders require that all participants who develop, own, provide, manage, service and use information systems and networks be aware of and understand security issues and take action appropriate to their role to protect cybersecurity and cyber assets. Government must take a leadership role in bringing about this Culture of Security and supporting the efforts of other participants.*

1-Goals:

CS 1.1 As part of national strategy, undertake efforts to promote a national Culture of Security consistent with UNGA Resolutions 57/239, *Creation of a global culture of cybersecurity*, and 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*.

2-Actions:

CS 2.1 Implement security plan for government owned and operated systems and networks.
CS 2.2 Implement security awareness programs and initiatives for users of government systems and networks.
CS 2.3 Develop Culture of Security outreach partnerships with business and industry.
CS 2.4 Support outreach to civil society with special attention to the needs of children and individual users.
CS 2.5 Enhance S&T and R&D activities.

3 – Dialogue and Training Resources:(*available from the U.S. or internationally*)

CS 3.1 Government systems and networks (CS 2.1, 2.2)

- The U.S. Federal Information Security Management Act of 2002 (FISMA) http://csrc.nist.gov.sec-cert/index.html
- HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection"
- Federal Acquisition Regulation (FAR), parts 1,2,7,11, and 39.
- The National Strategy to Secure Cyberspace: http://www.dhs.gov/interweb/assetlibrary/national_Cyberspace_Strategy.pdf
- US CERT site: http://www.us-cert.gov/
- NIST site: http://csrc.nist.gov/ and http://csrc.nist.gov/fasp/ and http://csrc.nist.gov/ispab/

CS 3.2 Business and private sector organizations (CS 2.3, 2.5)

- National Cyber Securitiy Partnership: www.cyberpartnership.org
- US CERT: http://www.us-cert.gov/
- DHS/Industry "Cyber Storm" exercises: http://www.dhs.gov/dhspublic/display?content=5410
- DHS R&D Plan: http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf
- President's Information Technology Advisory Committee report on Cyber Security research priorities: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

CS 3.3 Individuals and civil society (CS 2.4)

- Stay Safe Online: http://www.staysafeonline.info/
- US CERT: http://www.us-cert.gov/nav/nt01/
- OECD's Anti-Spam toolkit, www.oecd-antispam.org
- See also: The USG response to the OECD questionnaire on implementation of a Culture of Security (DSTI/ICCP/REG(2004)4/Final). Provides a comprehensive outline of USG efforts in this area. Available together with responses from other OECD countries at the OECD security web site: http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase
- New Zealand: www.netsafe.org.nz
- Canada: www.psepc-sppcc.gc.ca

May 16, 2006

Key U.S. Participants:

Government:

Department of State
Office of Coordinator for International Critical Infrastructure Protection
Bureau of Political- Military Affairs
Function: The Department of State leads federal efforts to enhance international cyberspace security cooperation and serves as an initial point of contact for contact with the USG.

Department of Homeland Security
National Cyber Security Division (NCSD)
Function: The NCSD is responsible to identify, analyze and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning.

Department of Justice
Computer Crime and Intellectual Property Section (CCIPS)
Criminal Division
Function: CCIPS is the 24/7 contact for international computer crime cases and other investigations involving electronic evidence and is also responsible for the same matters domestically. CCIPS also addresses domestic and international computer crime and critical infrastructure protection policy matters, including in multilateral groups.

Department of Commerce
National Telecommunications and Information Administration (NTIA)
Function: The NTIA carries out the Department's responsibilities for the economic security component of CIP and works with another Commerce agency, the National Institute of Standards and Technology (NIST), on international cooperation regarding security standards.

INDUSTRY:

Information Technology Association of America (ITAA):

About: The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 325 corporate members throughout the U.S., and a global network of 70 countries' IT associations. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection,

telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, digital content, systems integration, telecommunications, and enterprise solution fields. For more information visit www.itaa.org. 1401 Wilson Boulevard, Suite 1100, Arlington, VA 22209

The SANS Institute
www.sans.org

About: SANS is one of the largest sources for information security training and certification in the world. It also develops, maintains, and makes available at no cost, a collection of research documents about various aspects of information security, and operates the Internet's early warning system - Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Many SANS resources, such as the weekly vulnerability digest (@RISK), the weekly news digest (NewsBites), the Internet's early warning system (Internet Storm Center), flash security alerts and more than 1,200 award-winning, original research papers are free to all who ask.