Philippine National Cyber Security Plan 2005

EXECUTIVE SUMMARY

The initiative to formulate a National Cyber Security Plan is part and parcel of the current national effort to address critical infrastructure protection concerns. It forms part of the National Critical Infrastructure Protection Plan (NCIPP) which outlines the strategies and programs to be pursued in protecting the nation's critical infrastructures.

This Plan addresses the cyber aspect of critical infrastructure protection. While it focuses on the nature and characteristics of information and communication technology it takes into account important physical aspects and dimensions of critical infrastructure protection to achieve more effective measures to respond to the challenges of cyber threats.

In formulating this Plan, it was deemed necessary to determine the nature and characteristics of the Philippine Cyberspace. Here, it is defined as the total apparatus (elements and systems) that enables people and network/computer systems to communicate with each other. It is the space where information is posted, exploited, manipulated, traded, accessed and created by the interaction, communication and collaboration of people and organizations via the network of information and communication system infrastructures.

The components of the Philippine Cyberspace include (1) Enterprise Networks/ Intranets, (2) Local Internet Service Provider (ISP), (3) Regional Network Providers (RNP), (4) Internet Backbone, (5) User Services, (6) Online Content, (7) Source of Online Content, (8) End-Users, and (9) Telecommunication Services.

The cyberspace continues to face a myriad of challenges. These challenges include threats in the form of events, situations and conditions that tend to disrupt, degrade and destroy cyber infrastructures. Generally, threats originate either from accidental and deliberate sources such as (1) accidents and malfunctions, (2) hacktivism, (3) cyberterrorism, (4) information warfare, (5) foreign intelligence, (6) technoterrorism, and (7) cybercrimes.

This plan is also consistent with our existing international commitment with the United Nations, APEC and the ASEAN where each member state or economy agreed to jumpstart collective efforts to secure the cyberspace against terrorism.

The primary goals of this Plan include: (1) assuring the continuous operation of our nation's critical cyber infrastructures, (2) implementing capacity-building measures to enhance our ability to respond to threats before, during and after attacks, (3) effective law enforcement and administration of justice, and (4) a cyber security-conscious society.

There are four (4) strategies identified which are necessary to protect critical cyber infrastructures namely: (1) Understanding the Risk, (2) Controlling the Risk, (3) Organizing and Mobilizing for Cybersecurity, and (4) Institutional and Policy Build-Up. Each strategy has specific programs to be implemented.

In general, this Plan seeks to institutionalize the necessary capabilities in the government and in the private sector to adequately meet and respond to challenges and threats against cyber infrastructures that are critical to the national way of life and well-being.

Protecting the future is the primary responsibility of each and every Filipino today. If the Philippines intends to join the ranks of nations that have become information-based societies, security of the of the nation's digital infrastructures cyberspace must be pursued with urgency. It should be made a vital component of the over-all strategic, operational and tactical priorities of our national security

strategy
.

INTRODUCTION

Consistent with the President’s agenda of national development through the utilization and development of information and communication technology, is the protection of digital infrastructures which should be pursued urgently. The importance of information and communications technology (ICT) is underwritten in the fact that it has been identified as the "foundation of the Philippine’s future economic development."

ICT has become an integral component in the operation and management of the economy and government. ICT is important to our nation’s capacity to carry out information-based public and private enterprises. Most of these information-based enterprises like those telecommunication companies, banks, transportation and government agencies among others are considered as critical infrastructures. The importance of ICT is also underscored by the fact that mutual dependencies and interconnectedness among the various critical infrastructures are enabled through ICT, or sometimes referred to as digital or cyber infrastructures.

Digital infrastructures are the platforms through which the Philippine cyberspace spans. It is utilized by economic enterprises to improve productivity, hasten delivery of products and services, and increase competitiveness. They are also used extensively not only to facilitate the exchange and delivery of information such as those spanning a wide range of resources for research, education, entertainment, etc., but also those that involve crucial public services and government functions.

Our dependence on ICT, however, has opened up vulnerabilities that can be exploited by criminals and terrorist organizations and other forms of malicious exploitations and lawless activities. The successful exploitation of these vulnerabilities can cause tremendous damages and major disruptions to the normal operation of the economy and government, thereby posing serious implications to national security and to the welfare of our people.

While ICT provides opportunities for national development, it also brought along new kinds of threats that challenge national interest and security. ICT has also become a weapon or new ways and means to wage wars and perpetrate crimes and terrorism.

This plan is a response to these challenges. It shall be called the National Cyber Security Plan (NCSP), and will form part of the National Critical Infrastructure Protection Plan (NCIPP) to protect our critical cyber or digital infrastructures, referred to in this volume as the cyber aspect of critical infrastructure protection. It will serve as the guide upon which our actions will be based to help assure the resiliency of our critical infrastructures.

While it can stand as a separate program, the NCSP shall support and enhance the physical aspect of critical infrastructure protection. It will address the information and communication technology security or cyber security requirements of critical infrastructures.

The NCSP outlines the strategies and programs necessary to protect the nation’s critical cyber infrastructures. It highlights the necessary and specific cyber security measures in accordance with the strategies, guiding principles and basic framework set and defined in the NCIPP.

As recognized in the NCIPP, the protection of critical cyber infrastructures necessitates the need to implement the concept of “shared responsibility” that requires coordination, cooperation and collaboration between the private and the public sectors. Nonetheless, it still falls to the government the primary task of creating a conducive environment for the protection of critical cyber infrastructures.

PART ONE - DEFINING THE CYBERSPACE

The formulation of plans and strategies to secure the cyberspace is hinged upon the proper understanding of the nature and characteristics of our cyber or digital infrastructures. Thus, this section shall provide an brief description and importance of the cyberspace.

I. THE PHILIPPINE CYBERSPACE

At present, the term cyberspace is conventionally described as “the non-physical terrain created by computer systems.” In technical terms, cyberspace consists of computer networks as well as the worldwide network of computer networks that use the Transmission Control/Internet network protocols to facilitate data transmission and exchange. Cyberspace is differentiated from physical space such that the latter refers to an aspect of reality visible to the naked eye, while the former refers to an ethereal reality in which information in the form of communicated messages coexist and are transmitted. Cyberspace, therefore, should not be confused as being imaginary; it is real and exhibit physical reality through servers, routers, cables, switches, computers and electronic messages.

For the purposes of this Plan, cyberspace is the consequence of the operation of the total apparatus (elements and systems) that enables people and network/computer systems to communicate with each other. These apparatus are called information and communication system infrastructures. Hence, the protection of cyberspace requires securing this “total apparatus”.

Cyberspace resides in the information and communication system infrastructures of Internet Service Providers (ISPs), gateways, independent networks of corporations, and telecommunication companies represented by domain names, Internet Protocol (IP) addresses, MAC addresses, e-mail addresses and telephone numbers. These stress the inextricable importance of the physical components (hardware) in the protection of the Philippine Cyberspace.

The Philippine Cyberspace is therefore the space where information is posted, exploited, manipulated, traded and accessed, created by the interaction, communication and collaboration of people and organizations via the network of information and communication system infrastructures. It is a consequence of the use of these networks of physical infrastructures. Today, they are now called digital or cyber infrastructures.

II. SIGNIFICANCE OF THE DIGITAL INFRASTRUCTURES

Digital infrastructures are the platforms to the Philippine Cyberspace which are critical for key social, political, military and economic functions such as the managing, and operating of the country’s power plants and dams, the electric power grid, the transportation and air traffic control systems including financial institutions. They are also vital in the day-to-day operations of business, government and non-government institutions. Business establishments, large and small, rely on them to manage communication and payroll, track inventory and sales, as well as perform research and development functions, generate food production and many others. Digital infrastructures are keys to our nation’s capacity to carry out information-based public and private enterprises. Most of these information-based enterprises are considered critical infrastructures vital to the operation of the government and the economy.

Critical infrastructures have been revolutionized by advances in information technology in the form of digital infrastructures. Taking advantage of the speed, efficiency and effectiveness of computers and digital communications, all critical infrastructures are now increasingly being connected and interdependent.

Over the years, the reliance of critical infrastructures on digital infrastructures has tremendously increased to cope with the demand for better business processes and competitiveness aside from better public service and national security. Today, digital infrastructures are crucial for banking, local and international communication services, generation and distribution of water and power, production and distribution of good and services, transportation and travel, entertainment, security, education and many other applications that have changed the way we do things as individuals or organizations. With the rapid increase of digital infrastructures, they are now considered as strategic resources and assets that play an important role in the nation's economic development and competitiveness, security and well-being. Their disruption or destruction will have debilitating impacts to national security.

III. COMPONENTS OF THE PHILIPPINE CYBERSPACE

Basically, the components of the country's cyberspace are those digital infrastructures that interconnect national, regional and global information and communications networks. These components are identified as follows:

1. Enterprise Networks/ Intranets

Enterprise Networks or intranets pertain to independent networks, local area networks (LAN) and wide area networks (WAN) that are connected through the telecommunication channels. Said networks cater to their organization's business applications, critical infrastructures included.

2. Local Internet Service Provider (ISP)

These are organizations that provide gateways between packet-switching networks and Public Switching Telephone Networks (PSTN). These are networks through which most customers gain access to the Internet using telephone lines. They are sometimes referred to as second level ISP's. Examples of these are Infocom, Mozcom and Pacific Internet.

3. Regional Network Providers (RNP)

These entities provide WANs across large geographic areas. They function as client/server systems integrator, value-added reseller, and/or provider of Internet services to a wide geographic market.

4. Internet Backbone

Composed of organizations that provide major interconnection between different networks, they consist of:

♣ Network Service Providers (NSP) – These are organizations that provide the foundation of the Internet backbone, which is largely based upon the architecture of the Internet's precursors. Considered as peering centers, NSP offers national and international interconnecting Internet services to wholesale level RNPs and large ISP's through so-called priority Network Access Points (NAP).

♣ Network Access Points (NAP) – Network Access Points offer a mechanism for NSPs and ISPs to interconnect. Collectively, they operate as the Public Internet Backbone that connects to ISPs, POP and hosts.

♣ Long Distance Carriers – They supply a national network of communication channels for the Internet and long distance voice and data communications. In general, the NAPs contract the long distance carriers for the channels needed for their backbone.

5. User Services

These are organizations that provide domain names, email hosting, newsgroups, telnet, FTP, and storage.

6. Online Content

These are information resources that are published in websites and stored in databases of ISP's and and organizations that own them..

7. Source of Online Content

Sources of Online content are materials where information or data are generated and transformed into digital form. They include books, files, pictures, recordings, video financial data and etc.

8. End-Users

End-users pertain to people and organizations that utilize the network for their personal and business purposes.

9. Telecommunication Services

These are comprised of the facilities that provide connection of communication channels to ISP's, independent networks, and individual subscribers and users.

PART TWO:
CHALLENGES IN CRITICAL CYBER INFRASTRUCTURE PROTECTION

The Philippine cyberspace is challenged by a myriad of threats each day. These challenges, both actual and potential, brought unprecedented reshaping to our national security preparations and requirements. Enhancing our country's ability to understand and recognize these challenges is necessary in order to adequately manage the growing threats to our critical infrastructure

I. CATEGORIES OF CYBER THREATS

Cyber threats are events, situations and conditions that tend to reduce, disrupt, degrade and destroy digital infrastructures. Generally, threats originate either from accidental and deliberate sources.

In general, accidental causes are natural (e.g., a lightning surge that destroys a power supply in a network that causes part of the network to fail) or human but non-deliberate (e.g., faulty design, usage of infested media or accidental cutting of data cables). Accidental causes may also be attributed to situations that directly relate to safety, reliability and trustworthiness.

Deliberate problems are the result of conscious human behaviour. In dealing with deliberate problems, one is faced with malicious intent. A malicious human may seek to hide his or her tracks, making it difficult to identify the nature of the problem caused (or even to identify that a problem has been caused). A malicious human can, in principle, tailor actions to produce a desired effect beyond the damage to the actual system attacked -- unlike an accidental problem whose effects are randomly determined.

There are seven (7) more specific categories of threats to the cyberspace. These are accidents and malfunctions, hacktivism, cybercrimes, techno-terrorism, cyberterrorism, foreign intelligence and information warfare.

1. Accidents and Malfunctions

This category includes operator error, hardware malfunctions, software bugs, data errors, damage to physical facilities, inadequate system performance and system malfunctions. An example of this is the famous Y2K or millennium bug. Occurrences of these threats are attributed to disaster, calamities, and lack of knowledge, as well as lack of maintenance, factory defects and faulty designs.

2. Hacktivism
Considered as the marriage of hacking with activism, it covers operations that use hacking techniques against a target Internet site with the intent of disrupting normal operations but without causing serious damage. It also includes electronic civil disobedience, which brings methods of civil disobedience to cyberspace like virtual sit-ins and blockades, automated e-mail bombs, web hacks and computer break-ins including the use of malicious codes.

3. Cyberterrorism

The exploitation of digital infrastructures for terrorist ends, it comprises of politically-motivated hacking operations designed to cause grave harm such as loss of life or severe economic damage. An example would be an intrusion into an air traffic control system and causing two planes to collide.
4. Technoterrorism

This is the intermediate step between "conventional" terrorism and "cyberterrorism." Unlike the cyberterrorist, the technoterrorist will attack those systems that exist in the physical world to disrupt cyberspace. Thus, the computer itself (hardware rather than software) is the target of the technoterrorist. The technoterrorist will use "conventional" weapons such as bombs and physical destruction to disable or destroy digital infrastructures.

5. Information Warfare

Defined as being concerned “with the defensive and offensive use of information and information systems to exploit, corrupt, or destroy an adversary’s information and information system while protecting one’s own.”47 Winn Schwartau, a pioneer on the topic of information warfare has developed three classes: personal information warfare which is characterized by the electronic attack against an individual’s privacy; corporate information warfare where corporations use information and its associated technology to destroy or win against their competitors; and, global information warfare which targets entire industries, nations and global economic forces.

6. Foreign Intelligence

The cyberspace is a potentially lucrative source of strategic and competitive intelligence that can be collected by intelligence agencies of governments and their military and police organizations. Intelligence that can be collected in the cyberspace include reports on current events, analytic political and economic assessments and plans, as well as programs and operations of government, political organizations, non-government organizations/people's organizations (NGOs/POs) and business organizations. It encompasses monitoring, eavesdropping and interception of communications or electronic messages.

7. Cyber Crimes

Synonymously referred to as computer crimes, they are characterized by hacking or unauthorized access to computer systems or networks, or forcibly taking over a computer network to destroy and/or modify data and programs including stealing information that can cause disruption to the network. Reasons may vary from personal gains to political reasons. Cyber crimes include theft, sabotage, vandalism, cyberstalking, child pornography, copyright violations, piracy, trademark counterfeiting, Internet fraud and others.

Likewise, acts which disrupt or interfere with the normal conduct of transactions over the cyberspace are regarded as cyber crimes. According to the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, in Vienna on April 10-17 2000, Cyber crime is defined as "any crime capable of being committed in an electronic environment, where crime refers to behavior generally defined as illegal or likely to be criminalized." Specific cyber crimes have already been identified by the international community as well as the Philippine legislative body, and will be elaborated in the latter parts of this section.

II. TOOLS FOR CYBER ATTACKS

In carrying out these threats, several tools and weapons are used by perpetrators of cyber attacks. The following are some of the most commonly known tools:

1. Back Door / Trap Door

This is a set of instructions that permits an unauthorized or authorized user to bypass the system's security measures (usually a network firewall), usually referred to as backdoor entrances.
These program codes are placed by developers and vendors to make it easier for them to modify or repair system parameters. Because they are usually compromised, they are used as entry points for hacking. These can also be program codes that have been planted by an attacker into a computer system's firewall in the form of a trojan horse. The Trojan horse acts as a slave waiting for a command to be executed and controlled remotely by a master (usually the attacker).

2. Trojan Horses

These are programs that appear to be valid and useful but usually contain hidden instructions that can cause damage to the system. A destructive software that disguises itself as a benign application, they are usually utilized in order to place a backdoor/trap door into a compromised system.

3. Virus

This is a special type of Trojan horse that can replicate itself and spread, just like a biological virus, causing damage to a computer system or network. Depending on the author's motive, a program infected with virus may cause damage immediately upon execution, or it may wait until a certain event has occurred, such as a particular date, time or command. It should be noted that computer virus infection is increasing by 47% per year perpetrated by hackers who maintain 30,000 hackeroriented sites on the Internet.

4. Logic Bomb

This is a type of Trojan horse whose destructive actions are set to occur when a particular condition occurs, such as reaching a particular clock-time of the initiation of a particular program. Logic bombs are sometimes used for computerized vandalism and revenge. They are designed to go off long after the programmer has left the organization.

5. Worm

A worm is a program that replicates itself via a permanent or dial-up network connection. Unlike a virus, which seeds itself within the computer's hard disk for file system, a worm is a self-supporting program. It can also be used to spread time bombs, viruses Trojan horses and etc.

6. Packet Storming

This is a form of attack that involves the flooding of ports with large number of packets with the intent to deny service to the network. It can be repeated in rapid fire succession generating enough traffic to shut major networks. This is sometimes called the "smurf attack".

7. E-mail Bombs

More commonly known as email spamming, this is the bombardment of email accounts with thousands of messages, distributed with the aid of an automated tool, causing a recipient's incoming email box to jam.

8. Packet Sniffing

These are program utilities that easily permit unauthorized persons to capture packet data and examine this data. Sniffers monitor network data and can be a self-contained software program of hardware devices which usually act as network probes or "snoops" examining network traffic but without intercepting or altering it.

The two kinds of packet sniffing are PASSIVE and ACTIVE. Passive sniffing is usually done in a local area network environment within the same subnet while ACTIVE sniffing is done in a larger-scale environment, usually over a routed wide-area network.

9. Software Robots

These are programs that automatically traverse the web's hypertext structure designed to retrieve documents from a site, and reference all documents in a recursive manner. Sometimes called web wanderers, crawlers or spiders,

software robots are usually used to carry out search tasks but they can also be designed to steal information, destroy data, violate copyright or strain resources on another site and also overload networks and servers.

10. Chipping

This pertains to the installation of microchips in the production of integrated circuits by manufacturers that can be used for sabotage, by serving as control and locator for some future undertaking.

11. Nano-Machines and Microbes

These are tiny robots that are smaller than ants and are used to attack computer hardware by crawling and entering computers through slots and shutting down electronic circuits. A special breed of microbes can also be used to destroy integrated circuits.

12. Electronic Jamming

This is the deliberate radiation, re-radiation and reflection of electromagnetic energy for the purpose of disrupting or prevent the use of electronic devices, equipment, or systems.

13. High Energy Radio Frequency (HERF) Guns–EMP Bombs

HERF guns are radio transmitters that can shoot a high-power radio signal at an electronic target to disable it. EMP bombs are weapons that use electromagnetic pulse that can be detonated near electronic devices. It can destroy all computer and communication systems in a large area.

14. Distributed Denial of Service (DDoS)

DDoS attacks employ armies of "zombie" machines that are controlled by a single master server. These machines will then inundate a target server with thousands of packets of data, in an attempt to overwhelm the server and cause it to crash.
DDoS attacks have always been a tool of choice for attackers in taking down entire networks.

15. Steganography

Steganography is simply taking one piece of information and hiding it within another picture or document. Computer files such as images, sound recordings, and disks contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information like encrypted mail, for instance.

Cyber terrorists can use information-hiding to assist them in their plot to destroy infrastructures and cause damage to key government sites and services. These attackers can embed full messages and communications inside pictures that people would never suspect. Information-hiding can also be used for hiding Trojans, spreading viruses, concealing backdoors, hiding destructive wiping programs, imbedding links, and passing secret information.

III. MODES OF OPERATION

The usual modes of operations are the following:

- Hacking is defined as the unauthorized access to a computer system to gain knowledge about a particular computer system and how it operates.

- Cracking, on the other hand, is the unauthorized access to computer systems to sabotage, steal information, and modify data or congest information traffic into the computer network for personal or political gains.

- Phreaking is the unauthorized entry to or hacking of a telecommunication system in order to gain access to a telephone line or make free calls. It is also a means to gain control of a phone switch in order to add additional phone lines and modify billing information.

IV. POTENTIAL THREAT SOURCES

Threats to critical cyber infrastructure will increase as development of these infrastructures also progresses. These threats may come from a variety of sources which may be either internal or external to the cyber infrastructure per se.

Threat sources include, among others:

- Nations (hostile or non-hostile) - for economic, political and security reasons
- Foreign Intelligence Service – for information superiority through collection of strategic intelligence and information warfare
- Business Competitors – for competitive advantage through industrial espionage and competitive intelligence
- Terrorist Organizations – for disruption and destruction through cyber terrorism among others.
- Organized Crime Groups – for personal and organizational gain through all forms of cyber crimes
- Insiders – for revenge or economic gain through sabotage and theft

V. VIEW OF THE THREAT

Threats to critical cyber infrastructure will rapidly increase in terms of frequency and lethality as development and use of these infrastructures also increases. The US Department of Defense came up with a projection on how these threats will be in the future as shown in the table below:

PERPETRATOR Validated
Existence Existence
Likely but
Not validated Likely
By
2005 Beyond
2005

Incompetent
W

Hacker
W

Disgruntled Employee
W

Crook
W

Organized Crime
L
W

Political Dissidents
W

Terrorists Groups
L
W

Foreign Espionage
L
W

Tactical Countermeasures
W

Orchestrated Tactical IW
L
W

Major Strategic Disruption
L

Source: IW (Defense) by DoD, USA, 1995
Where: W – WIDESPREAD L - LIMITED

VI. MOTIVATIONS

Threat sources likewise have diverse individual and collective motivations or intentions. While some perpetrators do not intend to cause large-scale damage to cyber infrastructures, many do engage in these activities to realize political and economic ends such as achieving competitive advantage, instituting revenge, deliberately invading privacy, spreading ideologies and others.

The identification of potential threat sources and the understanding of their motivations are crucial to knowing what type of preparedness and security requirements must be organized to minimize, avert or eliminate potential exposure.

VII. INCREASING RISK

Despite the benefits, the increasing use and rapid growth of critical cyber infrastructures have amplified the risks in our national security environment.

Here are the major contributory factors why such a situation occurs despite the benefits that ICT provides:

1. Dependency – Increasing dependence on the use of information and information and communication systems for individual and corporate undertakings.

2. Interdependency – Digital infrastructures are interdependent in terms of system configurations, connectivity and applications. The failure of one digital infrastructure can cause the failure of another infrastructure or vice versa.

3. Globalization – The globalization of business operations and processes requires the need for real-time information and information resources. Inability to perform these functions can constitute substantial income and opportunity losses.

4. Standardization of Technology - Standardization of technology for interoperability and system efficiency opens up windows of vulnerabilities that will be common to all systems and to the knowledge of everyone.

5. Technology as a Force Multiplier – Information and communication technology provided equal opportunity to government, military and police organizations as well as to individuals, criminal and terrorist organizations. ICT provides the advantage of speed, stealth, wide coverage in terms of distance and target, anonymity, low cost, and high success potential among others. It only takes a personal computer connected to a network and a computer virus to inflict tremendous damage on a global scale. ICT is also an effective medium for propaganda.

PART THREE: INTERNATIONAL AND DOMESTIC CYBER SECURITY REGIME

The pervasiveness of threats to critical cyber infrastructure has long been considered an international problem. This prompted the international community to draft guidelines and implement measures to curb its increasing potential to undermine the peaceful world order. The Philippines, being a member of different international organizations, recognizes and subscribes to these guidelines as essential ingredients in its own cyber security planning and programs.

I. INTERNATIONAL REGIME

A. UNITED NATIONS

The importance of dealing with cybersecurity concerns attained international status and character owing to its pervasiveness and capability to undermine the peaceful world order. The UN General Assembly during its 81st Plenary Meeting on December 4, 2000 adopted Resolution 55/63 entitled Combating the Criminal Misuse of Information Technologies which provides among others that:

(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(i) To the extent practicable, information technologies should be designed to help prevent and detect criminal misuse, trace criminals and collect evidence;

(j) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

In a subsequent Resolution 56/121, the UN moved to invite Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, and take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

The most significant effort on the part of the UN in the area of cybersecurity was the adoption of Resolution 57/239 entitled Creation of a Global Culture of Cybersecurity during its 78th Plenary Meeting on 20 December 2002. This resolution provided an annex wherein it recognized nine complementary elements in creating a global cybersecurity culture and set Member-States' individual responsibilities. For the purposes of this Plan, extensively quoted hereunder is the content of the annex of Resolution 57/239 which enumerates the said elements.

(a) Awareness. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(b) Responsibility. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(c) Response. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(d) Ethics. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(e) Democracy. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(f) Risk assessment. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(g) Security design and implementation. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(h) Security management. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(i) Reassessment. Participants should periodically review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

B. APEC CYBERSECURITY STRATEGY

On October 21, 2001 the APEC Leaders issued their Statement on Counter-Terrorism that condemned terrorist attacks and deemed it imperative to strengthen cooperation at all levels in combating terrorism in a comprehensive manner. As part of this statement, the leaders called for strengthening APEC activities in the area of critical infrastructure protection, including telecommunications. On May 30, 2002, the Telecommunications and Information Ministers of the APEC economies issued the Shanghai Declaration that included a Statement on the Security of Information and Communications Infrastructures and a Program of Action.

The expansion and potential effects on individual member-economies of computers and information networks have made it important for them to coordinate their cyber crime and infrastructure protection efforts more rapidly and efficiently. Issues and activities in the following areas namely legal developments, information-sharing and cooperation, security and technical guidelines, public awareness, training and education and wireless security, serve as the basis for APEC's efforts on cyber crime and critical infrastructure protection. Said concerns could also form the basis of meeting the stated objectives of Leaders and Ministers.

APEC recognizes that the fight against cyber crime and the protection of critical infrastructures is built upon the legal frameworks of every economy. In particular, cyber security depends on every economy having (1) substantive laws that criminalize attacks on networks, (2) procedural laws to ensure that law enforcement officials have the necessary authorities to investigate and prosecute offenses facilitated by technology, and (3) laws and policies that allow for international cooperation with other parties in the struggle against computer-related crimes.

C. ASEAN CYBER SECURITY INITIATIVE

During the Third ASEAN Telecommunications and Information Technology Ministers Meeting (3rd ASEAN TELMIN), ASEAN Ministers, in a joint statement, vowed to enhance regional cooperation in cybersecurity. Specifically, the ASEAN members committed to establish National Computer Emergency Response Teams (CERTs) by 2005. All member countries will also, by 2004, shall have established a common framework for sharing cybersecurity threat and vulnerability assessment information. Cybersecurity expertise and information will be shared among member countries to help develop cybersecurity policies and exchange real-time information on cybersecurity issues.

II. LEGAL REGIME IN THE FIELD OF CYBER SECURITY IN THE PHILIPPINES

The government has to have laws instituted to help protect companies and consumers from abuses and to address internet security in a global context. The Philippines is governed by the following legislations pertaining to the utilization, development and protection of the Philippine cyberspace:

- Republic Act 7935 or the Philippine Public Telecommunications Policy Act enacted on March 1, 1995 which regulated the telecommunications industry in the country;

- Republic Act 8484 entitled Access Devices Regulation Act of 1998 dated February 11, 1998 which regulated the issuance and use of certain access devices. It defined access device fraud as a criminal offense;

- Executive Order No 467 dated March 17 1998 which set forth guidelines that will govern the operation and use of satellite telecommunications facilities and services in the country;

- Republic Act 8747 or the Philippine Year 2000 Readiness and Disclosure Act which was approved on June 01, 1999, setting the necessary guidelines to ensure the readiness of Philippine computer systems, products and services against the Y2K bug;

- Executive Order 269 dated January 12 2004 which created the Commission on Information and Communications Technology as the governing body in all ICT-related activities in the country.

One of the most important cybersecurity legislations in the Philippines at present is Republic Act 8792 or the E-Commerce Act which was enacted on June 14, 2000. While Section 33 of RA 8792 now lays out how hacking, cracking and piracy should be punished, the government still need to pass another law on cyber crime, cyber fraud and similar offenses.

At present the Congress still has to pass the consolidated version of four cyber crime bills (House Bill Nos. 1310, 3241, 4083 and 5560) that were filed during the Twelfth Congress. The consolidated version “AN ACT DEFINING CYBERCIME, PROVIDING FOR PREVENTION, SUPPRESSION AND IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES” OR THE CYBERCRIME PREVENTION ACT OF 2003 shall have to re-submitted to congress for enactment.

PART FOUR:
THE NATIONAL PLAN FOR CRITICAL CYBER INFRASTRUCTURE SECURITY

This National Cyber Security Plan seeks to institutionalize the necessary capabilities in the government and the private sector to adequately meet and respond to challenges and threats against critical cyber infrastructures.

Programs laying the necessary foundations to provide an assurance of continuous operation of our critical cyber infrastructures and ensure business continuity are outlined in this section.

I. CYBER INFRASTRUCTURE PROTECTION REQUIREMENTS

The nature and characteristics of cyber threats have made the challenge of protecting the critical cyber infrastructure all the more difficult for stakeholders. Meeting this challenge requires technological expertise, concerted action from national and local agencies, the private sector, the citizenry and international community. Thus, the following are necessary in order to meet such challenges:

♣ A focal point that will coordinate and integrate all efforts at the national level;
♣ Laws and regulations to control and deter cyber threats;

♣ Public-private sector and international partnerships;

♣ Well-informed and active citizenry;

♣ Effective law enforcement capabilities;

♣ Robust systems

♣ Generation of resources for sustainability of programs.

II. GENERAL DIRECTION AND GOALS

The general direction of the national cyber security plan is focused on how to achieve the following:

• Assuring the continuous operation of our critical cyber infrastructures.

• Capability-building measures to respond before, during and after attacks.

• Effective law enforcement and administration of justice

• Cyber security conscious society

III. GUIDING FRAMEWORK

1. Promoting Secure Environment

• Identification and elimination of threats. It involves knowing the threats and their effective neutralization.

• Eliminating vulnerabilities. It entails the identification and removal of weaknesses and increased level of resiliency.

- Defeating attacks. It requires the application of appropriate and adequate countermeasures.
- Reducing losses or damages. It necessitates the implementation of contingency plans and other actions to mitigate potential losses and damages.

2. Implementing a resiliency program for business continuity

3. Implementing effective law enforcement programs and proactive legal and policy regime.

IV. CYBER SECURITY STRATEGIES

There are four (4) strategies that were formulated which are necessary to protect critical cyber infrastructures: Understanding the Risk, Controlling the Risk, Organizing and Mobilizing for Cybersecurity, and Institutional and Policy Build-Up. Every strategy has corresponding programs to be undertaken.

STRATEGY 1 - UNDERSTANDING THE RISK

The most fundamental strategy in protecting the nation’s critical cyber infrastructures is to first understand the nature of threats to Philippine cyberspace. This strategy involves a national and continuing threat assessment. It also necessitates assessing the vulnerabilities of digital infrastructures given their current protective measures. This strategy also entails the need for a cyber intelligence capability as a proactive measure of understanding and overcoming these threats.

A. NATIONAL ASSESSMENT

The Assessment Program shall consist of two primary programs: the national cyber geography analysis and the risk assessment.

1. Philippine Cyber Geography Program

a. Inventory

This program calls for the identification and accounting of digital infrastructures in order to determine the extent or degree of criticality as a means to prioritize and allocate resources. This will include accounting of physical facilities, hardware, software and people.

b. Cyber-Geography

This program will undertake acquisition of knowledge pertaining to demographics, traffic, statistics and other relevant information which may be used to map out the Philippine Cyberspace for program formulation and implementation.

2. Risk Assessment

Risk assessment represents an important step in understanding the threats, vulnerabilities, countermeasures and impacts to national security. It will have the following components:

a. National Threat Assessment

National threat assessment program will be implemented to provide basis for and continuing understanding of the nature of cyber threats and how they can be addressed effectively from operational and strategic perspectives.

Likewise, a cyber or digital intelligence program will be created specifically designed for pro-active measures. It shall be accomplished to get acquainted with the hacker's world, its personalities, operations and plans.

Cyber intelligence is defined as the process of acquiring and utilizing threat-related knowledge in the cyberspace that pertains, but not limited, to the nature and characteristics of cyber threats, their modus operandis, plans, organizations, personalities and other relevant information.

b. Vulnerability Assessment

Vulnerability assessment programs shall be implemented to identify weaknesses in CI protective programs and to institute appropriate corrective measures on a periodic basis. This program will include the following:

b.1. Formulation of a Vulnerability
Assessment Framework and
Checklist

This framework and checklist shall be used to gather essential information on IT security threats and measures, critical security policies and practices on networks, systems, applications, and data and its classification, and external systems; cyber attacks and glitches experiences; and cyber attacks and glitches recovery plan.

b.2. Security audit, survey and
inspection

This will entail the conduct of a periodic security audit, survey and inspection as way to ensure implementation of security programs as well as a means to identify weaknesses.

c. Impact Analysis

It shall be implemented to determine the implications of any attack to digital infrastructures on the operations of government and the economy.

STRATEGY 2 - RISK CONTROL

Risk control requires comprehensive security planning, effective resolution of crisis and risk monitoring. This strategy shall address the aspects of mitigating or reducing vulnerabilities, likelihood of threat occurrence and potential losses or damages.

A. PREVENTIVE CAPABILITY PROGRAMS

1. Cyber Intelligence

The cyber-intelligence program will be designed to conduct intelligence operations against potential threats as a way to better know them in terms of organization, modus operandi, plans and linkages. This program shall be able to provide periodic assessment and address information requirements of law enforcement and military units in the interdiction of terrorists, spies and criminals.

This program entails the following:

a. Creation of a Cyber Special Operations Unit to be managed and supervised by TFSCI.

b. Monthly National Intelligence Estimates (NIE) that will embody strategic and operational intelligence on cyber crimes, cyber terrorism and foreign and competitive intelligence operations.

c. Development and management of a Hacker's Database

d. Development and implementation of a specialized cyber-intelligence training curriculum for the AFP and PNP intelligence training institutions. This training shall form part of the development of their cyber intelligence capability.

2. Warnings & Advisories

This program seeks to provide necessary information on threats and security alerts and other related matters to all critical infrastructure owners and operators and the general public in order for them to take precautionary measures as well as strengthen their security measures. These warnings and advisories shall include computer attack information, trends or modus operandi, wanted cyber criminals and terrorists and updates on patches and protective measures among others.

B. PROTECTIVE CAPABILITY PROGRAMS

1. Building Robust Systems

Building robust systems that will eliminate redundancies as well as back-up systems that can withstand attacks. It shall embrace the adoption of reconstitution and rehabilitation measures to ensure immediate recovery from attacks. Also included is the implementation of a comprehensive ICT security programs covering robustness in terms of system design, security systems, personnel and physical security, information and document security among others.

This shall also incorporate the formulation and issuance of security standards that can help in guiding IT security managers.

2. Intrusion Detection

This program envisions monitoring intrusions as a way to arrest or prevent the occurrence of an attack. This will be a function of the RP-CERT, Regional/Sectoral CERTs and monitoring points.

3. Operations Security (OPSEC) Program

a. Information Security Program for the government focused in the proper handling of classified and critical information

b. Implementation of an encryption system to protect critical information.

4. Security Audit

This program requires the periodic conduct of security audits for the identification of vulnerabilities, in addition to ensuring the strict implementation of security programs

5. Consumer Protection Program

This program envisions putting up mechanisms to address consumer protection issues which include the following:

a. Consumer safety
b. Consumer Education
c. Remedy and redress in case of fraud
d. Product information for choice
e. Access to products
f. Product evaluation and testing

C. RESPONSE CAPABILITY PROGRAMS

1. Establishment of Computer Security
Response Units

a. The RP-CERT

The G-CSIRT will be restructured as a national computer emergency response team and will be renamed RP-CERT. It shall be a public-private partnership to protect the nation's cyber critical infrastructures. Besides recovery and reconstitution, the RP-CERT shall be the focal point for incident and consequence management, which embraces prevention and protection of and response to attacks against critical infrastructures.

b. Regional / Sectoral CERTS

To support the RP-CERT, this program entails the establishment of regional or sectoral computer emergency response teams across the country which will enable faster and more localized response to cyber incidents. They may be housed in any government regional or local units as may be determined, or in designated private sector organizations that have the capability to undertake this program.

These regional sectoral CERTS shall serve as immediate points of contact for government agencies, local government units and private sector entities. It shall coordinate with the RP-CERT for purposes of monitoring and coordination of responses.

c. Establishment of Cyber Crime
Complaint Center (C4)

This program envisions to provide a mechanism to receive and develop Internet-related criminal complaints and refer the same to law enforcement agencies for any investigation they deem to be appropriate. A website shall be developed and maintained as the primary complaint reporting nexus.

D. ENHANCEMENT OF LAW ENFORCEMENT CAPABILITY

1. Cyber Cops

This program projects enhancing the current law enforcement capability of the PNP and NBI. It shall be able to deploy at least 1 or 2 forensic investigators and incident responders in every provincial and regional command and office of the PNP and NBI. It shall provide local and international trainings on forensic and investigation, incident response, preservation of evidence, data recovery/retrieval and analysis, digital intelligence and other relevant courses.

2. Establishment of National Forensic Laboratory

This program seeks to establish a decent national forensic laboratory that will be called the National Computer Forensic Laboratory (NCFL), serving as a processing laboratory and center for computer crime evidence repository. It shall provide support to law enforcement operations in addition to conducting training on computer forensics and investigation.

3. Establishment of Regional Forensic Laboratory

This program aims to establish strategic regional forensic laboratory that can provide localized support for law enforcement units.

4. Capacity-Building for Judges and Prosecutors

This program is centered on providing trainings for judges, prosecutors and lawyers to help them in the effective handling of cyber crimes and in the administration of justice.

E. BUSINESS CONTINUITY / RESILIENCY PROGRAM

This program endeavours to provide measures and mechanism to mitigate losses/damages and allow critical infrastructures to recover and reconstitute immediately to arrest further disruption in their operations.

1. Establishment of Corporate Disaster and Recovery Plan

This requires all CI’s to craft and adopt a Corporate Disaster and Recovery Plan which will define contingency measures in case of attack or disaster aside from outlining immediate recovery and resumption procedures for their normal operations.

This plan should include:

a. Redundancy and back-up systems

b. Rapid Assessment of attack and extent of damages, determination of vulnerabilities exploited and conduct of rehabilitation procedures to avert or deter similar attacks previously experienced by the system

c. Adoption of standard operating procedures, techniques and tools for common cyber security problems.

d. Establishment of a coordination mechanism with RP-CERT and law enforcement units.

F. REMEDIATION PROGRAM

This program is focused on developing security remedies and solutions to cyber attacks through private sector partnership. This will require the participation of competent business, educational and other relevant organizations and institutions to provide support and solution during and after cyber attacks.

STRATEGY 3 - ORGANIZATION AND MOBILIZATION FOR CYBER SECURITY

This strategy requires the organization and mobilization of human, financial, and relevant resources for implementing the National Cyber Security programs. Mobilization, as used in this section, involves not only the determination of roles or functions each stakeholder or partner has to play but also setting up mandates and responsibilities that will form the basis of such roles. Cybersecurity, being the indispensable component of critical infrastructure protection, draw strength from each stakeholder's recognition of the urgency and immediacy of their active participation.

A. ESTABLISHMENT OF A FOCAL POINT

The TFSCI will serve as the focal point for all policy and convergence effort and shall lead in the formulation and implementation all national cyber security programs and other related program.

B. CREATION OF A NATIONWIDE MONITORING POINTS

The establishment of monitoring points that will serve as listening posts for intrusions requires that they be set up at strategic points around the country. They will detect, gather and help analyze information with regards to cyber threats. Envisioned as a public-private sector partnership, it will give the nation a clear picture of the threat situation in the Philippine cyberspace.

C. PUBLIC AND PRIVATE PARTNERSHIP / COOPERATION

1. Public-Private Partnership Forum

This program seeks to establish a strong public-private sector partnership forum on cyber security by requiring the mobilization and cooperation of the private sector, especially the owners and operators of critical infrastructures as well as the industry associations. This partnership shall include among others sharing of information and expertise.

Public –private partnership shall be in the form of:

a. Capacity-Building
b. Information-Sharing
c. Threat Assessment
d. Joint Management of Cyber Security Programs
e. Digital Intelligence
f. Counter-Intelligence
g. Remediation
h. Utilization of the Reserve or Auxiliary Force
i. Incident Reporting
j. Advocacy

2. International Partnership / Cooperation

This program aims to forge partnerships with foreign governments and international organizations for exchanging information, sharing of best practices, capacity-building and capability development aside from law enforcement.

D. ADVOCACY AND PUBLIC AWARENESS

This program envisions implementing a Cyber security advocacy program that will rally the general public to protect the Philippine cyberspace. This program shall specifically focus on:

1. Computer Ethics
2. Computer Security
3. Incident Reporting

The awareness program shall be incorporated in the educational curricula of DepEd and CHED and TESDA.

STRATEGY 4 - INSTITUTIONAL BUILD-UP

This strategy calls for institutional reforms that are necessary to address the challenges of cyber threats. To provide the necessary legal regime and policy environment, this demands for regulatory and legislative agenda.

A. PASSAGE OF CYBER CRIME LAW

1. The Cyber Crime Bill that will define and criminalize cyber offenses, to be certified as an urgent bill.

2. Actively lobby for the passage of the Cyber Crime Bill.

B. ADMINISTRATION OF JUSTICE

1. Creation of special court to administer cyber crimes.

2. Mandatory and continuing educational program for lawyers and judges to better equip them in the

prosecution of cyber crimes.

3. The resolution of issues and problems related to Evidence Law, or more specifically, the acceptability of electronic evidence in computer crime prosecutions.

C. SECURITY STANDARDS

1. The adoption and implementation by all government agencies and GOCC's of relevant international and local standards like the ISO 17799 and BS7799 as applicable and those promulgated by the Bureau of Standards under ISO 9001:2000 quality management systems requirements;

2. The adoption of an Information Security Management System (ISMS) as a requirement in the Integrated Information Systems Plan of each government agency.

D. EDUCATION & TRAINING

1. Training of law enforcement agencies on computer forensic and investigation and handling of digital evidences.

2. Capacity building program judges and prosecutors to allow them to effective administer justice on cyber crime related cases;

3. Integrate and institute relevant cyber security courses in government educational programs.

4 Establish partnership with foreign governments and international organizations on cyber security training.

E. KNOWLEDGE MANAGEMENT (KM)

This program is centered on adopting Knowledge Management as a way to get the right information to the right person at the right time. Existing technological innovations and best practices on cyber security have to be captured, stored, analyzed and disseminated to end-users to improve their security programs.

1. Establishment of knowledge resource centers to be used by law enforcement units, CI operators and their ICT security managers, government officials and other relevant users;

2. Establishment of linkages with international knowledge centers to facilitate exchange and sharing of cybersecurity information and the setting up of an online infrastructure to support it;

F. RESEARCH & DEVELOPMENT

This program endeavours to undertake research and development including, but not limited to, the following areas:

1. Cryptography
2. Information Warfare

3. Intrusion Detection
4. Hacking
5. Vulnerability Assessment

This shall be jointly undertaken with the private sector, with an incentive scheme to generate support from them.

PART FIVE: THE WAY AHEAD

The threats to our critical cyber infrastructures are real. The growing exploitation of information and communication technology to improve the lives of Filipinos, coupled with our increasing dependence to these infrastructures for the operation of our economy and government, poses greater risk given the threats that are inherent to these opportunities. It is therefore imperative that the protection of these infrastructures should be a strategic component in national security programs to ensure the protection of our national interests.

No feasible combination of domestic or international policy options can make us completely invulnerable to cyber attacks in the future. Nevertheless, enhancing security in our critical cyber infrastructures can prepare the country to all forms of malicious activities or threats that lay ahead in the cyberspace.

The private sector has to assume a major and supportive role in organizing and mobilizing communities, business and supportive organizations and groups towards our national goal of securing our critical infrastructures. We have to communicate and advocate for strong public support to this program by educating and partnering with stakeholders.

In today’s security environment, cyber threats whether individual, organization or nation-sponsored, are designed to cripple a nation’s capacity to carry out its information-based enterprises. Threats metamorphose faster than our capability to implement counter-measures. Being caught unprepared to meet these challenges might prove disastrous for the country.

Protecting the future is the primary responsibility of each and every Filipino today. If the Philippines intends to join the ranks of nations that have become information-based societies, security of the Philippine cyberspace must be pursued with urgency. It should be made a vital component of the over-all strategic, operational and tactical priorities of our national security strategy.

APPENDICES

APPENDIX 1 – CSWG WORKSHOP OUTPUT
APPENDIX 2 - CYSWG WORKSHOP OUTPUT

The TFSCI-CySWG Implementation Master Plan

A project of
The Task Force for the Security of Critical Infrastructure (TFSCI)
Cyber Security Work Group

Asst Sec Angelo Timoteo Diaz de Rivera
Head, TFSCI Cyber Security Work Group

28 June 2004

INTRODUCTION

Terrorism, cyber and otherwise, continues to be one of the most serious threats facing the security of countries all over the world. No country is immune to attack or exploitation by terrorists and no one can afford to retreat from the problem.

The Philippines is no exception. Its government, therefore, should step-up its defense program to safeguard the nation not only from physical terrorist attack, in general, but from cyber threats to its major, critical infrastructure nationwide.

The nation's critical infrastructures, such as: telecommunications, banking, agriculture, and industrial centers, and their mutual dependencies and interconnectedness as enabled through information and communications technology (ICT) is a prime target, vulnerable at the moment, even to the most basic of virus attacks and malicious conduct. The high dependencies of these critical infrastructures on ICT have made them highly vulnerable to the malevolent intention of lawless elements through cyber exploits and terrorism.

The threats of attacks to critical infrastructure have serious ramifications to the nation's immediate economic survival. With a new mandate from the people, the President, Her Excellency Gloria Macapagal-Arroyo, is in the best position to take the lead in recognizing the urgency and immediacy of providing a short, as well as, a long term solution to the protection of critical infrastructures and tapping both the private and public sector to collaborate in this shared national responsibility.

Through a resolution submitted during the First National Summit on Critical ICT Protection at the EDSA Shangrila on 16 April 2004, to the office of the President, through Executive Secretary Romulo, the joint public-private Task Force on Security for Critical Infrastructure (TFSCI) has put forth the development and implementation of a RP National Cyber Security Strategy (RP-NCCS) in the soonest possible time to include but not limited to the following:

a. Formulation, fast-tracking and pro-active advocacy of related regulatory and legislative agenda in order to provide the necessary legal regime and policy environment.

b. Conduct of a nationwide cyber security awareness program to promote a common understanding among stakeholders;
c. Conduct of risk and vulnerability assessment in order to identify risk areas and effect the establishment and adoption of internationally-accepted cyber security standards;
d. Institutionalization of cyber-security capability-building programs in order to produce a critical mass of RP cyber-security professionals; and
e. Establishment of a National and Sectoral Computer Security and Incident Response Team to ensure that the country is able to immediately respond to all possible forms of cyber threats and incidents.

To set the tone and initiate action, the Task Force, after a March workshop in DAP, Tagaytay agreed to pursue subsequent planning activities through the creation of five (5) planning teams.

THE CYSWG EFFORTS

In 13 January 2004, the NCC– CySWG crafted its preliminary Work Plan which was submitted and approved by the COC-IS thru the TFSCI

In this preliminary work plan the CySWG identified the following priority programs/ projects:
♣ A database of critical cyber infrastructure
♣ Establishment of national, regional and sectoral Computer Security Incident Response Teams (CSIRT)
♣ A nationwide adoption of Information Security Standards
♣ Cyber security policies and implementation plans (National Cyber Security Strategy)

On March 28-29, 2004, a CySWG organizational workshop was conducted at DAP, Tagaytay to decide on the final organizational setup, identify short and long- term programs and activities, and define functions and tasks of the various CySWG committees under the Task Force for the Security of Critical Infrastructure (TFSCI).

The following five (5) committees were formed during the DAP workshop and these were formalized at The National Security Summit held at the Shangila EDSA Hotel last 16 April, 2004. The committees are:

1. Risk and Vulnerability Assessment Committee (R/VAC)
2. Training and Education Committee (T-TRAIN)
3. Security Awareness and Advocacy Committee (SAWAT)
4. Formulation and Implementation of Cyber Security Policies Committee (FISPOL)
5. Incident Intervention and Consequence Management Committee (I-ICON)

An Oversight Committee chaired by DG Tim De Rivera was also formed to oversee and monitor the planning and implementation process to be followed by the CySWG Task Force committees.

THE 5 TFSCI-CYSWG PLANNING COMMITTEES

The various committees are depicted as shown below

The major objective and function of each committee is shown in the following table:

Committee Major Objective
FISPOL Formulate and implement policies, regulations and rules of conduct for CySWG members and affected parties or industries.
RVAC Identify and assess risk and vulnerabilities of critical infrastructures
SAWAT Promote security awareness training to ciritical infrastructure and affected publics
T-TRAIN Develop competent security professionals to protect and support cyber infrastructure
I-ICON Provide coordination, response and exchange of incident information among the various in-government, private and regional/global incident response teams on a 24x7 basis
O-OVER Oversee the planning and implementation of the various CySWG committee efforts

SUB-COMMITTEE WORK

The organizational workshop was soon followed by the following sub-committee workshops to finalize the individual sub-committee plans and programs:

♣ April 15 & 16 - to kick off the TFSCI-CSWG activities, a National Cyber Security Summit was conducted with an end view to increase awareness on the CySWG plans and programs, and to foster public and private partnership
♣ April 30 & May 1 – planning workshop at DAP, Tagaytay for the Risk and Vulnerability Assessment Committee (R/VAC)
♣ May 26 & 27 – planning workshop at Las Brisas, Antipolo for the Formulation and Implementation of Cyber Security Policies Committee (FISPOL)
♣ May 28 & 29 – planning workshop at Las Brisas, Antipolo for the Security Awareness and Advocacy Committee (SAWAT)
♣ June 15 & 16 – planning workshop at DAP, Tagaytay for the Training and Education Committee (T-TRAIN)
♣ June 17 & 18 – planning workshop at DAP, Tagaytay for the Incident Intervention and Consequence Management Committee (I-ICON)

In between, several other small group meetings took place among the various members of the committees to work on after-workshop assignments and other unfinished business as needed.

THE TFSCI-CYSWG IMPLEMENTATION PLAN

This plan therefore is a result of the planning efforts of the various committees of the Cyber Security Work Group (CySWG) under the auspices of the Task Force on the Security of Critical Infrastructure (TFSCI).

The plan is being presented as an initial working plan based on the perspective of the committee members under the influence of their respective agency training, orientation and bias. It is suggested that the plan undergo validation by the senior members of the TFSCI and from the overall view of a composite Physical Security and Cyber Security perspective. There were also the consideration of funding, executive preference, and other national prioritization issues that were not taken into account during the CySWG planning workshops.

THE CYBER SECURITY WORK GROUP (CYSWG) MISSION

To ensure that the critical infrastructure of the country is
99.9% safe and protected in cyberspace

THE CYBER SECURITY WORK GROUP FUNCTION

The information and process flow among the various CySWG functions are envisioned as follows:

CYSWG GOALS AND OBJECTIVES
The objectives, strategies and action plans submitted and recommended by the five (5) committees under the CySWG Task Force are detailed in the Appendix of this report. These are consolidated and summarized in table form in the following pages.

CYSWG OBJECTIVES, STRATEGIES AND ACTION PLAN
Objective Strategies Action Plan
I-ICON 1. To develop the country's capability to respond to computer security incidents
1.1. Set up a National Computer Security Incident Response Team (NCSIRT) Coordinating Center or a National Information Security Agency (NISA) as appropriate
1.1.1. Formalize and finalize plan for establishment of the NCSIRT center
1.1.2. Establish and set up physical and organizational office infrastructure
1.1.3. Establish and develop linkages with international CSIRTs and inhouse/incountry infosecurity units
1.1.4. Establish coordination with law enforcement agencies locally and globally (NBI, PNP, FBI, Scotland Yard)
1.2. Identify and develop capacity building programs 1.2.1. Organize and select qualified personnel
1.2.2. Identify training needs
1.2.3. Acquire necessary equipment, tools and supplies
1.2.4. Work with T-Train team to develop courseware and training mechanisms
1.2.5. Conduct continuing training and upgrading of personnel.
1.3. Adopt and adapt applicable Alert and Warning System 1.3.1. Define communication system and alert procedures
1.3.2. Set up website and other communication facilities
1.3.3. Design and establish alert procedures
1.3.4. Promote NCSIRT system and capabilities
1.4. Adopt and adapt best practice and procedures for Incident Handling System 1.4.1. Identify and benchmark applicable incident handling system to include: audit, preservation of forensic data, investigation and prosecution assistance subsystems
1.4.2. Adopt and adapt post-incident handling and analysis system

Objective Strategies Action Plan
SAWAT 2. To promote appropriate security awareness training for sectors whose mission critical systems are heavily ICT-dependent

2.1. Initially promote to primary stakeholders of selected sectors and eventually broaden coverage of security awareness program to other sectors and stakeholders 2.1.1. Determine target market and define performance indicators for measuring advocacy effectiveness
2.1.2. Identify ICT-dependent sectors
2.1.3. Tap other industry organizations to assist and support the awareness campaign (ITFP, CIOF, ISSSP, PCCI, PMAP)
2.1.4. Train and tap pool of competent SAWAT resource persons/speakers
2.1.5. Identify appropriate ICT forums and conferences to implement SAWAT programs
2.2. Use of Television, Radio, Internet and Print (TRIP) media to create multiplier effect 2.2.1. Define target market (CIOs, Users) and message content
2.2.2. Determine marketing strategy in terms of content/media mix vs. target sectors/audience
2.2.3. Develop and implement promotions advocacy campaign (plans and programs) through PIA and/or outsourced public relations agencies.
2.3. Integrate cybersecurity awareness into existing e-government projects and in basic ICT curriculum

2.3.1. Consult and plan strategy with DepEd, CHED and TESDA
2.3.2. Consult and dialogue with private ICT educational institutions
2.3.3. Issue necessary directive and guidelines to government promotions, training and development centers (PIA, DAP, NCC)

Objective Strategies Action Plan
R-VAC 3. To assess the cyber vulnerabilities of the Nation's critical infrastructure as well as those authorities responsible for the business continuity of government 3.1. Institutionalize the process of reviewing and assessing risk and vulnerabilities of cyber critical infrastructures 3.1.1. Establish RP-R/VA mechanisms, performance measures and standards
3.1.2. Conduct regular risk assessment activities and workshops
3.1.3. Monitor compliance on a continuing basis
3.2. Build up of a R/VA database 3.2.1. Determine extent and complexity of database sourcing, storage and access system.
3.2.2. Source and acquire necessary equipment, tools and technology
3.2.3. Initiate build up and propagation of database
3.2.4. Integrate system resources with I-ICON system
3.3. Adopt and adapt assessment forms and methodologies for immediate implementation 3.3.1. Source, review and benchmark existing assessment forms, methodologies
3.3.2. Consult and adapt as applicable
3.3.3. Pilot and/or implement as deemed fit.
3.3.4. Monitor effectiveness of assessment instruments and methodology.

Objective Strategies Action Plan
FISPOL 4. Formulate and implement policies, regulations and rules of conduct for TFSCI-CySWG members and affected parties and industries 1.1. Adopt and adapt best practice on policy formulation and implementation
1.1.1. Conduct survey and research
1.1.2. Establish communication exchange arrangements with other countries or cyber entities
1.1.3. Consult and draft policy manual and guidelines
1.1.4. Benchmark/validate policies with other countries' policy regime
1.2. Legislate policies and regulatory requirements where necessary 1.2.1. Identify appropriate legislative/regulatory bodies to seek support
1.2.2. Schedule action agenda and deliberations
1.2.3. Monitor progress to completion
1.3. Publish, monitor and report on policy implementation effectiveness 1.3.1. Collect related security policies issuances
1.3.2. Prepare summaries, abstracts and annotations as needed
1.3.3. Design, print and distribute materials
1.3.4. Work with SAWAT team for integration into promotions and advocacy program
T-TRAIN 5. To develop and implement responsive training programs to produce a sustainable number of Filipino cyber security experts/professionals at par with their international counterparts
5.1. Develop responsive training programs for ICT security professionals
5.1.1. Establish training center for cyber security excellence (under NCC or independent center of excellence)
5.1.2. Develop or outsource necessary courseware and equipment, tools required
5.1.3. Conduct and implement training programs

5.1.4. Partner with private training providers or vendors for more comprehensive
5.2. Establish assessment and certification program/centers for cybersecurity professionals 5.2.1. Define competence and criteria for assessment and certification
5.2.2. Establish assessment and certification process
5.2.3. Forge assessment and certification working partnerships with technology owners and providers

ORGANIZATIONAL REQUIREMENTS: HOW TO PROCEED FROM HERE

Considering that the members of the Task Force Committees consist of volunteer government and private employees who may not be available to commit their time and effort in a continuing, as-needed and sustained basis, the CySWG must convert itself or seek the set up or organization of a permanent body with an official charter. This body must, as a minimum have full-time, knowledgeable and qualified ICT professionals and managers who will polish and fine-tune the plan and carry out its implementation based on their (new people) respective capacities and capabilities. Where extra hands and know how are needed, the managers and leaders of the renewed permanent body can simply tap the talents and abilities of either the current members of the CySWG committees or outsourced to experts in the field.

All the committees agreed to the formation of a permanent body to implement the TFSCI master plan. Each member realized his role was temporary and his responsibility self-imposed, if at all. Some members have expressed their willingness to be part of the new body, if at all formed, depending on their assigned roles and individual working arrangements.

Although no formal organizational structure or composition of the new permanent organization was discussed and submitted during the various planning meetings and workshops, the consensus was that the permanent body will have to be formed depending on the political and financial situation at the time of formation.

Some functions though are critical and have to be manned by experts in these fields. The two most critical functions of the new organized permanent body (New-CySWG) are:

- Technical Training (T-TRAIN)
- Incident Response (I-ICON)

THE TECHNICAL TRAINING (T-TRAIN) FUNCTION

The T-Train function will have to be done professionally and on a continuing, sustained basis. At the moment, the necessary expertise and know how, in terms of course content and delivery mechanisms are not available in one single entity or training institution. It is suggested that the training be formalized initially under the NCC, considering that NCC already has the training facilities and the mandate to do ICT and related training.

The NCC facility can be part of the permanent New-CySWG organization until such time that the plans of NCC or the New-CySWG will say otherwise.

NCC, as the New-T-Train can now implement and upgrade the T-Train plan which includes tapping outside expertise on an as-needed basis. The first order of the day is for NCC to organize a train-the-trainor program and carry out the certification process for its newly trained ICT Security mentors and instructors.

The New-T-Train can follow the plan of action of the T-Train committee as follows:

- Identify training gaps
- Outsource and tap applicable programs/technologies, courseware and trainors
- Implement training and delivery programs

The T-Train committee has also identified as a resulting business or output, consulting, curriculum development and certification as among its potential product or services to follow. Since the critical need for the immediate time frame is for training on ICT security of government and the critical infrastructure, the auxiliary business of T-Train may have to wait and its pursuit subject to the will and wherewithal of the permanent officers or managers to be designated. Training, per se, is already a full-time job and a major undertaking concern for most managers. It will take a leader with an insatiable business sense and acumen to expand into the complex world of consultancy and courseware development as an add-on business.

For the certification, this may be better done in cooperation with TESDA and the ICT-Industry Working Group who are now in the process of professionalizing the certification so these can be brought to a stage where the industry and the business community can look at a certified ICT worker with pride and confidence rather than with doubt and distrust.

THE INCIDENT RESPONSE (I-ICON) FUNCTION

The incident response function has to be a permanent and fully funded function of the New-CySWG. This is and will be the heart of the cyber protection capability of the country. If the new I-ICON fails to beat, the whole body or network of data, information and processing of such, stops.

The I-ICON function and for that matter the task of providing response and protection to the information community is proposed by the CySWG through the creation of a National Computer Security Incident Response Team (NCSIRT). It is also referred to as the Government CSIRT or G-CSIRT. If an agency, these can be referred to as the National Information Security Agency (NISA) to encompass all forms of security issues and concerns whether LAN-based, Cyber-based or simply a corporate misdemeanor or crime against a standalone information system in a private or government enclave.

The I-ICON function is a coordination and feeding center for the country's input and output of cyber nuances. Into its bowels and veins will flow the various threats and incidents of intrusions, viruses, attacks and even simply misuse or abuse of computer use.

Contrary to the notion of border patrol and control, the I-ICON will never have direct control or supervision over any other cybersite, whether on-country or off-country. The major function and significance of a government incident response coordinating center, however, is its ability and capability to warn, monitor, and inform the cybercommunity of threats and incidents so all those within reach and coordinating with the center will be fully warned and therefore can arm themselves accordingly.

The only reason a threat or attack can materialize and succeed is when its intended target is uninformed, misinformed or incapable of defending itself. These inadequacies can be overcome by proper training and preparation and a reliable, dependable, 24x7 alert system.

THE OTHER FUNCTIONS

For the other functions, these can continue as committee work and eventually can be absorbed by the New-CySWG, G-CSIRT or NISA to be formed. Once a new set of permanent employees are employed, the other tasks and function may be relegated to inhouse experts or simply outsourced on an as needed basis.

The Risk Assessment (RVAC) function can be done on a quarterly or continuing basis by outsourced third party assessors. The New-CySWG only have to come up with standards by which critical infrastructure and institutions are to be assessed.

The Awareness function and activities (SAWAT) can be implemented inhouse or outsourced to a public relations agency, once the marketing advocacy plan is done. Marketing, and especially advocacy efforts like those required for cybersecurity are better in the hands of marketing-oriented professionals than in ICT people's hands. Technical people, and we will have the more technically inclined in the New-CySWG, will be the wrong people to advocate security. They will either scare the hell out of their constituents or droop them to sleep with their technical litanies.

Lastly, the Policies function (FISPOL) shall eventually become the responsibility of the New-CySWG management and not an adhoc committee from the outside. Once the business of the permanent organization is installed, any policy, guidelines, directions and the like, will have to emanate from the management and/or their direct superiors.

The oversight function will also have to be relinquished to the New-CySWG leadership. Theirs will be the responsibility and accountability of making this country, safely, securely and soundly functioning in LAN or Cyber space.

SHORT-TERM PLAN

For the short-term (up to the end of the year), the various committees have put up their action plans in terms of activities and deliverables. Details of these plans and activities are in the attachments. The attachments though reflect a first draft resulting from the sentiments of those who were present and participated during the workshops. Only the more implementable or doable activities were selected from the long list of recommended actions produced by the five (5) committees during their respective planning workshops.

The individual committee worksheets with all their detailed computations and assumptions are included in the hard copy outputs as well as in the accompanying CD for those who may want to review them at a later date.

RECOMMENDATIONS

From a practical perspective, there are two major recommendations, and these are:

1. Form the G-CSIRT or NISA as soon as possible. From the findings of the workshop, there is a need to formalize the creation of a “Response Team” at the least. And these team has to have the necessary mandate and authority to work with, negotiate and represent the national interest on matters of information security as a whole.
2. Formalize the development and implementation of a National Strategy for Information Security as a whole (not just Cyber Security). With the passage of the E-commerce Law in 2000 and the formation of the ITECC and the CICS, the National Strategy for Information Security will be a boon and welcomed protective mantel to the many other ICT plans and strategies adopted and adapted by the ICT community in the last decade. Cyber as well as inhouse or local information security breach can damage a business or even whole government more than it can any breach of physical security. Some companies with headquarters in the collapsed Twin Towers as a result of the 9-11 tragedy continue to do business simply they had backups and contingency provisions for their data and information systems. But no business can continue once their mass of data and their ability to process and compute is wiped out by a virus or malicious attack.

CONCLUSION

Implementing the plans and programs herein proposed or revised as needed, will require a different set of knowledge, attitude and skills set. It is recommended that the final composition of staff and / or committee members who will carry out these plans and programs be selected based on their knowledge, attitude, skills and availability to carry out plans and programs… and not just to plan!

APPENDIX 2 – SAMPLE RISK ASSESSMENT QUESTIONNAIRE

III. ORGANIZATION INFORMATION

A. Contact Information (Optional)
Respondent Name :
Email Address :
Job Function :
Name of Immediate Supervisor :
Job Function of Supervisor :
B. Organization Information

Company Name :
Address :

Sector : θ Agriculture and Food
θ Banking and Finance
θ Emergency Services
θ Energy
θ Government Services
θ Information and Communication
θ Manufacturing
θ Public Health
θ Strategic Commercial Centers
θ Transportation
θ Water Supply
In which geographic locations is the organization, or its products/services, present?

What is the main purpose or mission of your organization?

What are the products/services being offered by your organization?

How does your organization's product or services affect the people, economy, and the government?

What is your organization's gross income?

θ Less than 10 M
θ 10 M to 50 M
θ 50 M to 100 M θ 100 M to 500 M
θ 500 M to 1,000 M
θ More than 1,000 M
How many employees are in your entire organization?
θ Less than 500
θ 501 to 1,000
θ 1,001 to 2,500
θ 2,501 to 10,000 θ 10,001 to 50,000
θ 50,001 to 100,000
θ More than 100,000
Approximately, what is your organization's information technology budget for this year? IT budget covers software, hardware, implementations, salaries, consultants, and other expenses?
θ Less than 1M
θ 1M to 5M
θ 5M to 10 M θ 10M to 50M
θ 50M to 100M
θ More than 100M

Who is primarily responsible for Information Security in your organization?
θ Chief Executive Officer (CEO)
θ Chief Operating Officer (COO)
θ Chief Financial Officer (CFO)
θ Chief Information Security Officer (CISO)
θ Chief Security Officer (CSO)
θ Chief Privacy Officer (CPO)
θ Chief Risk Officer (CRO) θ General Counsel
θ Business Unit Executive/ Vice President
θ Information Technology Executive
θ Information Security Executive
θ Network/System Administrator
θ Internal Audit Director
θ Other (please specify)

IV. SYSTEM-RELATED INFORMATION
A. Data and Information
1. What are the mission critical data or information of your organization that will have a high or medium level of impact if the data or information is destroyed, altered, or compromised?
θ Customer Information
θ Financial Information
θ Sales and Marketing Information
θ Research and Development Information
θ Products and Services
θ Plans/Design Information
θ Others: ________________________________
2. What are the consequences if data or information is destroyed, altered, or compromised? θ Loss of service
θ Financial costs
θ Loss of employment
θ Legal implications
θ Loss of trust
θ Others: _________________________________
3. Does your organization have an information classification system?
Information is classified according to:
θ Sensitivity – a classification based on the nature of confidentiality of the information to determine its use and disclosure
θ Criticality - a classification based on the availability of the information
θ Guidelines for classifying information is documented
θ Procedures for labeling and handling information (storage, transmission, and destruction)according to its classification are documented and implemented
θ Responsibility for classifying information is clearly defined
θ Yes θ No
4. Does your company maintain an inventory of assets?
An inventory of the following assets are maintained:
θ Information assets, e.g.databases
θ Software assets
θ Hardware assets
θ Others: __________________________________
θ Responsibility for the maintenance of inventory records are assigned and documented
θ Yes θ No

B. Application System Information

The table provided below will be used to answer the following questions:

1. What are the mission critical application systems that process your organization’s data and information?
2. What is the purpose of the system?
3. What are the functions of the system?
4. What are the features of the system?
5. Who are the user groups of the system?
6. What are the internal and external interfaces of they system?

NOTE: Internal interfaces refer to the other IT systems within the organization that the system needs to connect with. External interfaces refer to the other IT systems outside the organization the system needs to connect with.

Application System Purpose Users Functions Features Interface/s

C. System Sensitivity and Criticality

For each of the identified mission critical systems the table provided below will be used to answer the following questions :

1. What is the sensitivity and criticality level of the information processed by the system?

NOTE: Sensitivity refers to the nature of disclosure of the information being processed
Criticality refers to the availability of the information being processed

2. What is the impact of the loss of integrity, loss of availability and loss of confidentiality of the mission critical data or systems to the security, health, safety, public welfare or economic well-being of the citizens or on the delivery of basic services of the government?

θ What is the impact of a temporary, short-term or minor disruption, destruction or breach in operations or security of the system to the security, health, safety, public welfare or economic well-being of the citizens or on the delivery of basic services of the government?

θ What is the impact of a permanent or major disruption, destruction or breach in operations or security of the system to the security, health, safety, public welfare or economic well-being of the citizens or on the delivery of basic services of the government?

3. What are the other sectors (based on the list of sectors refer to III.B) that will be significantly affected by the system?

Application System Information Sensitivity Level
(H- High,
M- Medium, L- Low) Information Criticality Level
(H- High,
M- Medium, L- Low) Impact of temporary or short-tem disruption
(H- High, M- Medium, L- Low) Impact of permanent or major disruption
(H- High,

M- Medium, L- Low) Affected Sectors

θ H θ M θ L θ H θ M θ L θ H θ M θ L θ H θ M θ L

θ H θ M θ L θ H θ M θ L θ H θ M θ L θ H θ M θ L

θ H θ M θ L θ H θ M θ L θ H θ M θ L θ H θ M θ L

θ H θ M θ L θ H θ M θ L θ H θ M θ L θ H θ M θ L

θ H θ M θ L θ H θ M θ L θ H θ M θ L θ H θ M θ L

D. Technical Infrastructure

Answering the following questions below shall attempt to establish the following:
a. Identification of different operating systems that host corporate application systems
b. Identification of hardware components that are used to support the system
c. Identification of network infrastructure media that are used to support the system
d. Identification of other facilities that the system depends on

1. What types of hardware are being used to support the organization's critical applications? (Check all that apply) θ RISC-based
θ Intel-based
θ Mainframe
θ Citrix Metaframe
θ Others: ______________________________

2. What operating systems are used to host the organization's critical applications? (Check all that apply) θ Solaris
θ Windows
θ Linux
θ Unix
θ MAC OS
θ MS-DOS
θ IBM OS
θ Others: ______________________________

3. What network infrastructure media are used to support the Company's application systems? (Check all that apply.) θ LAN/WAN
θ Unshielded twisted pair
θ Shielded twisted pair
θ Coaxial cable
θ Fiber Optics
θ Wireless
θ Others: ______________________________

4. What are the other support infrastructures/ facilities that the system depends on? (ex: external telecommunications systems, Internet, water system, etc) θ Please specify:

5. Generally, what security technologies are utilized in your organization? θ Digital Ids
θ Intrusion Detection
θ PCMCIA
θ Physical Security Controls
θ Encrypted Login
θ Firewalls
θ Reusable Passwords
θ Anti-virus Software
θ Encrypted Files
θ Biometrics
θ Access Control

V. SECURITY / CONTROLS ANALYSIS
A. Management Controls
6. Does your organization have information security infrastructure?
θ There is an IT security document that states the organization's security vision, mission, and security management structure
θ Information security roles and responsibilities are defined, documented, and address separation of duties
θ The management provides visible support for security initiatives
θ A committee exists to provide oversight for the security function
θ A security contact has been designated for the organization
θ Yes θ No
7. Does your organization have information security policies?
θ A central person/group maintains, reviews, and updates information security policies (i.e. security officer, security department, security committee)
θ Security policies are reviewed on a periodic basis:
Every __________ month(s)
θ Security policies are published and made available to users
θ The following areas are addressed in documented security policies:
θ Business Continuity Management
θ Change Control/Management
θ Computer and Network Management
θ Electronic Access Control
θ Email Usage and Protection
θ Encryption
θ Incident Response
θ Information Asset Classification and Data Protection
θ Internet Usage
θ Password Management
θ Personnel Security and Hiring Standards
θ Physical Access
θ Privacy and Confidentiality
θ Remote Access
θ Security Assessment and Compliance
θ Security Awareness

θ Systems Development and Maintenance
θ Vendor/Third Party Management
θ Web Application Security
θ Virus Protection
θ Yes θ No
8. Does your organization follow laws, international standards, best practices, or frameworks for implementing information security?
θ ISO 17799 (Code of practice for information security management)
θ COBIT (Control Objectives for IT)
θ Common Criteria for IT Security
θ ITU (International Telecommunication Union)
θ NIST (National Institute of Standards and Technology)
θ TSSIT (Technical Security Standards for IT)
θ E-commerce Law
θ Others: ____
θ Yes θ No
9. Does your organization practice standard system name conventions?
Standard naming conventions are utilized for:
θ Servers
θ Workstations
θ Usernames accounts and groups
θ Yes θ No
10. Would your organization consider hiring reformed hackers as consultants? θ Yes
θ No
11. Does your organization have a program for reviewing and testing security controls?
Program includes:
θ Internal Audit
θ External Audit
θ Security Consulting
θ Others: ______________________________________
θ Security assessments are performed at least once a year
θ Security assessment procedures and methodologies are documented
θ Access to security testing tools and utilities are restricted to authorized personnel
Security assessments include:
θ Security specialists to perform penetration testing
θ Vulnerability scanners
θ Policy compliance checking tools
θ Performance tools
θ Independent review and audit of security policies and controls
θ Yes θ No

B. Operational and Technical Controls
1. Does your organization have personnel security measures with respect to security?
θ Staff are aware of their security responsibilities via details in their job descriptions
θ Job applicants' claims of previous experience, qualifications and identity, and character references are verified
θ Employees and contract staff are required to sign confidentiality or non-disclosure agreements upon employment
θ Access privileges to systems, facilities, restricted areas are revoked upon termination of employment
θ Yes θ No

2. Does your organization have an information security awareness program?
θ Users have undergone an information security awareness training program
θ Users are regularly updated in organizational policies, standards, guidelines, and procedures.
Users are made aware and appropriately trained on the following security topics:
θ Acceptable use of computer systems
θ Access control
θ Data classification and handling
θ Email security
θ Internet security
θ Password security
θ Others: ____________________________
Security policies, topics or issues are communicated to the users through means such as:
θ Seminars
θ Intranet or email
θ Printed memos, pamphlets, posters, or signs
θ Videos
θ Yes θ No
3. Does your organization have a process for responding to security incidents?
θ Reporting guidelines and procedure is documented for reporting security incidents, security weaknesses, or software malfunctions
θ Users are made aware and trained on handling 'social engineering' attempts or attacks
θ The methods of social engineering and recognizing possible attack.
θ Handling suspicious requests for information or action through proper verification of identity and authority of the requesting person
θ Responsibility for reviewing and progressing of the closure of the incident is defined
θ Employees who are found to be responsible for incidents are subject to disciplinary process
θ Yes θ No
4. Has there been any security breaches, system intrusions or incidents that have occurred in the organization within the last 12 months?
Incident was caused by:
θ Insider
θ Outsider
θ Yes
θ No θ Don't know
5. In an event of a detected security incident, what actions did management take? Actions taken:
θ Conducted investigation and resolved with a solution
θ Employee suspension/dismissal
θ Filed court case
θ Did not report incident to law enforcement agencies
Others: ___________________________________
6. What are probable reason/s that your organization would not report security incidents to law enforcement agencies? θ Avoid negative publicity at all costs
θ Competitors would use the situation to take advantage
θ Unaware that they could report incidents
θ Civil remedy deemed as the best thing to do
θ Lack of legislative laws and provisions
θ Others ____________________________________
7. Does your organization have physical controls in place to protect sensitive areas/rooms?
The following controls are utilized
θ Secure IDs/Swipe Cards
θ Biometric controls are used to access data centers

θ CCTV/Surveillance cameras and guards are in place to monitor premises
θ Others: ___________________________________
θ A list of persons authorized to access rooms are maintained and periodically reviewed.
θ Logs and information captured by these technologies are regularly reviewed
θ Sensitive areas/rooms are not explicitly identified with obvious "signboards"
θ Sensitive areas/rooms are restricted to authorized personnel
θ Visitors are always signed in and escorted
θ Yes θ No

8. Does your organization take steps to prevent loss, damage or compromise of equipment and interruption to business activities?
θ Important equipment (e.g. servers) are located in secure areas to minimize exposure from fire, flooding, water damage, corrosive agents, electromagnetic radiation and smoke
θ Equipment are protected from power failure, e.g. use of a UPS, backup power
θ Equipment are maintained in accordance with the manufacturer's requirements
θ Computers are secured with lock devices
θ Equipment cannot be removed from its designated area without written authorization
θ Room is environmentally controlled to maintain correct temperature and humidity
θ Appropriate fire suppression and prevention devices are installed and working
θ Others: ____
θ Yes θ No

9. Does your organization implement general measures to protect the company's information from interception?
θ There is a "clear desk" policy in operation
θ Paper and computer media are locked away when not in use
θ Computer monitors are located to prevent viewing by unauthorized persons
θ Password protected screensavers are activated when the computer is left unattended.
θ Computers are logged off at the end of day
θ Electronic office appliances (printers, fax machines, etc) are appropriately/logically placed
θ Others: ____
θ Yes θ No

10. Does your organization's systems have documentation?
System documentation includes:
θ User's Manual
θ Vendor Supplied documentation of purchased software
θ Vendor Supplied documentation of purchased software
θ In-house application's documentation
θ Change management procedures
θ Security baselines
θ Performance benchmarks
θ Others: _______________________________
System documentation :
θ Are periodically reviewed and updated
θ Have a revision history
θ Yes θ No

11. Does your organization maintain system logs?
System logs are maintained for the following:
θ Internet connections
θ Access attempts
θ Critical Applications
θ Internal network devices (e.g. firewalls, routers, IDS, etc)

θ Logs are stored securely in a central location
θ Access to logs are strictly controlled
θ A copy of the logs is kept for at least ________ days
θ Yes θ No
12. Does your organization review logs for security related events?
System log reviews:
θ Occur at least daily
θ Use automated tools
θ Are performed by trained personnel
θ System clocks are synchronized with a trusted server time
θ Yes θ No
13. Does your organization have backup and restore procedures in place?
Backup and restore procedures are:
θ Documented
θ Tested annually to ensure effectiveness
θ Performed by trained personnel
Backup tapes/disks are:
θ Made at least once (1) a week
θ Kept based on a defined retention period
θ Stored in fireproof safes
θ Retired once their life-span has been reached
θ Yes θ No
14. Does your organization have a Business Continuity Management Process?
The Business Continuity Plan (BCP) is:
θ Documented
θ Managed by a dedicated group
θ Addresses different events that could cause interruptions to business processes (i.e. flood, fire, equipment failure, etc)
θ Reviewed, tested, and updated on a regular basis (At least annually)
θ Addresses every department/office
θ Users are trained on their BCP responsibilities
θ An “off-site back-up data center” is in place
θ Yes θ No

15. Does you organization have a process for managing user accounts?
θ There are procedures for requesting and approving user accounts and modifying privileges
θ Excessive privileges are not granted; User privileges are based on job function
θ User access is revoked days within the user’s termination or resignation
θ User access is reviewed regularly
θ User’s identity is verified prior to a password reset
θ Yes θ No
16. Does your organization enforce a patch management process?
θ Vulnerabilities and exploits are monitored regularly
θ Security patches and important fixes are applied upon further testing
θ Patch application procedures are documented
θ Yes θ No
17. Is the security of critical systems tested prior to production deployment?
θ Vulnerability and penetration testing is performed in accordance to documented system testing methodology
θ System interfaces are thoroughly tested
θ An independent external party periodically assesses the security posture of critical systems

θ Patch application procedures are documented
θ Yes θ No
18. Does your organization have a password policy?
θ Unique user name and password for user authentication is required
θ Password complexity scheme is in place and is technically enforced where feasible
θ Systems are configured to require users to change passwords after a determined period of time
θ Systems are configured to implement password histories
θ Yes θ No
19. Are logical controls implemented within your organization's network design?
θ Firewalls
θ Intrusion Detection/Prevention Systems (IDP)
θ Network Honeypots
θ Anti-virus systems
θ Anti-spyware and Anti-adware systems
θ Web filtering mechanisms (i.e. websphere, etc)
θ Others: ___________________________________
θ Yes θ No
20. Are the internal systems secured?
θ Application, server, and network performance and availability are monitored
θ Critical systems are monitored for security violations
θ Systems are scanned for unauthorized software installations
θ Desktops machines, laptops, and servers are configured according to your organization's technical configuration standards
θ Password protected screensavers are used to protect the desktop
θ Networks are properly segmented
θ Host based firewalls are implemented between segregated networks
θ Others: _____________________________________
θ Yes θ No
21. Are the systems in your Internet/DMZ environment secured?
θ Publicly accessible systems are tested for vulnerabilities and hardened prior to being deployed in production
θ All essential protocols (i.e. DNS, LDAP, SMTP, FTP) are securely configured
θ Firewalls are configured to allow only the necessary protocols directed to necessary destinations from trusted sources
θ All traffic entry and exit points are filtered by the firewall
θ The DMZ architecture is multi-tiered
θ Others: _____________________________________
θ Yes θ No
22. Are there security configuration baselines documented and implemented for systems in your organization?
There are security baselines for the following:
θ Operating systems
θ Routers, switches
θ Firewall
θ Remote access and authentication servers
θ Others: _____________________________________
θ Security baselines are reviewed every year
θ Yes θ No
23. Does your organization have virus protection software in place?
Virus protection/detection software exist at the following levels:
θ Firewall level

θ Desktop level
θ Server level
θ Mail server level
θ Web server level
θ Internet gateway level
θ Network segment level
θ Mobile (including PDA) level
θ Formal virus prevention and outbreak contingency plans and procedures in place
θ Virus definition files are updated on levels where anti-virus solutions are installed
θ Others: ____
θ Yes θ No
24. Is data encryption being used in your organization for sensitive systems?
Types of encryption implemented are:
θ File level encryption
θ Traffic level encryption
θ Database level encryption
θ Password encryption
θ Yes θ No
25. What type of network connection is viewed or cited as a frequent point of attack? θ Internal Systems
θ Remote Dial-in
θ Internet
26. Are controls in place to secure network access?
θ External networks are limited and secured by a firewall
θ There are documented procedures to activate new network connections
θ External networks are monitored for security violations
θ Connections to legacy systems are secured
θ Yes θ No
27. Are remote access connections secured?
θ Remote access connections are authenticated
θ Remote access are connected via VPN
θ Remote access is limited to only the needed applications and systems
θ There are procedures in place for approving and processing vendor requests for remote access in the network

VI. THREAT AND VULNERABILITY
1. What are the possible threat actions or events that may be conducted by threat sources? What is the likelihood (High, Medium, Low) of occurrence for the possible threat actions? Human Threat Sources: Low Medium High
Hacking/cracking θ θ θ
Social engineering θ θ θ
Physical Assault θ θ θ
Fraud θ θ θ
Theft θ θ θ
Unauthorized access to systems and information θ θ θ
Information sale or disclosure θ θ θ
Abuse of computer resource θ θ θ
System sabotage θ θ θ
Input of malicious codes (virus, worms, trojans) θ θ θ
Accidental input of erroneous data or information θ θ θ
Others: θ θ θ

Natural Threat Sources:
Earthquake θ θ θ
Typhoon/Flood θ θ θ
Lightning Strike θ θ θ
Others: θ θ θ
IT Related/Physical/
Environmental Threat Sources
Software Bugs θ θ θ
Computer/Hardware Failure θ θ θ
Network Failure θ θ θ
Electrical Failure (blackout, brownout, etc) θ θ θ
Fire θ θ θ
Others: θ θ θ
2. What are the possible motivations for attack by the human threat sources?
θ Ego/Challenge
θ Revenge
θ Destruction
θ Exploitation
θ Monetary gain
θ Competitive advantage/Intelligence
θ Unintentional errors and omissions (e.g. data entry errors)
θ Others: ____

3. What are likely sources of attack? θ Disgruntled Employees
θ Industry/Market Competitors
θ Independent Hackers
θ Foreign Corporations
θ Foreign Government
4. What are the types of attack or misuse detected in the last 12 months? θ Denial of Service
θ Laptop
θ Active Wiretap
θ Telecom Fraud
θ Unauthorized Access by Insiders
θ Virus
θ Financial Fraud
θ Insider abuse of internet access
θ System penetration
θ Telecom eavesdropping
θ Sabotage
θ Theft of proprietary information
5. How much cost did your organization incur due to the types of attack or misuse detected in the last 12 months? θ Denial of Service ______________
θ Laptop ______________
θ Active Wiretap ______________
θ Telecom Fraud ______________
θ Unauthorized Access by Insiders ______________
θ Virus ______________
θ Financial Fraud ______________
θ Insider abuse of internet access ______________
θ System penetration ______________

θ Telecom eavesdropping ______________
θ Sabotage ______________
θ Theft of proprietary information ______________
6. Has your organization’s web site been attacked or misused within the last 12 months? θ Yes (If yes, how many incidents? __________)
θ No
θ Don’t know
7. If your organization’s web site had been attacked, where did the attacks originate? θ Inside
θ Outside
θ Both
θ Don’t know
8. What types of attacks had been detected on your organization’s web site? θ Vandalism
θ Financial Fraud
θ Denial of Service
θ Theft of Transaction information
θ Others
9. What are the possible vulnerabilities that may be exploited by the identified threat sources?
Lack of or inadequate management and personnel security controls
θ Lack of information security policies
θ Lack of security orientation and awareness for personnel
θ Lack of or insufficient training of personnel on proper use of equipment
θ Lack of or insufficient training of personnel on job-related activities
θ Poor employer-employee relationship
θ Lenient hiring and screening procedures
θ Others: ____
Lack of or inadequate physical and procedural security controls
θ Lack of or inadequate monitoring of data centers
θ Lenient implementation of ID policy
θ Inadequate protection of computer processing facilities from damage against fire, water, electrical failure
θ Inadequate incident reporting and response procedures
θ Lack of backup and recovery procedures
θ Lack of or inadequate operating procedures for systems
θ Lack of business continuity or disaster recovery planning
θ Poor user access management procedures
θ Others: ____
Lack of or inadequate technical and logical security controls
θ Lack of or inadequate access control management
θ Use of weak passwords
θ Lack of or inadequate virus protection controls
θ Lack of system updates and patches
θ Poor network design