Government of the Republic of Trinidad & Tobago

National Cyber Security Strategy

Prepared by the Inter-Ministerial Committee for Cyber Security,
December 2012

Table of Contents

1.0 Executive Summary

Governments, businesses and citizens are increasingly becoming large consumers of Information and Communication Technologies (ICTs) and electronic services, relying more on ICTs in the areas of management, communication, education, commerce, procurement and service provision. The reality of the environment is that for all the opportunities that ICTs bring, security risks are also present. These, if not mitigated and managed, can have a deleterious effect on the reputation of the Government of Trinidad and Tobago, domestically and internationally.

This Strategy seeks to guide all operations and initiatives related to cyber security in Trinidad and Tobago. It is based on the government's Medium Term Policy Framework, 2011-2014, which underscores the role of ICT in advancing national development. Its main objectives are as follows:

i. To create a secure digital environment that will enable all users to enjoy the full benefits of the Internet;

ii. To provide a governance framework for all cyber security matters by identifying the requisite organizational and administrative structures necessary, inclusive of human resources, training and capacity building and budgetary requirements;

iii. To protect the physical, virtual and intellectual assets of citizens, organizations and the State through the development of an effective mechanism that addresses and responds to cyber threats regardless of their origin;

iv. To facilitate the safety of all citizens by promoting awareness of cyber risks and developing effective and appropriate protective measures to mitigate risks and attacks;

v. To help prevent cyber attacks against critical infrastructure and secure information networks by building competency among primary stakeholders and the general public;

vi. To minimize damage and recovery times from cyber attacks through effective incident management measures; and

vii. To create a legal and regulatory framework to maintain order, protect the privacy of users and criminalize attacks in cyberspace.

In order to achieve these objectives, five (5) key areas of focus have been identified:

1. **Governance:** The fundamental goal is the establishment of a Trinidad and Tobago Cyber Security Agency (TTCSA) as the main body responsible for all cyber security matters, and the coordinating centre for all cyber security operations.
2. **Incident management:** The establishment of Computer Security Incident Response Team (TT CSIRT) as a national focal point for incident reporting, incident management and incident response.
3. **Collaboration:** The establishment of public-private/civil society partnership in securing Trinidad and Tobago's cyber infrastructure, as well as the promotion of cooperation with international organizations.
4. **Culture**: Awareness raising, training and education in cyber security throughout the country.
5. **Legislation**: The drafting and enactment of relevant cybercrime legislation to criminalise appropriate offences, prosecute offenders and protect citizens.

Through this Strategy, the Government envisions the creation of a secure and resilient cyber environment, based on collaboration among all key stakeholders, which allows for the exploitation of ICT for the benefit and prosperity of all.

2.0 Introduction

Information and Communication Technology (ICT) provides the basis for the development of every modern and progressive society and allows for incorporation into the global information economy.

Governments, businesses and citizens are increasingly becoming large consumers of ICTs and electronic services. This growing reliance is demonstrated through *inter alia*, its infusion in education, ongoing enhancement of communication networks, improved facilitation of international trade, changes in management and procurement systems and advances in health care provision. In the last twelve (12) years, ICT usage has increased by 1,310.8% in Latin America and the Caribbean[1]. The World Economic Forum, Global Information Technology Report shows that Trinidad and Tobago's readiness to leverage ICT for increasing competitiveness and development jumped upwards from 79 out of 133 countries in 2010[2] to 60 out of 142 countries in 2012[3].

The transformative potential of ICTs and the Internet has been recognised by the Government of the Republic of Trinidad and Tobago (GoRTT) which identified ICT and the establishment of a diversified knowledge economy as discrete development pillars within its Framework for Sustainable Development[4]. The intent is to promote universal and equitable access to and use of ICTs and the Internet, so as to address the digital divide and provide for the inclusion of underserved and/or un-served communities.

Yet, a corollary to the many opportunities offered by ICT is the presence of various risks in cyberspace. Thus, the country's response to internal and

[1] World Internet Usage and Population Statistics, June 2012, http://www.internetworldstats.com/stats.htm
[2] World Economic Forum, "The Global Information Technology Report 2009-2010: ICT for sustainability, 2010. p. xvii. http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf.
[3] World Economic Forum. "Global Information Technology Report: Living in a hyperconnected world": 2012. p. xxiii. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf
[4] Government of Trinidad and Tobago, "Innovation for Lasting Prosperity: Medium Term Policy Framework, 2011-2014", October 2011

external threats must include the deployment of technology to monitor and analyze natural and man-made disasters, the physical protection of the information infrastructure that supports the knowledge-based economy and the mitigation of threats that can result from the misuse of computer systems. In seeking to address these threats, there is a requirement to ensure the maintenance of effective communication among relevant stakeholders. This is a key component in realizing and maintaining the general ICT security objectives of **availability, confidentiality and integrity.**

This Strategy seeks to guide all operations and initiatives related to cyber security in Trinidad and Tobago. It recognises the critical need for an overarching governance framework, appropriate cybercrime legislation and the establishment of a national Cyber Security Incident Response Team (CSIRT). It also acknowledges the importance of building awareness among all stakeholders (government, business, academia, civil society and citizens) of their roles and responsibilities in establishing a secure ICT environment.

2.1 What is Cyber Security?

Although there is a lack of international consensus on the definition of cyber security, Trinidad and Tobago subscribes to the International Telecommunications Union's Telecommunication Standardization Sector, (ITU-T) Recommendation X.1205(X.cso) which states that:

> "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and*

maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."[5]

Effective cyber security would ensure system availability, integrity, authenticity, confidentiality, and non-repudiation. It would address user privacy and enhance trust in related systems.

3.0 A Case for Action

The globally-interdependent network of digital ICT infrastructures referred to as "cyberspace" is the underlying force driving the growth of the global knowledge economy. ICT continues to impact all sectors of society in countries worldwide, enabling new business practices, new modes of government-citizen engagement, and changes in interpersonal interactions. This, as a result, changes the face of, *inter alia,* economic, social and political structures and activities, public infrastructure, public services, education and national security. The ICT industry itself is also continually growing. Within the last decade, technologies have become even more powerful. Access to cyberspace has now become easier through new mechanisms such as mobile devices and mobile broadband, whereby, digital content can be produced and shared within minutes on social networks.

Threats to cyberspace are of critical concern to all countries. The ITU reports that there is evidence to show that cyber attacks are growing in sophistication, frequency and gravity; for example, due to the automation of business processes, it is estimated that as many as 80 million hacking attacks are conducted daily[6]. Security firm Symantec reports that global annual losses resulting from cybercrime are valued at US$388 billion. In a study conducted in twenty-four (24) nations by the firm, 69% of those surveyed claimed to

[5] International Telecommunication Union Definition of Cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[6] International Telecommunication Union, 'Understanding Cybercrime: A Guide for Developing Countries', April 2009, p. 72

have been the victim of cybercrime. It was found that 431 million adults, more than a million a day, fall victim to cybercrime each year[7].

Cyberspace provides the environment that facilitates organized virtual attacks on information assets, as well as physical infrastructure. These attacks can be carried out even by using readily available consumer technology.

Sophisticated cybercriminals can conceal their identities, locations, and paths of entry. They can leverage cyberspace to disrupt communications, hinder or delay defensive, offensive or emergency response. The virus Stuxnet[8], for example, which was discovered in 2010, was designed to target industrial control systems used to monitor and run large-scale industrial facilities such as power plants, oil refineries, and gas pipelines.[9]

In Trinidad and Tobago, the following areas are among those susceptible to compromise by criminal or terrorist elements:

- online banking and financial networks;
- online government services such as TTBizLink;
- real-time information systems, such as the Supervisory Control and Data Acquisition (SCADA) systems that manage the pumping stations at the Water and Sewerage Authority (WASA) and the Trinidad and Tobago Electricity Commission (T&TEC);
- revenue-dependent oil, gas and petrochemical infrastructure;
- air transport and public ground transportation.

Experiences in Trinidad and Tobago, like those globally, have underscored the truism that increasing reliance on cyberspace brings both opportunities and threats. The rapid integration of the Internet into almost all aspects of social and economic activity and the ubiquity of ICT has increased the

---

[7] Symantec, 'Norton Cybercrime Report 2011'
http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

[8] The ultimate goal of Stuxnet was to manipulate the physical equipment attached to specific industrial control systems so the equipment acted in a manner programmed by the attacker, contrary to its intended purpose.

[9] Symantec, 'Duqu: The Precursor to the Next Stuxnet'
http://www.symantec.com/outbreak/?id=stuxnet

vulnerability of all facets of society. The country has witnessed an increase in a number of cyber incidents including child online pornography, online bullying, attempted domain hijacking and website hacking. The April 2012 hacking into the Ministry of Finance and Parliament websites and the July 2012 Automated Teller Machine (ATM) skimming scam whereby well-hidden cameras were used by thieves, to capture the personal identification numbers for some customers' debit and credit cards, from a few major banking institutions, are recent local examples of increasing cybercrime incidents[10].

Questioned in an online magazine "ICT Pulse", an IT/network security expert expressed the view that the biggest trends in threats and intrusions in Trinidad and Tobago are the increasing "presence of command and control BOT, attempted domain hijacking and fake antivirus as well as constant port scans."[11]

The GoRTT has embarked on a number of programmes to increase ICT access and affordability and to reduce the digital divide. These include the eConnect and Learn (eCAL) Programme through which all students entering secondary schools in Form 1 are provided with laptops; and the fleet of buses that facilitates ICT training and capacity building in rural underserved and un-served areas. These programmes are evidence of the importance that has been attached to ICT and the Internet as a critical component in achieving economic growth, global competitiveness and a better life for citizens.

Such an approach allows for the maximum realisation of the benefits to be derived from the digital revolution. At the same time however, it is incumbent that strategies be implemented that address the risks, particularly to our children and young people, associated with the use of the Internet.

[10] Cyber Unit and Fraud Squad probe ATM scam. Trinidad Guardian. July 10, 2012. http://www.guardian.co.tt/news/2012-07-09/cyber-unit-and-fraud-squad-probe-atm-scam

[11] Expert insights 3: Cyber threats and security in the Caribbean. ICT Pulse: ICT issues from a Caribbean perspective. April 1, 2012. Interview with Aaron Manzano, of HMP Consulting in Trinidad and Tobago. http://www.ict-pulse.com/2012/03/expert-insights-3-cyber-threats-and-security-in-the-caribbean/

Thus, Trinidad and Tobago must define and implement the necessary policies, strategies and plans to ensure continuing confidence and trust in the reliability of the Internet, the security of the systems connected thereto and the safety, security and resilience of the country's ICT digital infrastructure.

4.0 Strategic Foundation

The GoRTT's Medium Term Policy Framework (MTPF)[12], 2011-2014 underscores the role of ICT in advancing national development. It notes that:

1. "The use of ICT is an essential element of the infrastructure underpinning the creation of a modern, competitive economy in an information rich, knowledge and technology-driven world.
2. Creating a diversified and knowledge intensive economy is at the core of building international competitiveness, stimulating new areas of economic growth and moving up the value chain.[13]"

The MTPF is premised on the Framework for Sustainable Development which is built upon seven interconnected development pillars. Pillar Four *(Information and Communication Technologies – Connecting Trinidad and Tobago and Building the New Economy)* acknowledges the extent to which the adoption and utilization of ICT is a critical success factor in achieving sustainable development. Cyber security is one of the cornerstones of this new ICT paradigm, as the establishment of the appropriate legislative framework and enforcement machinery to detect, combat and protect against cybercrime is considered fundamental.

4.1 Vision

The GoRTT will create a secure and resilient cyber environment, based on collaboration among all key stakeholders, which allows for the exploitation of ICT for the benefit and prosperity of all.

[12]Government of Trinidad and Tobago, "Innovation for Lasting Prosperity: Medium Term Policy Framework, 2011-2014", October 2011
[13]Ibid

4.2 National Policy Considerations

The following are key policy positions that have been adopted in order to define the cyber security strategy for the protection of Trinidad and Tobago's national assets and interests:

- The entity responsible for the coordination, implementation, monitoring, continuous improvement and governance of cyber security initiatives will be the Trinidad and Tobago Cyber Security Agency (TTCSA);

- Cyber security is a component of the national security strategy and the national ICT plan which in turn are subsets of the Policy Framework for Sustainable Development. As such, all relevant policies and strategies are aligned to the overarching policy framework;

- The cyber security strategy takes into account data protection and privacy considerations;

- Comprehensive national cybercrime legislation that is regionally and internationally applicable and harmonised will be enacted and implemented;

- The cyber security strategy as far as possible will be guided by international agreements and standards;

- A culture of cyber security will be promoted in an effort to raise awareness and build confidence in the ICT environment;

- Coordination and collaboration at the national, regional and international levels will be promoted and strengthened; and

- Research and development in the area of cyber security will be encouraged in order to build capacity and maintain a resilient knowledge base.

5.0 Framework

Developing and implementing a national cyber security plan requires a comprehensive strategy that includes a broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, civil society, academia, businesses, and citizens) in the process.

The following **strategic objectives** have been identified in accordance with international guiding frameworks:

i. To create a secure digital environment that will enable all users to enjoy the full benefits of the Internet;

ii. To provide a governance framework for all cyber security matters by identifying the requisite organizational and administrative structures necessary, inclusive of human resources, training and capacity building and budgetary requirements;

iii. To protect the physical, virtual and intellectual assets of citizens, organizations and the State through the development of an effective mechanism that addresses and responds to cyber threats regardless of their origin;

iv. To facilitate the safety of all citizens by promoting awareness of cyber risks and developing effective and appropriate protective measures to mitigate risks and attacks;

v. To help prevent cyber attacks against critical infrastructure and secure information networks by building competency among primary stakeholders and the general public;

vi. To minimize damage and recovery times from cyber attacks through effective incident management measures; and

vii. To create a legal and regulatory framework to maintain order, protect the privacy of users and criminalize attacks in cyberspace.

In order to achieve these objectives, five key areas have been identified and are outlined hereunder:

1. Governance
2. Incident Management
3. Collaboration
4. Culture
5. Legislation

5.1 Governance

Trinidad and Tobago's cyber security efforts must be able to effectively address the dynamic and challenging nature of threats to cyberspace. This requires an overarching governance framework to effectively coordinate and manage a comprehensive cyber security strategy.

Existing vulnerabilities that could create the most disruption to Trinidad and Tobago's critical systems and infrastructure must be identified and addressed. The Government will promote development of new systems with less vulnerability together with an ongoing assessment of emerging technologies for weaknesses. Common standards for securing ICT infrastructure, services and data repositories will be developed and enforced throughout Trinidad and Tobago. Periodic review of standards, policies and regulations will also be undertaken. Communication between and among Government Ministries and Agencies will also be promoted.

In order to manage the country's response to ever-evolving cyber threats, and to coordinate the wide cross section of entities with perceived overlapping authority for the management of these issues, it is imperative to establish

cohesion between the public sector, the private sector and all key stakeholders. In this regard the implementation of a Governance Framework is required to deliver the infrastructure needed to manage and coordinate all activities related to this response.

The GoRTT will establish the Trinidad and Tobago Cyber Security Agency (TTCSA) by way of legislation which will provide the required services for the following key functions:

1. Implementation and advice on the national cyber security strategy;
2. Provision of situational awareness information, and collection and analysis of data on cyber security issues;
3. Promotion of efficient network and information security management;
4. Raising awareness and promotion of local and international cooperation.

The Agency will be responsible for coordinating and or managing the following core functional areas of cyber security.

1. Development and implementation of management frameworks for all functional areas;
2. Incident response and management;
3. Cyber forensics and investigations (this function will be performed by the Cyber Crime Unit of the Trinidad and Tobago Police Service);
4. Promotion of cyber security culture, education, training and research;
5. Communications, international collaboration, public and private partnerships;
6. Cyber security legal issues, (continuous review and recommended amendments to legislation);
7. The interdependence of Critical Information Infrastructure Protection (CIIP) and Critical Infrastructure Protection (CIP).

This governance framework will provide a sustainable structure which can evolve to meet and address the reality of cyber security in Trinidad and Tobago.

The proposed organisational structure for the TTCSA has been developed and is attached as Appendix I.

5.2 Incident Management

In order to secure and strengthen the country's critical information infrastructure, coordinated efforts should be made to mitigate, and/or control incidents in the quickest and most efficient manner. There is therefore a requirement for an organization which can serve as the national focal point for incident reporting, incident management and incident response.

The GoRTT will establish a Trinidad and Tobago Computer Security Incident Response Team (TT-CSIRT) which will be responsible for:

- dissemination of cyber security information;
- technical guidance and support in the event of a cyber-incident;
- collaboration between and among government entities at the national level, the private sector, academia, and the international CSIRT community.

TT-CSIRT would possess the capabilities to:

- Provide warning of potential threats, incidents, and attacks;
- Facilitate information-sharing among the TT-CSIRT constituency relating to best practices, investigative information, coordination of incident response, and incident management procedures and processes;
- Analyse cyber vulnerabilities, incidents, and attack methodologies;
- Provide technical assistance to the GoRTT and other stakeholders within the national framework;
- Conduct investigations, and forensics analysis;

- Defend against attacks with special focus on critical information infrastructure; and
- Lead national-level recovery efforts in the event of a cyber-incident.

TT-CSIRT will be developed and implemented based on industry standards and international best practices, and will ensure the national community is aware of the protocols for reporting cyber incidents.

TT-CSIRT will be housed in the TTCSA.

5.3 Collaboration

The protection of cyberspace is a shared responsibility with each individual actor playing a key role in the security chain. If cyber security is truly to be realised, approaches must be pertinent to the local context while also being compatible and interoperable with those at the international level. This underscores the critical importance of national and international cooperation and collaboration.

5.3.1 National Collaboration

A public-private/civil society partnership is essential in securing Trinidad and Tobago's cyber infrastructure. The GoRTT will partner with the private sector and civil society in the implementation of its cyber security strategy.

Cooperation will be facilitated, through information sharing, participation in technology forums and research and analysis, to provide input for the development and dissemination of best practices for cyber security.

Private enterprises, including Internet Service Providers (ISPs), have an important role in securing cyberspace as they own major networks and computer systems. These entities will be encouraged to evaluate the security of those networks that impact the security of Trinidad and Tobago's critical infrastructure. Such evaluations would include:

- Conducting risk assessments and audits;
- Developing continuity plans which consider staff and equipment; and
- Participating in industry-wide information sharing and best practice dissemination.

The Ministry responsible for national security will also foster the development of cyber security certification programmes that will be nationally recognized and accepted by the public and private sectors.

5.3.2 International Collaboration

Given the interconnectivity of ICT infrastructures and the global nature of cyber threats, international cooperation and collaboration is required to secure the ICT environment. Such collaboration would involve raising awareness of cyber security, improving the exchange of information sharing of reciprocal data, participating in the formulation of international norms and standards, adopting and adapting such standards and good practices in all dimensions of cyber security; mutual legal assistance and participating in coordinated investigations and prosecutions of cyber criminals.

A key aspect of this international cooperation is the promotion of discussions from the perspective of a Small Island Developing State (SID), especially as it relates to international conventions on cybercrime which may have an economic impact on Trinidad and Tobago and other small states. This will necessitate greater participation in international standard-setting organisations at the regional, hemispheric and international level.

To date, the primary sources of international assistance for Trinidad and Tobago in the area of cyber security have been the Organization of American States (OAS), European Union (EU), Caribbean Telecommunications Union (CTU) and the International Telecommunication Union (ITU). Nonetheless, information exchange and cooperation will be strengthened with other multilateral organizations including the Caribbean Community (CARICOM), the Commonwealth Secretariat and the Council of Europe. Avenues for enhanced bilateral cooperation will also be explored.

5.4 Culture

It is recognized that awareness at the national level constitutes a pre-requisite for effective protection in cyberspace. The GoRTT will assume a leadership role in developing a culture of cyber security. This will necessitate the adoption of a multi-disciplinary and multi-stakeholder approach inclusive of awareness- raising, embedding cyber security in the wider aspects of policy formulation and educating all users of ICT and the Internet on their respective roles in cyberspace.

Further, the GoRTT, in coordination with the private sector, will work to educate the general public and small, medium and large businesses on basic cyberspace safety and security issues. The initial focus will be on the elaboration of guidelines and the creation of programmes in cyber safety for primary and secondary school students.

Higher education institutions will also be encouraged to adopt policies and measures necessary to improve system security.

Scientific research and innovation are also critical to ensuring cyber security and development of the national digital economy. Thus, training and ongoing research to develop innovative security tools will be conducted in order to maintain reliable systems while building resistance to current and future threats. The GoRTT will allocate resources for training and education of individuals who can develop such tools and specialise in securing critical information infrastructure.

The Ministries responsible for national security and science and technology will also promote advanced training for cyber security professionals in public and private educational institutions as well as promote the establishment of standards for the certification of qualified ICT security professionals.

The Ministry responsible for national security will encourage private organizations and companies to provide sufficient opportunities for continuing education and advanced training in the workplace to maintain

high skill standards and the capacity to innovate. It will also champion the coordination of training programmes between the government and the private sector.

5.5 Legislation

One of the objectives of the national policy framework is the expansion of the country's internet connection capabilities so that every stakeholder will be able to conduct business and have access to a wide range of governmental services. As a corollary to this, it is recognized that the government must play an important role in ensuring that there is clear policy with a regulatory and legal framework in relation to cybercrime. The GoRTT would therefore develop a national cybercrime policy and enact national cybercrime legislation.

Recognizing that strong policing of cybercrime is necessary for the enjoyment of the benefits of the digital environment, the GoRTT will develop a well-defined legal framework to establish and maintain order and security for users of the electronic environment and sanction those who deliberately cause damage to computers and electronic networks.

The legislative framework will:

- Adopt an omnibus approach to tackle computer and computer-related crime to account for rapid ICT developments at the global level;
- Establish offences which include, illegal access, illegal interception, and infringement of Intellectual Property Rights, identity-related crimes, unsolicited electronic junk mail or SPAM, cyber-bullying, as well as aiding and abetting;
- Facilitate the collection and admissibility of electronic evidence;
- Encourage cross–border investigations with regional and international governments and their enforcement agencies; and
- Create a pool of judicial experts from public and private sectors to share expertise and knowledge.

6.0 Operational Goals and Related Activities

The National Cyber Security Strategy as defined in the five operational goals can be represented in a tabular format, as outlined hereunder.

Operational Goals	**Actions**
1.0 Create an appropriate Governance framework for cyber security	1.1 Establish a Trinidad and Tobago Cyber Security Agency; 1.2 Develop and implement common ICT security standards across Government; 1.3 Provide a mechanism for periodic review and assessment of national cyber security policies and regulations.
2.0 Develop National Incident Management Capabilities	2.1 Establish a centralized computer security incident response (TT-CSIRT); 2.2 Establish shared situational awareness across the GovNeTT; 2.3 Develop a coordinated national cyberspace security response system to prevent, detect, respond to and

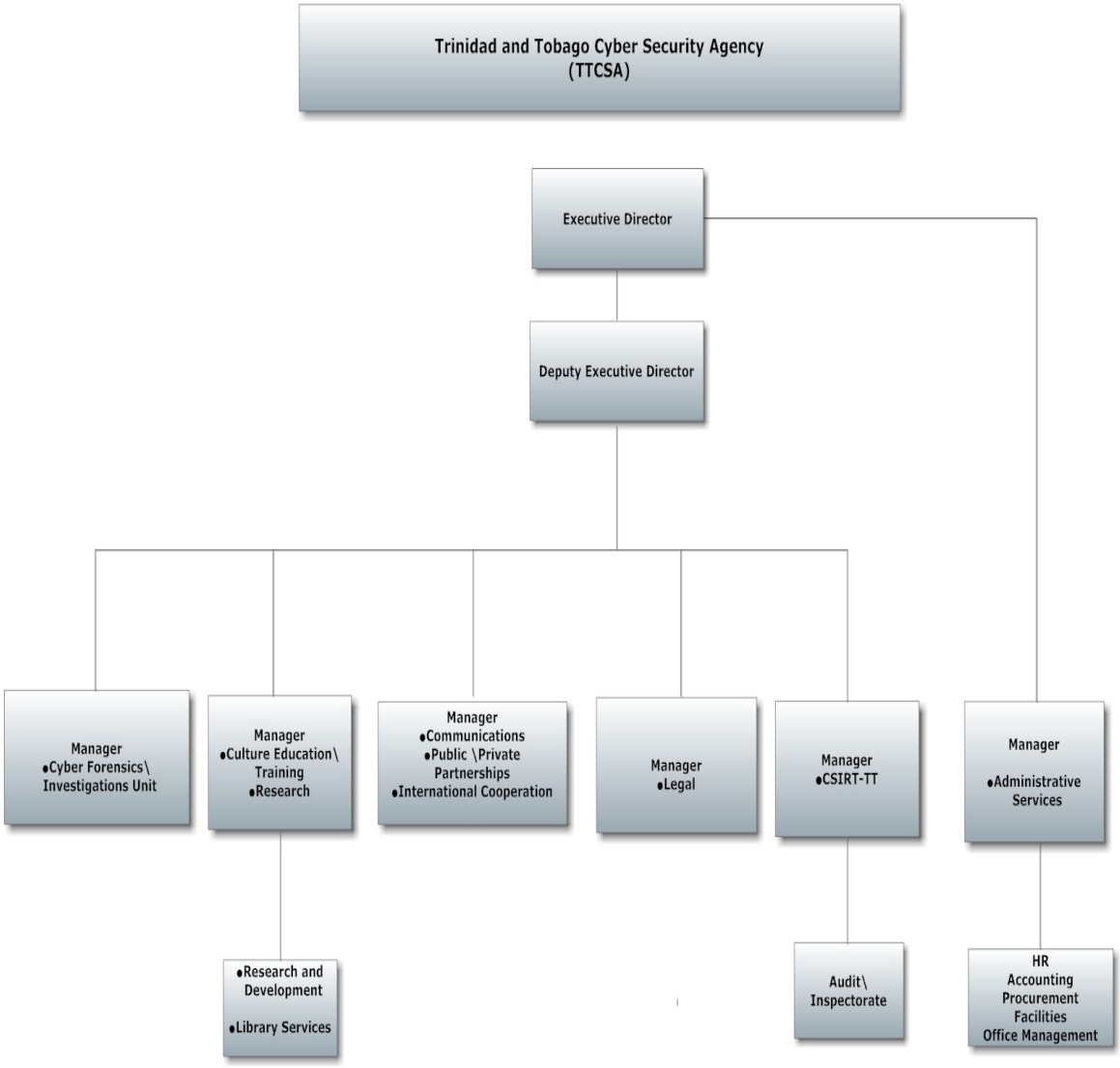
		recover from cyber incidents;
	2.4	Establish focal points for managing cyber incidents that bring together critical elements from government (including law enforcement) infrastructure operators and vendors to reduce both the risk and severity of incidents;
	2.5	Participate in watch, warning and incident response information sharing mechanisms;
	2.6	Develop, test and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.
3.0 Develop government, civil, and private industry collaborative relationships that work to effectively manage cyber risk and to protect cyberspace.	3.1	Provide a mechanism for bringing a variety of perspectives, expertise, and knowledge together to reach consensus to enhance security at a national level;
	3.2	Include industry perspectives in the earliest stages of

		development and implementation of security policy and related efforts;
	3.3	Encourage development of private sector groups from different critical infrastructure industries to address common security interests collaboratively with government;
	3.4	Bring together the private, civil and public sectors in trusted forums to address common cyber security challenges;
	3.5	Encourage cooperation among groups from interdependent organisations and agencies;
	3.6	Establish cooperative arrangements for incident management between Government and various groups.
4.0 Promote a national culture of cyber security consistent with United Nations General Assembly Resolutions 57/239 entitled "Creation of a global culture of	4.1	Implement a cyber security plan for government operated systems;
	4.2	Implement security

cyber security"; and 58/199 entitled "Creation of a global culture of cyber security and the protection of critical information infrastructures".	awareness programmes and initiatives for users of systems and networks; 4.3 Encourage the development of a culture of cyber security in business enterprises; 4.4 Support outreach to civil society with special attention to the needs of children and individual users; 4.5 Promote a comprehensive national awareness programme so that all stakeholders - business, the general workforce and the general population - secure their own parts of cyberspace; 4.6 Develop awareness of cyber risks and available solutions; 4.7 Enhance science and technology (S&T) and research and development (R&D) initiatives; 4.8 Review existing privacy regime in accordance with the digital environment; 4.9 Make IT security a priority in higher education;

	4.10 Revise organizational security policy and improve the use of existing security tools; 4.11 Integrate work in higher education with the national effort to strengthen critical infrastructure; 4.12 Improve collaboration between higher education, industry and Government.
5.0 Deter Cybercrime	5.1 Enact and enforce legislation relating to cyber security and cybercrime; 5.2 Build local capacity of law enforcement and prosecution authorities; 5.3 Build local judicial capacity.

7.0 Appendix: Organizational Structure for the Trinidad and Tobago Cyber Security Agency



8.0 Glossary

(i) **Computer Security Incident Response Team:** A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client.

(ii) **Control and command BOT:** a group of compromised computers running software that are under external control.

(iii) **Critical Infrastructure:** means computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, defence or international relations of the State; or provision of services directly related to national or economic security, banking and financial services, communications infrastructure, national public health and safety, public transportation, public key infrastructure or any combination of those matters.

(iv) **Cyber bullying:** refers to a person being tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person, using the Internet, interactive and digital technologies or mobile phones.

(v) **Cyberspace:** Cyberspace integrates a number of capabilities, such as sensors, signals, connections, transmissions, processors, and controllers, and generates a virtual interactive experience accessed for the purpose of communication and control regardless of a geographic location. Cyberspace allows the interdependent network of information technology infrastructures, telecommunications networks, such as the Internet, computer systems, integrated sensors, system control

networks and embedded processors and controllers common to global control and communications.

(vi) **Domain hijacking:** intentionally accesses a computer without authorization or exceeds authorized access.

(vii) **eConnect and Learn (eCAL) Programme:** This represents Government's primary programme for increasing accessibility to ICTs among students and infusing ICT in education through the provision of laptop computers to all students entering secondary school in Form 1. It is aimed at ensuring that students develop the capacity and requisite skills required for the 21st century.

(viii) **GovNeTT:** The Government Wide Area Network (GWAN) is the network backbone for communication and collaboration among Government Ministries and Agencies which provides an enterprise-wide platform for government-related ICT services including the capacity to provide email, Internet access, messaging, etc.

(ix) **Hacking:** A common term usually used to describe unauthorised entry on to a computer, network or website.

(x) **Information and Communication Technology:** refer to technologies people use to share, distribute, gather information and to communicate, through computers and computer networks.

(xi) **Skimming:** A type of fraud in which the numbers on a credit card are recorded and then transferred to a duplicate card. This is done without the knowledge of the original credit card holder.

(xii) **SPAM:** Bulk sending of emails to users

(xiii) **TTBizLink**: The name given for the Single Electronic Window for Trade and Business Facilitation which is aimed at improving the country's global competitiveness through the application of ICT.

(xiv) ***ttconnect*:** multi-channel delivery suite of e-services through which information and services can be accessed. This is comprised of the following five (5) delivery channels:

- ***ttconnect*** Online – e-Government Portal
- ***ttconnect*** Service Centres – Brick and mortar service counters located strategically in different parts of Trinidad and Tobago ***ttconnect*** Self-Serve – Automated, self-serve kiosks
- ***ttconnect*** Mobile – accessing government information and service via handheld smart phones
- ***ttconnect*** Express – ICT customized buses as mobile service centres.

9.0 References

1. Cyber Unit and Fraud Squad probe ATM scam. Trinidad Guardian. July 10, 2012. http://www.guardian.co.tt/news/2012-07-09/cyber-unit-and-fraud-squad-probe-atm-scam

2. Expert insights 3: Cyber threats and security in the Caribbean. ICT Pulse: ICT issues from a Caribbean perspective. April 1, 2012. Interview with Aaron Manzano, of HMP Consulting in Trinidad and Tobago.http://www.ict-pulse.com/2012/03/expert-insights-3-cyber-threats-and-security-in-the-caribbean/

3. Government of Trinidad and Tobago, "Innovation for Lasting Prosperity: Medium Term Policy Framework, 2011-2014", October 2011

4. International Telecommunication Union, 'Understanding Cybercrime: A Guide for Developing Countries', April 2009

5. International Telecommunication Union, 'National Cybersecurity Strategy Guide', September 2011 People's Partnership, 'Prosperity for All- 2010 Manifesto of the People's Partnership for a United People to Achieve Sustainable Development for Trinidad and Tobago'

6. Symantec, 'Duqu: The Precursor to the Next Stuxnet' http://www.symantec.com/outbreak/?id=stuxnet

7. Symantec, 'Norton Cybercrime Report 2011' http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

8. World Economic Forum, "The Global Information Technology Report 2009-2010: ICT for sustainability, 2010. p. xvii. http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf.

9. World Economic Forum, "Global Information Technology Report: Living in a hyperconnected world": 2012. p. xxiii. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

10. World Internet Usage and Population Statistics, June 2012, http://www.internetworldstats.com/stats.htm