د افغانستان اسلامي جمهوريت

د مخابراتو او معلوماتي تکنالوجۍ وزارت

Islamic Republic of Afghanistan

Ministry of Communications and IT

National Cyber Security Strategy of Afghanistan (NCSA)

Prevention - Protection - Safety - Resiliency

AUTHOR	VERSION CONTROL	DATE
ZMARIALAI WAFA	2.0	November 2014

About National Cybersecurity Strategy of Afghanistan (NCSA):

In late 2001, after the establishment of the interim government, Afghanistan stepped into new horizons of political and socio-economic rehabilitation and reconstruction. The subsequent transitional and the elected Afghan government introduced new legislations which assisted private companies to make investments in the country and provide various services including telecommunications and ICT services for the people of Afghanistan.

The Ministry of Communications and Information Technology (MCIT) was the first among the sectoral government entities in Afghanistan to design new strategies and policies, enabling private sector to make huge investment in the telecommunication and IT sectors.

In 2009, MCIT established the first Cyber Emergency Response Team (CERT) in Afghanistan and it was officially named as AFCERT. The mandate of AFCERT was to fight against cyber threats and crimes and provide awareness and solutions on cyber security to the government and private sector. In its first two years of operation, AFCERT submitted an official report to the MCIT senior management regarding an upsurge in the cyber and electronic crimes in the country. In order to fight the said crimes, it was vital to conduct a risk assessment of all government ICT infrastructures and come up with a solution to mitigate those risks. AFCERT's proposal on preparing a draft of Cyber Security Strategy for the country was accepted by the MCIT and ICT Council and to this end the MCIT and ICT Council established a committee.

In 2012 the first awareness workshop on drafting the NCSA was held in ICTI Institute, supported and funded by the US Department of Commerce. It was a 4 day workshop and all government CIOs, ICT heads, private sector and academia participated and studied and analyzed various strategies from different countries.

The NCSA committee was chaired by Information Systems Security Directorate of MCIT and held its regular meetings and assessments for one year. After a series of assessments and recommendations, the NCSA committee finalized and submitted the first draft of the strategy in July 2014 to the MCIT and ICT Council to review and adapt its action plan.

Acknowledgment:

We would like to thank MCIT senior management especially H.E. Minister Amirzai Sangin, Deputy Minister IT Mohammad Aimal Marjan, Deputy Minister Technical Baryalai Hassam, Deputy Minister Administration Wahabuddin Sadaat and ICT Council for accepting our proposal of drafting the NCSA.
We would also like to thank the NCSA Committee (Ministry of Finance, Ministry of Interior Affairs, Ministry of Defense, Ministry of foreign Affairs, National Directorate of Security, Ministry of Justice and Attorney General's Office) for their time, efforts and dedication in drafting the NCSA.

Special thanks to ITU-IMPACT for conducting an assessment on the establishment of AFCERT and providing support during the draft stages of NCSA. Our gratitude also goes to the US Department of Commerce for facilitating the first ever workshop on cyber security strategies.

ZMARIALAI WAFA
CHAIR NCSA COMMITTEE

Contents:

“ The art of war teaches us to rely not on the likelihood of the enemy’s not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Sun Tzu, the Art of War

Introduction

The use of information and communication technologies has been spreading rapidly in Afghanistan and ICTs are playing important roles in all aspects of our lives. Alongside the public sector, entities that provide services in critical infrastructure sectors like energy, health, aviation, communication and financial services have also been heavily using information and communication systems. These systems improve the quality and the speed of the services delivery - thus helping organizations work more productively, efficiently and contributing to the improvement of living standards.

As our public sector organizations use ICTs to provide services at an increasing rate, it has become an important aspect of our national security and competitiveness to ensure the security of information and communication technologies. The vulnerabilities inherent in ICTs may cause denial of service or abuse of service attacks, resulting in high scale economic losses, disturbance of public order and/or threats to national security.

It is a fact that cyber space offers opportunities of anonymity and deniability for attacks on information systems and data. The tools and knowledge required for attacks are often cheap and easy to get, and it has been observed that anyone or any systems across the world can participate in cyber-attacks, either knowingly or unknowingly. And it is deemed almost impossible to determine who finances and organizes these enduring and advanced cyber-attacks that target the information systems and data of critical infrastructures. These facts and conditions reveal the asymmetrical nature of the risks and threats in cyber space, making them even more difficult to tackle.

VISION

To establish and achieve a **Safe - Secure and Resilient** cyber space for the government, businesses and citizens of Afghanistan

MISSION

To protect and assure data, information and IT infrastructure security in Afghanistan's cyberspace, enhance capacities to prevent and response to cyber threats, protect the children and youth of Afghanistan in cyberspace, mitigate the risk of vulnerability, damage from cyber threats and incidents through a variety of standardized institutional structures, policies, procedures, people, technologies and administrative process

OBJECTIVES

1) To protect government ICT infrastructure, secure cyberspace for the citizens, improve and retain cybersecurity professional skills, encourage public - private partnerships, boost and maintain international cooperation.
2) To establish a framework for the information safety, assurance, information security policies, adaptation of international standards and best practices
3) To establish a regulatory framework in order to achieve resilient cyber space and its ecosystem
4) To enhance AFCERT capabilities to fight against cyber threats/crimes, draft and develop Disaster Recovery Plans for the government and Critical information infrastructures in the country
5) To develop and adapt suitable technologies, processes, based on the requirements of National Security
6) To establish testing and certification body to standardized and improve application and software development in the country
7) To promote and facilitate trainings for Information and Cyber security experts throughout the county
8) To safeguard data privacy of government, businesses and citizens by enabling the protection mechanisms for the data at rest and data at transit
9) To develop and promote public private partnership and engagement through technical and operational cooperation's and contributions in order to enhance the resiliency of cyberspace in the country
10) To enable and strengthen an effective prevention, investigation and prosecution of cyber and electronic crimes, enforce the law enforcement capabilities through an effective cyber law and legislation
11) To enhance and strengthen international cooperation's to fight cyber crimes

THE STRATEGY

1. Establishing a **Resilient** cyber ecosystem in Afghanistan

a) Information Systems Security Directorate (ISSD) of Ministry of Communications and Information Technologies (MCIT) to coordinate all cyber and information security related issues in the country with clearly defined roles and responsibilities. Having had the privilege of managing AFCERT since its establishment, ISSD should become an independent entity within Government structure once it reaches its maturity levels. This will avoid every kind of unwanted and unwarranted influence from other government and nongovernment entities on cybersecurity tasks and decisions - ensuring ISSD's full integrity.

b) Encourage both public and private sector to assign a member of senior management as Chief Security Officer (CSO), giving them the responsibility of cybersecurity efforts and initiatives in the country, ensuring public private partnership.

c) Encourage both public and private sectors to draft and develop their information security policies aligned with their business profile and services in compliance with international standards and best practices. Policies should be comprehensive, up to date with various data security methodologies, include Disaster Recovery Plan and business continuity.

d) Both public and private sectors to dedicate budget for cyber and information security activities and initiatives. The budget should be for the overall cybersecurity initiatives including IT infrastructure protection mechanisms, licensed software, patches and capacity building for IT personnel.

e) AFCERT to serve both public and private sectors as a first responder to cyber and computer incidents, given its professional staff and good reputation AFCERT will also work together with both sectors in order to establish mini and provincial CERTs for better coordination of the cybersecurity agenda, AFCERT will make sure that all entities adapt to and abide by the AFCERT assigned procedures and best practices in the field of incident response, cyber/computer crime scene data collection.

f) MCIT from security point of view will certify and approve any IT related procurement within the government, MCIT will come up with new guidelines and policies for the webhosting companies, software developers and IT services provider.

2. Establishing a **framework** for **information safety, assurance, information security policies**

a) ISSD of MCIT should enforce the adaptation of international standards, information security best practices, and compliance in order to ensure Confidentiality, Accessibility and Integrity of information throughout government networks.

b) Through the ISSD of MCIT enforce the adaptation of ISO 2700 series and other International standards for Information Security Management System (ISMS), information assurance, Information Systems and IT infrastructure audits, Vulnerability assessment, Risk management of the critical information infrastructures (CII), Business continuity, ensure Application security through Software Development Life Cycle (SDLC) and best practices and Penetration testing of IT infrastructures.
c) Enforce data classification of all governmental entities in order to ensure data confidentiality and apply access controls (Physical, Technical and Administrative) to ensure accountability.
d) Periodically conduct risk assessment and security standard compliance of the critical information infrastructures (CII).

3. Establishing a **regulatory** framework

a) MCIT will work together with the Ministry of Justice (MoJ) to develop legal framework and conduct for addressing cybersecurity issues
b) Develop the Cyber Law of Afghanistan and Child Online Protection policy with support and cooperation's of US-DOC, CLDP, European Commission, UNCITRAL and International Multilateral Partnership Against Cyber Threats (IMPACT)
c) Develop legal framework for private Certification Authority (CA) and secure electronic transaction system for business and financial institutes
d) Develop legal framework and policies to assure secure mobile computing, cloud computing, mobile governance and internet governance
e) Develop regulatory framework for auditing and certifying IT infrastructures for the sack of cyber security within the government and for those Solution providers (SPs) who are providing IT services to the government
f) Organize awareness campaign for all regulatory frameworks and periodically update the regulatory frameworks with the evolving technological advancements.

4. Enhance **AFCERT** capabilities

a) AFCERT as the focal point will act as first responder to any cyber incident or computer crime investigations within the government and private sector
b) Coordinate crime scene investigation report with law enforcement for further processes
c) Provide cyber related awareness to all government and nongovernment agencies through its Network Operation Center (NOC), workshops, seminars, email, magazines and newsletters
d) Extend its operation hours to 24/7 service availability within the timeframe of two years
e) Assist provinces in establishing the provincial CERTs
f) Keep strong engagement and coordination with regional CERTs in order to fight against cyber crimes

g) Coordinate cybersecurity exercises and conduct cyber drills with regional CERTs
h) Periodically provide advanced trainings and capacity building programs to enhance capacity and ensure improved performance.

5. Enabling **secure and sustainable e-Government** through the adaptation of best practices and reliable technologies

a) MCIT will adapt and implement a comprehensive information security framework to ensure a robust, secure trustworthy e-Government services throughout the government.
b) Afghanistan Root Certification Authority (ARCA) to enforce policies and mandate the use of Digital signature for all e-Gov, and m-Gov services within the government

6. Establishing **certification and testing** body

a) MCIT will dedicate an additional line and recruit a team of professional programmers solely to test and certify software and applications. The testing processes must be in compliance with all international standards, security has to be part of software developing life cycle. This will ensure the security and integrity of software/applications

7. Facilitating **trainings** for Information and Cyber security experts

a) MCIT will engage and coordinate training and capacity building programs with donor communities (World Bank, ITU, USAID) to secure funds for information security trainings, seminars and workshops for CSOs within the government and private sector
b) MCIT will work closely with the Ministry of Higher Education (MoHE) and Civil Services Commission to secure scholarships opportunities for masters programs in the field of information security.

8. Safeguarding **data privacy** of government, businesses and citizens

a) ISSD of MCIT will develop a plan and information security frameworks for the protection of Critical Information infrastructure. The plan should be inclusive of secure mechanisms for information flow while in transit and at rest with proper disaster recovery plan - meeting the business requirement
b) Guidelines and international standards will established for, Risk management, Crisis management and cyber/electronic crime investigation

9. Promoting public private **partnership**

a) Private sector will be encouraged to work closely with public institutions and being granted contracts and projects to deliver services complimentary to the government –

such as establishing private data centers that could turn support the government. This does not only promote a healthy competitive market but will also boost ICT economy in the government and build trust between both sectors

b) Facilitate collaboration and cooperation between stakeholders (Government and private sector) in the field of cybersecurity, protection of Critical information infrastructure, especially in implementation of cybersecurity action plan, implementation of international security standards and best practices

10. International Cooperation's

a) MCIT will work closely with MFA in order to develop and enhance multilateral relationship in cybersecuiry with the region and other countries through CERTs, information security agencies, law enforcement and Judicial entities

b) MCIT should keep close engagement and cooperation with IMPACT, ITU, ICANN, APT and other domestic and international organizations in order to fight against cyber crimes

Pressure Makes Diamonds!

National Cybersecurity Action Plan for the Term August 2014 –August 2015

This chapter includes the actions towards achieving national cybersecurity in light of the determined principles for the term 2014-2015 in the framework of the national cyber security strategy. There is one or two lead public organization and agency is appointed for each action item. However, each action can have more than one or two relevant organization and agency responsible for the implementation. In such cases, it is required that all the relevant organizations and agencies should act under the coordination of the lead organization and agency as required, and should also act in parallel with each other as required. There will be a lot more clarity on this once roles and responsibilities are laid out. There are a total of 5 action items scheduled to take place between 2014-2015. The deadline for some of the actions are determined and those actions which are envisioned to be repeated periodically and/or are of chronic occurrence are highlighted in particular

NO	Action	Responsible and Relevant Entity	Supporting Organization	Deadline	Remarks
1	Draft Cybercrime Law	MCIT, ISSD, MoJ, Parliament	US-DOC, CLDP, Council of Europe, IMPACT, UNCITRAL	December 2014	Kickoff meeting started in August 2014
2	Draft e-Transaction and e- Signature Law	MCIT, ISSD, MoJ, Parliament	US-DOC, CLDP, Council of Europe, UNCITRAL	December 2014	Kickoff meeting started in March 2014
3	Draft National Cyber/Information security Policy	MCIT, ISSD, National Security Council	MCIT	December 2014	Kickoff meeting started in March 2014
4	Draft ICT Law	MCIT, ISSD, MoJ, Parliament	US-DOC, CLDP, UNCITRAL, IMPACT, Council of Europe	December 2014	Kickoff meeting started in March 2014
5	Draft Intergovernmental IT security, Router, Switch, Firewall Policies	MCIT, ISSD	MCIT	December 2014	Kickoff meeting started in August 2014
6	Draft Computer crime incident response procedure	MCIT, ISSD	MCIT	December 2014	Kickoff meeting started in March 2014
7	Draft IT security training curriculum/schedule	MCIT, ISSD	MCIT	December 2014	Kickoff meeting started in March 2014
8	Auditing Financial institutes	MCIT, ISSD, Central Bank,	MCIT and Attorney General's Office	August 2015	Kickoff meeting starts in December 2014
9	Guidelines for forensic investigation	MCIT, MoJ and Attorney General's Office	MCIT, MoJ and Attorney General's Office	August 2015	Kickoff meeting starts in November 2014
10	Child Online Protection Policy	MCIT, MoE, NGOs	MCIT and IMPACT	August 2015	Kickoff meeting starts in December 2014

Definitions

The terms used in this document, refer to the following meanings:

Information systems: The systems involved in providing services, processes and data by means of information and communication technologies.

Cyber space: The environment, which consists of information systems that span across the world including the networks that interconnect these systems

Information systems of the government: The information systems, which belong to and/or are operated by the Government of the Islamic Republic of Afghanistan

National cyber space: The environment, that consists of the information systems that belong to public organizations, natural and legal persons,

Confidentiality: Authorized persons or systems only can access information systems and data, and the confidential information pertaining to information systems or confidential information in the system will not be disclosed by unauthorized persons or systems.

Integrity: Information systems and information can be changed by authorized persons or systems only,

Accessibility: Authorized persons and transactions can access information systems and the information therein within the required time and quality

Critical information infrastructures: The infrastructures which host the information systems that can cause, Loss of lives, large scale economic damages, Security vulnerabilities and disturbance of public order at national level when the confidentiality, integrity or accessibility of the information they process is compromised

PKI: Public Key Infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke Digital Certificates

ARCA: Afghanistan Root Certification Authority is the main body for the management of PKI Root and CAs in Afghanistan

IMPACT: International Multilateral Partnership Against Cyber Threats

ITU: International Telecom Union

CLDP: Commercial Law Development Program, an entity working under the US department of Commerce to support governments in developing their commercial laws

ICANN: International Corporation to Assign Names and Numbers is an independent international organization that manages the Domain Name Systems and Internet Protocol

UNCITRAL: United Nations Commission on International Trade Law

Cyber incident: Violation of confidentiality, integrity or accessibility of information systems or of the information being processed by these systems,

Cyber security: Protection of information systems that protect the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information being processed in this space, detection of attacks and cyber security incidents; putting into force the countermeasures against these incidents and then putting these systems back to their original states prior to the cyber security incident.

National Cyber Security: The cyber security of all services, processes and data –and the systems involved in provisioning of these- provided by the information and communication technologies in the national cyber space.