Qatar National Cyber Security Strategy

MAY 2014

TABLE OF CONTENTS

FOREWORD

The Internet has connected us to people all over the globe in ways that were unimaginable a decade ago, reducing barriers to communication and promoting cooperation in every area of our personal and professional lives. Cyberspace has become a dynamic and integral part of our society, propelling economic growth and innovation and enriching our lives in countless ways—and it will continue to expand and afford us even more opportunity in the future.

However, with these great rewards come new risks to the very infrastructure that underpins our ability to use the Internet safely and securely. Cyberspace, with its unlimited borders, provides those who would do harm with unparalleled opportunities to interfere with individuals and businesses. Luckily, we do not have to face this formidable task of cyber security alone. In this era of increasing—and increasingly malicious—cyber attacks of all sorts, keeping our networks and our people safe is one of the greatest global challenges facing all nations.

To address those challenges, Qatar is ramping up its cyber security efforts as well as working with our counterparts across the globe to ensure an open and secure cyberspace. In 2013, the Prime Minister established the National Cyber Security Committee to address the cyber agenda at the national level and to ensure that all public and private entities are adopting the right cyber agenda. And, we have developed a *National Cyber Security Strategy,* which is outlined in the pages of this document.

The objectives are very clear: safeguard the nation's critical information infrastructure; respond to and recover from cyber attacks; establish a legal framework and regulations to establish a safe and secure cyberspace; foster a culture of cyber security that promotes safe and appropriate use of cyberspace; and enhance our national cyber security capabilities.

While the government will lead the effort to safeguard government systems and networks, to succeed, cyber security must be a shared responsibility of government, businesses institutions, and individuals, and stakeholder coordination is essential.

As new, complex and global cyber security challenges emerge, Qatar is well positioned to be vigilant in enhancing the country's cyber readiness and resilience and protecting cyberspace for future generations. Inspired by the leaders of our nation, as envisioned in the *Qatar National Vision 2030,* we will continue to harness the power of information and communications technology to ensure a prosperous future for all of our people.

Dr. Hessa Al-Jaber
Minister of Information and
Communications Technology

EXECUTIVE SUMMARY

The Internet has been an unprecedented engine for development, social progress, and innovation. However, it is also used by cyber criminals, hackers, hacktivists, and foreign intelligence services who want to harm us by compromising or damaging our digital infrastructure. The unlimited borders of cyberspace have provided them with an unparalleled opportunity to interfere with individuals, businesses, government, and other institutions, and they use some of the most malicious and advanced techniques. One of the greatest global and strategic challenges of our time is how to sustain a safe environment while continuing to expand the benefits of a free and open cyberspace.

Qatar's rapidly developing economy is using information and communications technology (ICT) as a platform for innovation and prosperity. Resilience and security in cyberspace are vital to Qatar's continued success and growth. Therefore, a comprehensive national strategy is required to address current and emerging threats and risks.

In 2013, Qatar established the National Cyber Security Committee (Committee) to provide a governance structure for collaboratively addressing cyber security at the highest levels of its government. The Committee developed *Qatar's National Cyber Security Strategy (NCSS),* which represents a blueprint for moving forward to improve Qatar's cyber security. The NCSS combines good governance with a set of cyber security initiatives, measures, and awareness programs that will result in an efficient protective strategy in the long term.

The NCSS is based on a deep understanding of the threats and challenges Qatar is facing—from malicious actors to a shortage of workers with the necessary cyber security skills and a lack of reliable local providers of cyber security services—and is divided into several sections. Chapter 2 describes the threats and Qatar's existing capabilities in detail. Qatar's current capabilities to respond to the threats—from policy instruments such as the *National Information Assurance Policy,* and the *Banking Supervision Rules* to the technical and operational expertise in Qatar's Computer Emergency Response Team (Q-CERT), a trusted authority that promotes the identification and prevention of cyber attacks for the government and critical sectors—provide a strong foundation for continuing to improve Qatar's cyber security.

Chapter 3 describes Qatar's strategic approach to national cyber security.

Qatar's vision is to establish and maintain a secure cyberspace to safeguard national interests and preserve the fundamental rights and values of our society.

The vision is supported by five objectives that determine where action will be taken to deliver benefit and improve Qatar's cyber security:

- **Objective 1:** Safeguard the national critical information infrastructure;
- **Objective 2:** Respond to, resolve, and recover from cyber incidents and attacks through timely information sharing, collaboration, and action;

- **Objective 3:** Establish a legal and regulatory framework to enable a safe and vibrant cyberspace;

- **Objective 4:** Foster a culture of cyber security that promotes safe and appropriate use of cyberspace; and

- **Objective 5:** Develop and cultivate national cyber security capabilities.

Together, these objectives provide the foundation for protecting against, preparing for, detecting, responding to, and recovering from cyber incidents and attacks. Each objective is supported by initiatives that will drive action.

Chapter 4 provides details on the Qatari Government's Action Plan to achieve Qatar's cyber security vision. The Action Plan is organized by objective. The delivery of these projects will take considerable time and coordination between all stakeholders.

Successful implementation of the NCSS requires continuous commitment, governance, and action by various stakeholders who are connected by a shared vision and guiding principles. Qatar's approach to cyber security is based on three guiding principles:

- *The government will lead by example to safeguard government systems and networks, implementing cyber security requirements while building and adopting new technologies;*

- *Cyber security is a shared responsibility of all government entities, businesses, institutions, and individuals; and*

- *Qatar will pursue cyber security policies and initiatives that preserve society's fundamental rights and values, consistent with laws and regulations.*

Strong governance is needed to implement and manage execution of the NCSS. To that end, Qatar will establish the Cyber Security Coordination Office, which will report to the Prime Minister and be the focal point for cyber security activity across Qatar. This office will be responsible for: (1) establishing priorities to promote the highest level of cyber security in Qatar, (2) providing strategic direction for Qatar's cyber security efforts, and (3) working in close partnership with organizations with cyber security missions and mandates to fulfill the objectives of the NCSS.

This is an integrated and holistic approach that will enhance synergies, avoid duplication, and maximize resource utilization in managing the dynamic environment and emerging threats in cyberspace.

As new, complex, and global cyber security challenges emerge, Qatar's dependence on ICT will continue to increase. Qatar must be vigilant and enhance the country's cyber readiness and resilience, and the NCSS demonstrates Qatar's commitment to protecting a safe and secure cyberspace for future generations.

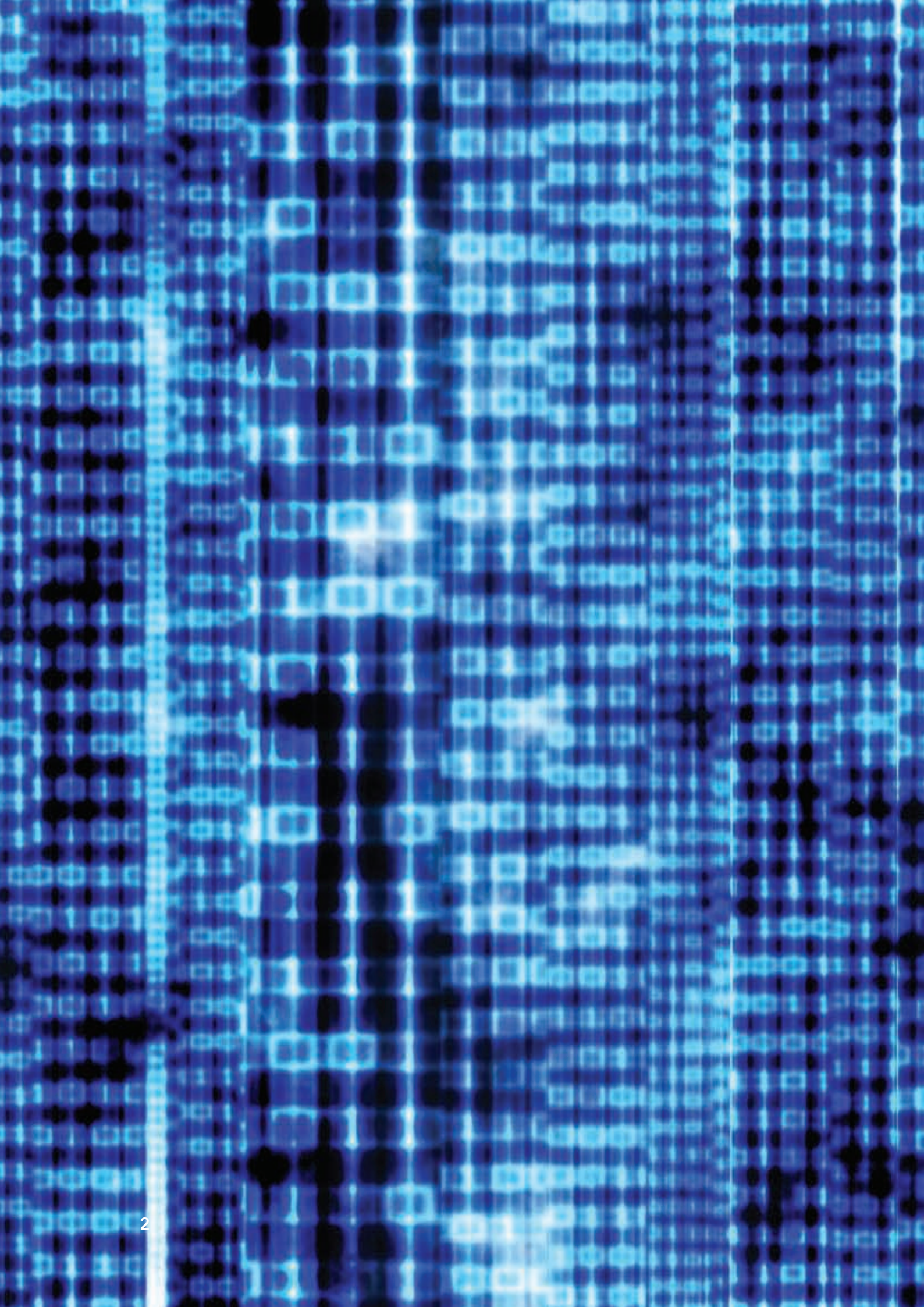
I. INTRODUCTION

Qatar is rapidly developing its economy, in part by embracing information and communications technology (ICT) as a platform for innovation and prosperity. The adoption of ICT is expanding Qatar's cyberspace, which has become integral to society, government, and businesses. Resilience and security in cyberspace are vital to Qatar's continued success and growth; therefore, a comprehensive national strategy is required to address current and emerging risks and threats.[1]

While ICT facilitates a well-connected society, it also increases the risk of undermining our social norms. The interconnected nature of cyberspace also increases the threat from a variety of malicious actors. These threats come from hackers, hacktivists, organized criminals, and even foreign governments. Qatar currently relies on a small set of penal statutes to investigate, prosecute, and punish cyber crime; however, additional measures are needed to ensure more comprehensive protection against cyber incidents and attacks.

To address current and emerging risks, *Qatar's National Cyber Security Strategy (NCSS):*

- Makes a commitment to protect Qatar's interests in cyberspace;
- Institutionalizes a cyber security vision and objectives for the future;
- Is grounded in the key principles of leadership, shared responsibility, and ethical values; and
- Is informed by mandates, other national strategies and international best practices, as well as the rights and values of individuals.



2. THE IMPORTANCE OF CYBER SECURITY TO QATAR

ICT systems provide government, businesses, institutions, and individuals with access to the information and knowledge needed to transform Qatar into a more advanced country by 2030.[2] Critical sectors in Qatar include but are not limited to finance, energy, electricity and water, government, and healthcare, and they are increasingly adopting the most modern digital applications. Doing so enables the delivery of high-quality, efficient, and effective services to customers in Qatar and around the world. These technologies will allow Qatar to sustain economic growth and development, provide a higher standard of living for future generations, create significant employment opportunities, and drive innovation and entrepreneurship.

Qatar's significant investment in technology has positioned the country as a regional leader. Qatar is ranked 23rd among 148 countries in the 2014 World Economic Forum's Networked Readiness Index.[3] Internet penetration is also well above the world average at 88 percent.[4] Assuring the safety and security of broadband services is essential to increasing broadband penetration and usage, and subsequently, increasing confidence in online activities.[5] In addition, Cyber Safety and Security is one of three key programs in the *National ICT Plan 2015: Advancing the Digital Agenda*. This plan is essential to: (1) improve connectivity; and (2) create an economy based on advanced technology solutions and services that will enrich society and distinguish Qatar as a regional leader in Arab-originated digital content.

Qatar has invested billions to improve the country's physical infrastructure. Enhancements include expanding and modernizing Doha's International Airport, building a new seaport, upgrading road infrastructure, and installing a new high-speed rail and metro system. In addition, Qatar is making sizeable infrastructure investments to host the 2022 Fédération Internationale de Football Association (FIFA) World Cup, including technology investments to provide new digital services for visitors and international viewers. These infrastructure enhancements will rely heavily on innovative and sophisticated ICT, presenting not only great opportunities for continued economic growth and expansion, but also opportunities to address cyber security throughout the project lifecycle.

KEY INDICATORS OF ICT USE IN QATAR[6]

- In 2012, 92% of households in the mainstream population had a computer, while 87% of mainstream individuals had a computer.
- In 2012, Internet penetration for mainstream individuals was approximately 88%.
- In 2012, Qatar's mobile penetration was approximately 100%—one of the highest penetration rates in the world.
- In 2012, 74% of companies in Qatar used computers, including desktops, laptops, and newer tablet technologies; an increase from 64% in 2008.
- In 2012, 66% of businesses in Qatar used the Internet; an increase from 51% in 2008.
- The number of businesses with an ICT security policy increased from 37% in 2010 to 61% in 2012.
- In 2012, skilled ICT professionals represented approximately 2% of Qatar's total workforce.

2.1 Threats

Increased ICT use and broadband connectivity bring enormous benefits to government, businesses, institutions, and individuals. However, vulnerabilities often accompany these benefits. As a key provider of clean fuel, a home to global companies, an early adopter of digital technologies, and a leader in regional affairs, Qatar is an attractive target for malicious actors who seek to cause disruption and destruction.

The cyber threat landscape has evolved from one of individual hackers to highly organized groups and advanced cyber criminal syndicates. Cyber attacks are more targeted and sophisticated than ever before. Powerful new malware is capable of stealing confidential data and disabling network infrastructure. Attacks on critical infrastructure, including industrial control systems (ICS), can disable physical machinery, cause catastrophic equipment failure, and even result in loss of life. Qatar, like many other nations, must be prepared to address the following types of threats:

- **Hacktivists.** These are individuals or groups who seek to disrupt systems and networks for a variety of motives, including notoriety, financial gain, or political agendas. They connect across borders to overwhelm targeted websites and access sensitive information. They may seek to harm their enemies by either shaming them or disabling their services. Hacktivists typically launch distributed denial of service (DDoS) attacks, deface websites, access sensitive government data, and publish the personal information of high-ranking persons and business leaders.

- **Advanced Persistent Threats (APT).** These occur when malicious actors use complex and unique malware to quietly gain access to proprietary or personal information and sensitive government information. They may also use customized solutions to take advantage of insiders, social engineering, network hardware, and third-party software to cause various malfunctions, destroy data, and disable networks.

CYBER THREATS TO QATAR

- Trojans, worms, and viruses were among the most common threats to Qatar from April to June 2013.[7]
- The Middle East and North Africa received the third highest volume of SMS spam (1.7 billion spam texts per month) from November 2013 to March 2014.[8]
- Qatar was one of the countries most affected by targeted attacks in 2013.[9]

- **Cyber Crime Syndicates.** These organizations seek account information to make fraudulent transactions or to siphon money. Information theft is also common, as cyber criminals will sell sensitive corporate information to unauthorized individuals or groups. Cyber criminals leverage various methods to achieve their objectives, such as distributing massive amounts of e-mails while posing as banks or other authorities to obtain customer identification and financial information. They may also use large-scale DDoS attacks to overwhelm Internet-dependent enterprises. Qatar anticipates that cyber crime syndicates may use 419 (advance fee) fraud scams to target unsuspecting individuals for financial gain prior to the 2022 FIFA World Cup in Qatar.[10]

- **Malicious Insiders.** These are trusted individuals who are motivated to compromise the confidentiality, integrity, or availability of an organization's information and information systems. Their motives may include financial gain, revenge, or ideology. Insiders do not need to infiltrate perimeter network defenses because they have trusted access to information and information systems and can use various methods to damage or destroy government and business systems.[11]

Cyber attacks are on the rise in Qatar and around the world; therefore, continued vigilance and attention is required. Qatar is committed to ensuring the security of information assets and systems essential to government, businesses, institutions, and individuals.

2.2 Challenges

The adoption of new technologies such as cloud computing and mobile applications, the implementation of smart-grid technology, and the substantial increase in technology users present key opportunities for development and innovation. These opportunities, however, exist in an increasingly fast-paced and evolving environment that will continue to impact Qatar's ability to innovate and compete in the global economy. The challenges in this environment include:

- **Cyber Security Skills and Services Deficits.** Globally, and in Qatar, there is a shortage of workers with the requisite knowledge, skills, and abilities to effectively understand the complexity of ICT and address cyber security issues. In addition, few local providers offer robust and reliable cyber security services. As ICT products and services increase in complexity, these deficits have the potential to grow, and if not adequately addressed, further impact the country's ability to protect critical information infrastructure (CII).

- **Global Supply Chain Risks.** The global cyber ecosystem is a system of interconnected systems that often include multiple components from various sources around the world. It is increasingly difficult to determine the origin and integrity of the components of ICT products. A global supply chain introduces weaknesses that malicious actors may exploit to launch attacks.

- **ICS Connectivity.** ICSs are increasingly connected to business networks and the Internet. While this connectivity provides efficiencies that enable the remote monitoring of the mechanical processes used for oil and natural gas production, electricity generation, and water purification, it also increases the vulnerability of ICSs to cyber threats.

- **Information Sharing Constraints.** Information owners or providers may be reluctant to share information about vulnerabilities, incidents, and best practices for fear of revealing weaknesses. In addition, individual organizations do not always understand that information they possess about cyber threats, vulnerabilities, and effective best practices can be of value to others.

- **Executive Leadership Awareness.** While information technology (IT) managers, chief information officers, chief technology officers, and chief information security officers typically address cyber security for their organizations, cyber security affects more than the smooth operation of an organization—it affects an organization's overall mission and its bottom line. Unfortunately, when communication between executive leadership and IT professionals is limited, the senior-most levels of the organization can lack awareness of the real risks or the resources necessary to implement security requirements, coordinate incident response, and mitigate those risks.

- **Changing Privacy Expectations.** Due to the increased use of personal information within government organizations and throughout international business, countries continue to enact and update privacy laws to protect individuals and their data. Many of these countries require "adequate levels of protection" before allowing international organizations to transfer data to destinations outside their borders.[12] When personal information is not properly protected, organizations face potential risks: for a government organization, this could mean loss of trust in its online services; businesses risk losing customers to global competitors.

2.3 Existing Capabilities to Meet the Threats and Challenges

Qatar recognizes the importance of cyber security and has worked diligently over the last several years to develop and implement cyber security protection measures across the country. These measures have made it possible for government, businesses, institutions, and individuals to respond to the threats and challenges in cyberspace, thereby providing a strong foundation for achieving cyber security objectives. Among these efforts:

- Qatar has developed strategies and implemented policies to safeguard CII that is important to national security and economic prosperity, such as that used for power generation, oil and gas production, financial transactions, healthcare, and government operations. The *National Information Assurance Policy* and the *National ICS Security Standard* provide important guidance on security controls and practices to protect CII and improve Internet security. In addition, as part of the National Information Assurance Framework, Qatar published *Anti-Spam Guidelines* in 2013 to reduce the impact of unsolicited electronic messages (or spam) on entities and individuals.

- To improve the security of financial transactions, the Qatar Central Bank (QCB) issued *Banking Supervision Rules,* which identifies the cyber security controls that banks must follow, such as reporting cyber incidents and attacks to QCB and the Qatar Computer Emergency Response Team (Q-CERT).

- Qatar has established Information Risk Expert Committees (IREC) in the finance, energy, and government sectors. These public-private partnerships deal with a variety of cyber security issues, including threats, vulnerabilities, and consequences; preparedness activities; and mitigation strategies. The IRECs facilitate the exchange of information within each sector and with other stakeholders to enhance CII resilience.

- Qatar has made progress in developing a domestic legal framework that provides national governance for cyber security, combats cyber crime, protects individuals' privacy, and promotes CII resilience. The enactment of Decree Law No. 16 of 2010 on the Promulgation of the Electronic Commerce and Transactions Law established penalties for crimes, including unlawful access to information systems, identity theft, and intercepting information or illegally interfering with an information system. In 2013, Qatar established the National Cyber Security Committee (Committee) to provide an overarching governance structure to oversee collaborative efforts to address cyber security.

- Qatar's investment in developing technical and operational expertise includes the establishment of Q-CERT, a trusted authority that promotes a strengthened cyber environment for the Qatari government and all critical sectors. Q-CERT seeks to proactively prevent and detect cyber threats before they cause significant harm.

- In December 2013, Qatar held its first national-level cyber exercise for critical sectors, including banking and finance, energy facilities and networks, government, and transportation, to enhance these organizations' capabilities to identify and mitigate cyber threats.

- Qatar continues to empower Internet users with the Cyber Safety Education and Awareness programs that provide information on cyber threats and cyber security prevention and detection tools.

- Qatar has established capabilities in digital forensics, enhancing its ability to investigate cyber crime. Qatar's Cyber Crimes Investigation Center and Information Security Center support efforts to safeguard the general public and crack down on criminals who use sophisticated technologies to carry out criminal activities.

- Qatar has formed strong international alliances and is an active participant in global efforts to shape international standards and norms on cyber security, including efforts in the International Telecommunication Union (ITU), the Forum for Incident Response and Security Teams (FIRST), and Meridian Process.[13]

The Qatari government is proactively investing in people, developing policies and processes, and implementing technology to improve cyber security for government entities, businesses, institutions, and individuals. Additional efforts, however, are needed to meet the demands of the future as new threats emerge and ICT reliance grows. Efforts to date have largely been distributed and from the bottom up. As a result, cyber security is neither institutionalized at the national level nor implemented across government entities, businesses, and other institutions. The Qatari government's ability to enforce laws and promote the adoption of cyber security best practices has been limited, making it difficult to combat cyber crime and help entities deter and defend against cyber attacks.

While businesses are beginning to appreciate the risks in cyberspace and take actions to improve cyber security, many follow independent policies and cannot obtain the necessary skills and technologies to institute effective cyber security best practices. Although individuals can access information about cyber threats as well as simple yet effective mitigation techniques, users require additional assistance to help maintain the health of their systems and protect their personal information. The efforts discussed above provide a strong foundation for the future; however, government entities, businesses, institutions, and individuals must work together to enhance Qatar's cyber security.


EDUCATION

3. QATAR'S NEW APPROACH TO CYBER SECURITY

Qatar's new approach to cyber security balances the need to protect interconnected ICT products and services with the need to provide opportunities that maximize the benefits and efficiencies found in ICT advances. The Qatari government will act to defend Qatar's interests in cyberspace from large-scale attacks and incidents that could harm national security. Specifically, the government is prepared to engage in diplomacy; participate in the formation of international rules; and bring military, intelligence, and security expertise to bear on cyber operations to protect the nation.

The NCSS represents an actionable path forward to achieve Qatar's cyber security vision for the future. It is a call to government, businesses, institutions, and individuals to create a more secure cyber environment. This section describes Qatar's cyber security vision and identifies the objectives and initiatives necessary to achieve that vision.

3.1 Vision

Establish and maintain a secure cyberspace to safeguard national interests and preserve the fundamental rights and values of Qatar's society.

3.2 Objectives

To achieve this vision, Qatar seeks to fulfill the following objectives:

Objective 1:	**Objective 2:**	**Objective 3:**	**Objective 4:**	**Objective 5:**
Safeguard national CII.	Respond to, resolve, and recover from cyber incidents and attacks through timely information sharing, collaboration, and action.	Establish a legal and regulatory framework to enable a safe and vibrant cyberspace.	Foster a culture of cyber security that promotes safe and appropriate use of cyberspace.	Develop and cultivate national cyber security capabilities.

Collectively, these objectives provide the foundation for protecting against and preparing for cyber threats (i.e., a proactive approach to cyber security) as well as detecting, responding to, and recovering from threats and challenges (i.e., reactive cyber security efforts).

3.3 Strategic Initiatives

The strategic initiatives below describe how Qatar will make progress against the cyber security objectives. While the initiatives are organized by objective, initiatives for one objective may enable progress and success for other objectives.

Objective 1: Safeguard national CII.

To make progress against the objective, Qatar will:

- Assess the risk to CII;
- Implement cyber security controls and standards to mitigate risk to CII;[14]
- Analyze cyber security trends and threats to CII and provide timely reports to stakeholders;
- Foster the use of trustworthy technology products and services; and
- Continuously monitor the security posture of CII.

Proactive cyber risk management is necessary to ensure that Qatar continues to identify and protect systems that support the delivery of essential services and capabilities. To prevent future cyber incidents and attacks, the government, critical sector organizations (CSO), and other organizations must adopt security controls and prioritize actions to mitigate risk to those assets, systems, and networks essential to Qatar's well-being, prosperity, and security.

In addition, Qatar is building the capability to collect and analyze cyber security incident, alert, and threat information from the Government Network, a network for government entities to connect over a secure communications platform, thereby allowing for improved information sharing and enhanced security for e-services. Through advanced data analytics, Qatar plans to correlate this information to identify trends related to security requirement compliance and cyber threat activity on the network.[15] This continuous monitoring of critical networks will enable Qatar to understand in close to real time the risk to networks, detect incidents, and take immediate actions to mitigate consequences.

Objective 2: Respond to, resolve, and recover from cyber incidents and attacks through timely information sharing, collaboration, and action.

To make progress against the objective, Qatar will:

- Enhance and maintain situational awareness capabilities;[16]
- Establish and continuously enhance incident response capabilities;
- Reduce cyber infections within CII;
- Establish mechanisms and procedures to facilitate timely information sharing and action among stakeholders; and
- Ensure preparedness by conducting cyber security exercises and drills.

Situational awareness is necessary to effectively detect, respond to, and recover from cyber incidents and attacks. Sector regulators and CSOs should have the capability to monitor network activity and maintain situational awareness. Information sharing among the critical sectors will further increase visibility into the current state of threats as well as provide an early warning system for preventing, detecting, and responding to cyber incidents and attacks. Qatar will establish the Cyber Security Coordination Office, which will report to the Prime Minister. The Office will be a focal point for coordinating core cyber security functions, including national cyber incident management. Collaboration and partnership among multiple stakeholders to share information and gain greater situational awareness of threats, incidents, and attacks will enhance Qatar's ability to anticipate, respond to, and recover from incidents and attacks with minimum impact to government, businesses, and society. Furthermore, national and sector-specific cyber exercises will be held regularly to improve information sharing, collaboration, and coordination among stakeholders; identify risks; and drive improvements.

Objective 3: Establish a legal and regulatory framework to enable a safe and vibrant cyberspace.

To make progress against the objective, Qatar will:

- Increase capabilities to combat cyber crime;
- Develop and implement laws, regulations, and national policies to address cyber security and cyber crime;[17]
- Monitor and enforce compliance with cyber security and cyber crime laws, regulations, and national policies; and
- Build and maintain strong international relationships to establish cyber security norms and standards.

Qatar seeks a dynamic legal framework that can keep pace with an evolving cyber threat landscape and new technologies as government entities, businesses, and society continue to mature. The development, enactment, and enforcement of a comprehensive set of laws related to cyber security and cyber crime will empower organizations by clarifying roles and responsibilities. Qatar will collaboratively consider the perspectives and input of relevant government entities and institutions to develop these laws, regulations, and national policies.

The Qatari government is committed to protecting its citizens and residents from cyber criminals. Qatar aims to combat cyber crime by neutralizing and reducing threats via enhanced law enforcement techniques and technologies related to gathering forensic evidence and investigating malicious activity.

The interconnected and distributed nature of cyberspace allows malicious actors to easily cross geographic boundaries. Combating cyber crime and other threats requires international collaboration. The Qatari government will coordinate with the international community to enhance capabilities in Qatar and to combat cyber crime internationally. Furthermore, Qatar will establish entities and acquire the capabilities necessary to increase its ability to prevent and combat cyber crime. Participation in international efforts to develop global cyber security standards and norms, identify and promote best practices, modernize and increase privacy protections, and maintain stable and effective Internet governance will further position Qatar to meet its obligations in cyberspace.

Objective 4: Foster a culture of cyber security that promotes safe and appropriate use of cyberspace.

To make progress against the objective, Qatar will:

- Enhance cyber security awareness across society using multiple channels;
- Encourage individuals to use cyber safety tools and solutions to protect against cyber threats; and
- Promote the development and delivery of cyber security education in schools, colleges, and universities.

Maintaining a safe and secure online environment is essential to fostering digital confidence. To encourage a profitable online economy, consumers must trust that their transactions are secure and their personal information is safe. Raising awareness and encouraging information sharing among government, businesses, institutions, and individuals are two of the most effective ways to improve cyber security. In addition, the appropriate collection, use, and protection of personal information will help consumers safeguard themselves from identity theft.

Qatar has begun building a cyber security culture through cyber safety campaigns, such as Safer Internet Day 2013, and targeted warnings about scams and other online threats via print and social media. Stakeholders from government, law enforcement, businesses, and academic institutions will work together to develop and implement cyber safety solutions and increase awareness of cyber security and associated legal requirements. Fulfilling this objective will require significant collaboration among government entities, businesses, and institutions to educate all audiences on the importance of cyber security and cyber safety.

Objective 5: Develop and cultivate national cyber security capabilities.

To make progress against the objective, Qatar will:

- Develop and maintain a professional cyber security workforce;
- Foster business opportunities and strengthen the competitiveness of the cyber security industry in the public and private sectors; and
- Invest in research to develop and commercialize innovative cyber security technologies and solutions.

Qatar must be at the forefront of educational initiatives that will build and maintain a cyber workforce. This workforce must be capable of defending and protecting against cyber incidents and attacks. Qatar needs employees in government and industry who can recognize new developments in cyberspace and understand how those developments may impact operations.

At the same time, Qatar must also continue to drive the local innovation necessary to identify and implement new solutions that will address the complex cyber security challenges of the future. Local cyber security businesses must be able to flourish and provide robust and reliable cyber security products and services that meet government and critical sector needs and requirements.

Development of a national cyber security research and development agenda that is focused on building solutions to prevent, predict, and overcome cyber attacks will further prepare Qatar for emerging cyber threats. Existing data analytics and social computing capabilities will enable Qatar to pursue an agenda that supports the application of real-time data analytics to detect cyber attacks, conduct forensics and remediate cyber events, and anticipate and ultimately defeat cyber attacks.

4. ACTION PLAN FOR 2014–2018

The Action Plan provides more detail on the Qatari government's plan to achieve Qatar's cyber security vision. The Action Plan is organized by objective. Various stakeholders from government entities and institutions, including the Ministry of Defense, the Ministry of Information and Communications Technology, the Ministry of Interior, Public Prosecution, Qatar Foundation, sector regulators and CSOs, the Supreme Education Council, and other organizations, must work collaboratively with many others to implement these actions for the benefit of Qatar.

Objective 1: Safeguard national CII.	
Initiative	**Action**
Assess the risk to CII	▪ Develop a national CII risk management framework to guide the identification of CII assets and organizations; assessment of threats, vulnerabilities, and consequences; and development of risk profiles ▪ Conduct regular risk assessments of CSOs and other organizations with CII ▪ Conduct dependency and interdependency assessments to identify systemic risks that cut across critical sectors
Implement cyber security controls and standards to mitigate risk to CII	▪ Establish and maintain a CII cyber security standard and maturity model, including specific cyber security controls ▪ Conduct regular evaluations and audits of CSOs to measure the effectiveness of cyber security programs and controls ▪ Develop risk management strategies to protect the most critical services, systems, and organizations and track implementation of those strategies ▪ Share information on risks and risk management strategies across sectors to enable the prioritization of mitigation actions and the investment of resources
Analyze cyber security trends and threats to CII and provide timely reports to stakeholders	▪ Create sector-specific or organizational security operations centers or threat intelligence centers
Ensure the use of trustworthy technology products and services	▪ Develop the capability to evaluate and certify ICT products and systems for use in critical sectors ▪ Develop guidelines that specify security requirements for ICT and cyber security service providers
Continuously monitor the security of CII	▪ Establish a capability to conduct continuous diagnostics and monitoring of networks to better understand risks, promote preventive measures, detect and treat infected devices, and notify affected users

Objective 2: Respond to, resolve and recover from cyber incidents and attacks through timely information sharing, collaboration, and action.	
Initiative	**Action**
Enhance and maintain situational awareness capabilities	▪ Establish and maintain a national cyber security coordination capability to improve Qatar's collective understanding of cyber security threats and incidents and help manage the response to national incidents ▪ Develop a national system for recording and monitoring cyber threats, incidents, and attacks
Establish and continuously enhance incident response capabilities	▪ Develop a process for coordinating and managing cyber incident response ▪ Establish information exchanges between cyber operations centers to facilitate incident response, share information, and provide training opportunities
Reduce cyber infections within CII	▪ Conduct regular assessments of networks to identify and remove malicious code on network infrastructure ▪ Develop and implement tools to detect APTs attacking CII
Establish mechanisms and procedures to facilitate timely action and information sharing among stakeholders	▪ Establish and operate systems and tools for disseminating threat and vulnerability information among trusted stakeholders ▪ Establish additional sector partnerships to bring stakeholders together to address cyber threats and improve CII preparedness and resilience ▪ Establish a forum to bring together security practitioners from across critical sectors to address systemic risks
Ensure preparedness by conducting cyber security exercises and drills	▪ Hold national cyber security exercises and incorporate lessons learned into policies, procedures, and operational capabilities ▪ Conduct sector-specific cyber security exercises to assess and test CSOs' incident response capabilities ▪ Participate in or host international cyber exercises to further establish relationships and test incident response coordination capabilities

Objective 3: Establish a legal and regulatory framework to enable a safe and vibrant cyberspace.	
Initiative	**Action**
Increase capabilities to combat cyber crime	▪ Create new abilities to investigate criminal activity through training, new forensic techniques, and access to technology ▪ Enact a Cyber Crime Law to provide law enforcement with additional authority and define criminal acts ▪ Collect statistics on cyber crime trends and methods
Develop and implement laws, regulations, and national policies to address cyber security and cyber crime	▪ Conduct regular reviews of laws and other policies to ensure they remain adequate to address emerging cyber security needs ▪ Enact proposed laws (e.g., Data Privacy and Protection Law, Critical Information Infrastructure Protection Law) to prevent misuse of personal information and protect CII
Monitor and enforce compliance with cyber security and cyber crime laws, regulations, and national policies	▪ Establish a scheme and process for determining if CSOs are adhering to laws and regulations and if they have implemented national policies ▪ Develop guidance and resources for CSOs, such as training, tools, and audit workshops, to promote the adoption of cyber security best practices and facilitate compliance with requirements ▪ Evaluate the NCSS and report annually on government and CSO efforts to implement the NCSS and improve cyber security
Build and maintain strong international relationships to establish cyber security norms and standards	▪ Engage regularly with international partners on policy and operations to raise cyber security awareness, identify and address threats, and coordinate actions to improve cyber security worldwide ▪ Enhance existing and establish new bilateral and multilateral agreements to promote information sharing, enable cyber crime investigations, and support cyber operations

Objective 4: Foster a culture of cyber security that promotes the safe and appropriate use of cyberspace.	
Initiative	**Action**
Enhance cyber security awareness across society using multiple channels	▪ Establish and maintain national cyber security awareness across different demographic groups, such as young children, students, parents, older adults, government employees, small and medium-sized enterprises, chief executive officers, and others ▪ Create an awards program to recognize excellence in cyber security for key contributions, such as innovative solutions and services or implementation of security controls and best practices
Encourage individuals to use cyber safety tools and solutions to protect against cyber threats	▪ Work with Internet service providers (ISP) and others to help individual users determine the health of their devices
Promote the development and delivery of cyber security education in schools, colleges, and universities	▪ Work with colleges and universities to develop and implement cyber security curricula and educational programs at the graduate and post-graduate levels ▪ Work with schools to establish cyber safety education programs as well as provide school teachers and administrators with materials to support the delivery of cyber safety education

Objective 5: Develop and cultivate national cyber security capabilities.	
Initiative	**Action**
Develop and maintain a professional cyber security workforce	▪ Develop a cyber security workforce competency model ▪ Establish local and national cyber security competitions for different age groups to identify and recognize highly talented Qataris, develop their cyber skills, and encourage them to pursue careers in cyber security
Foster business opportunities and strengthen the competitiveness of the cyber security industry in the public and private sectors	▪ Hold a Cyber Innovation Challenge to encourage small and medium-sized enterprises to develop innovative cyber security solutions and services
Invest in research to develop and commercialize innovative cyber security technologies and solutions	▪ Develop a national cyber security research and development agenda to drive investment in solutions that can be rapidly transitioned from development to operation ▪ Establish strategic partnerships with local and international universities, institutes, and research organizations for cyber research and development projects

5. IMPLEMENTATION APPROACH

Successful implementation of the NCSS requires continuous commitment, governance, and action by various stakeholders who are collectively responsible for the national approach to cyber security. These stakeholders are connected by a shared set of guiding principles that support Qatar's cyber security vision.

5.1 Guiding Principles

Qatar's approach to cyber security is based on the following three principles:

The Government Will Lead the Way. Governments have an important responsibility to safeguard government information, systems, and networks and ensure their confidentiality, integrity, and availability. The Qatari government will therefore lead by example, implementing cyber security requirements while building and adopting innovative and new technologies that provide the foundation for the economy.

Cyber Security Is a Shared Responsibility. Cyber security should be the responsibility of all government entities, businesses, institutions, and individuals.

- The Qatari government is responsible for protecting its information, systems, and networks; investing in the people, processes, and technologies necessary to safeguard the services that society relies on; and setting the direction for Qatar's continued economic development and growth.
- Businesses are responsible for protecting their information, systems, and networks from cyber threats; sharing information; and responding should cyber incidents and attacks occur.
- Individuals are responsible for being aware of threats; adopting best practices; understanding who is collecting their personal information; and securing their own information, systems, and networks.

Fundamental Rights and Values will be Preserved. In cyberspace, security and privacy are tightly intertwined. Strong security measures and sound best practices are encouraged to protect personal or private information from unauthorized access or misuse. Qatar will pursue cyber security policies and initiatives that preserve society's values and expectations, consistent with laws and regulations.

VALUES IN CYBER SECURITY

- Protect government, businesses, institutions, and individuals from unacceptable online content and behaviors;
- Show tolerance and respect;
- Embrace innovation and the free flow of ideas and information;
- Support collective and collaborative efforts to address complex cyber security challenges; and
- Promote an environment that rewards investment in security and technology.

5.2 Governance

Strong governance is needed to implement and manage execution of the NCSS. To that end, Qatar will establish the Cyber Security Coordination Office (CSCO), which will report to the Prime Minister and be the focal point for cyber security activity across Qatar. The CSCO will be responsible for: (1) establishing priorities to promote the highest level of cyber security in Qatar, (2) providing strategic direction for Qatar's cyber security efforts, and (3) working in close partnership with organizations with cyber security missions and mandates to fulfill the objectives of the NCSS.

It is essential that stakeholders commit to successfully implementing the NCSS. Stakeholders will be responsible for defining their own detailed implementation plans for the actions they need to fulfill. Government entities, CSOs, and other institutions will need to keep track of milestones and progress and be prepared to provide regular updates to the CSCO. In addition, stakeholders should commit to active and ongoing coordination across all levels of society to improve cyber security.

5.3 Performance Measurement

Stakeholder coordination, integrated decision making, and tracking progress will be required to accomplish the strategic initiatives and actions outlined in the NCSS and supporting documentation. The CSCO will define mechanisms to assess progress, work with the Committee and stakeholders to make decisions regarding prioritization or Action Plan amendments, and monitor efforts to advance the objectives using a variety of metrics. In addition, the CSCO will report annually on progress against the objectives, thereby providing ongoing visibility into efforts to secure Qatar's cyberspace.

6. MOVING FORWARD

Qatar will revise the NCSS every four years, or as necessary, to make coordinated adjustments and refinements to account for national and international legal, operational, and technological developments. This review will seek to align Qatar's cyber security vision with any new national-level strategy documentation (e.g., development strategies) and obtain input from stakeholders, as appropriate.

As new, complex, and global cyber security challenges emerge and Qatar's dependence on ICT increases, Qatar must be vigilant and continuously work in partnership to enhance its cyber security readiness and resilience in accordance with the NCSS. More than any other national-level document, the NCSS demonstrates Qatar's commitment to protecting Qatar's cyberspace for future generations.

ACKNOWLEDGEMENTS

We would like to thank the members of the National Cyber Security Committee, chaired by Dr. Hessa Al-Jaber, Minister of Information and Communications Technology, for their active participation and contributions during the development of the NCSS.

Brigadier **Saleh Khamis Al-Kubaisi**
Vice Chair, National Cyber Security Committee
Manager of Information Systems Department
Ministry of Interior

Lieut. Col. **Nawaf Ahmad Al-Rumaihi**
Head of Corporate Information Technology
State Security Bureau

Dr. **Saif Mohammed Al-Kuwari**
Director of Information Systems and Technology
Ministry of Foreign Affairs

Mr. **Ali Abdulla Al-Siddiqi Al-Emadi**
Manager of Information and
Communication Technology
Qatar Petroleum

Mr. **Ahmad Sultan Al-Mulla**
Manager of Information Technology Department
Ministry of Justice

Brigadier Eng. **Abdulaziz Falah Al-Dosari**
Director of Technical Affairs
Qatar Armed Forces

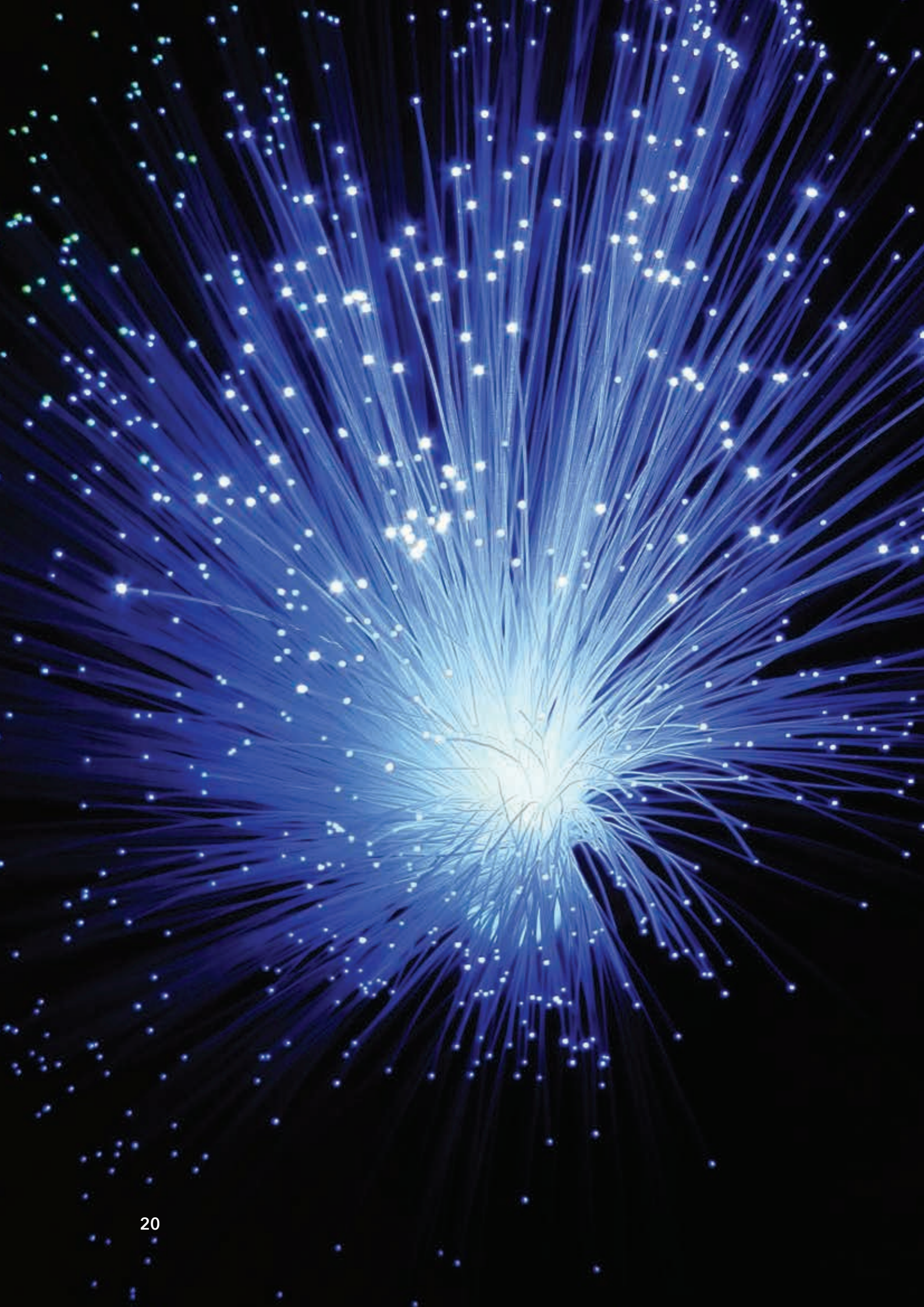
Mr. **Abdullah Mohammed Al-Naimi**
Chief Operating Officer
Qatar Credit Bureau

Mr. **Mustapha Huneyd**
Senior Manager for Corporate
Information Security
Ooredoo

Ms. **Maryam Haji Abdullah**
Manager of Information Technology Department
Public Prosecution

Mr. **Khalid Sadiq Al-Hashmi**
Executive Director for Cyber Security
Ministry of Information and
Communications Technology

We would like also to thank Mr. Rashid Zayed Al-Naemi, Cyber Security Specialist, Ministry of Information and Communications Technology, and Dr. Hoda Baraka, Advisor to the Minister of Information and Communications Technology, for their contributions to the development of the NCSS.



APPENDIX A. ABBREVIATIONS

APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CSCO	Cyber Security Coordination Office
CSO	Critical Sector Organization
DDoS	Distributed Denial of Service
EU	European Union
FIFA	Fédération Internationale de Football Association
FIRST	Forum for Incident Response and Security Teams
ICS	Industrial Control System
ICT	Information and Communications Technology
IREC	Information Risk Expert Committee
IT	Information Technology
ITU	International Telecommunication Union
NCSS	National Cyber Security Strategy
QCB	Qatar Central Bank
Q-CERT	Qatar Computer Emergency Response Team

APPENDIX B. DEFINITIONS

Awareness Campaign.
Communications and outreach activities designed to increase knowledge and support for cyber security, improve understanding of cyber threats and security practices, and encourage adoption and ownership of necessary changes in online behaviors.

Capabilities.
People, processes, and technologies that support cyber security efforts.

Critical Infrastructure.
Physical assets, systems or installations, which if disrupted, compromised, or destroyed, would have a serious impact on the health, safety, security, or economic well-being of Qatar or the effective functioning of the Qatari government.[18]

Critical Information Infrastructure (CII).
The information and communications technology systems, services, and data assets that are critical to Qatar based on the following classification criteria:

1. Identify the organization's key, core business processes and their dependency on assets owned and managed by the organization (e.g., power plant, refinery, general ledger, etc.);
2. Use impact severity table to determine an impact score for the loss/non-functioning of each key asset; and
3. Classify all assets as critical when the criticality score is greater than twenty (20).[19]

Impact Severity Table				
Impact Factor/Score	**Low/1**	**Medium/3**	**High/5**	**Severe/15**
Population Impact *(Potential for loss of life)*	<10	10–100	100–500	>500
Economic Impact/QAR *(Direct damage and restoration cost including CII networks/systems)*	<20M	20M–200M	200M–1B	>1B
Interdependency Impact *(On other sectors)*	Minor Impact	Moderate Impact/ Disruption	Significant Impact/ Disruption	Debilitation Impact
Scope Impact	Local	Large Local or Multiple Sectors (Partially)	National or Single Sector (Fully)	International or Multiple Sectors (Fully)
Service Impact *(Recovery time in days)*	<1	1–30	30–180	>180
Public Confidence Impact	Public perceives low national risk, high ability to control	Public perceives moderate national risk, moderate ability to control	Public perceives high national risk, low ability to control	Public perceives severe national risk, ability to control in doubt

Critical Sector.
The critical sectors in Qatar include but are not restricted to:

- Energy, Electricity, and Water
- Finance
- Government
- Healthcare
- Information and Communications Technology
- Transportation

Critical Sector Organization.
An organization that owns and/or operates a substantial portion of CII in Qatar.[20]

Cyber Crime.
Misconduct or crime committed using technology. Examples of cyber crime may include illegal access to systems or information, fraud, identity theft, or content-related offenses such as spam.

Cyber Security.
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. Cyber security 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. The general security objectives comprise the following: confidentiality, integrity (which may include authenticity and non-repudiation), and availability.[21]

Cyber Security Controls.
Safeguards or counter measures to ensure the confidentiality, integrity, and availability of information assets, systems, or networks and mitigate the risk to those assets, systems, and networks.

Cyberspace.
A virtual or electronic environment that results from the interdependent network of information and communications technology (e.g., the Internet, telecommunications networks, computer systems, and embedded processors and controllers) that links people with services and information.

Ecosystem.
A variety of interconnected and interdependent organizations, systems, and devices that interact for multiple purposes using different processes.

Exercise.
An interactive engagement (half-day to five days or more) that enables participants to react to a plausible scenario in a risk-free environment. Exercises provide an effective tool for testing incident response plans; validating policies, plans, and procedures; identifying vulnerabilities and reporting requirements; assessing risk and preparedness; discovering interdependencies and response gaps; creating a shared perspective and buy-in among diverse stakeholders; and building a common understanding of roles and responsibilities. An exercise may also be referred to as a simulation, seminar, tabletop, drill, or wargame.

Personal Information.
Recorded information about an individual, such as name, address, e mail, phone number, marital status, healthcare or financial data, employment history, and associations.

Policy.
A type of instrument such as a strategy, standard, framework, guideline, or other document that establishes, implements, guides, describes, or explains organizational responsibilities, authorities, actions, and procedures.

Resilience.
The ability to prepare for, adapt to, withstand, and rapidly recover from disruptions resulting from deliberate attacks, accidents, or naturally occurring threats or incidents.

Unintentional Insiders.
Those with authorized access to an organization's network, system, or information. Unintentional insiders can represent a threat due to non-malicious action or inaction that causes harm or impacts the confidentiality, integrity, or availability of networks, systems, or information.

APPENDIX C. REFERENCES

1 Resilience is the ability to prepare for, adapt to, withstand, and rapidly recover from disruptions resulting from deliberate attacks, accidents, or naturally occurring threats or incidents.

2 *Qatar National Vision 2030* envisions a prosperous country in which there is economic and social justice for all, and in which nature and man coexist harmoniously. It promotes human, social, economic, and environmental development to provide educational opportunities, preserve Qatar's national heritage, and maintain financial and economic stability.

3 Networked Readiness Index 2014, World Economic Forum, http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf.

4 "Percentage of Individuals Using the Internet," International Telecommunication Union (ITU), http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

5 The National Broadband Plan for the State of Qatar provides the necessary actions to maximize the use of broadband.

6 ictQatar, *Qatar's ICT Landscape 2013: Business;* ictQatar, *Qatar's ICT Landscape 2013: Households and Individuals*.

7 Microsoft Security Intelligence Report, Volume 15 January through June, 2013 (http://www.microsoft.com/security/sir/default.aspx)

8 April 2014 Threat Stats—SMS Spam Volume by month for each region, SC Magazine (http://www.scmagazine.com/april-2014-threat-stats/slideshow/1906/#2)

9 TrendLabs 2013 Annual Security Roundup, Cashing in on Digital Information: An Onslaught of Online Banking Malware and Ransomware, Trend Micro (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cashing-in-on-digital-information.pdf)

10 "419 Scammers Planning Ahead with 2022 World Cup Scams," Symantec, February 3, 2011, http://www.symantec.com/connect/blogs/419-scammers-planning-ahead-2022-world-cup-scams

11 Unintentional insiders—those with authorized access to an organization's network, system, or information—can also represent a threat due to non-malicious action or inaction that causes harm or impacts the confidentiality, integrity, or availability of networks, systems, or information.

12 For example, the European Union (EU) Data Protection Directive (Article 25[6] of directive 95/46/EC) requires special precautions to be taken when transferring data outside EU countries. See http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm for more information.

13 ITU is a United Nations agency that specializes in ICT issues, particularly infrastructure development, standardization, and international cooperation. FIRST is the global association of computer security incident response teams; it promotes information sharing and promulgates computer security best practices and tools for incident response. The Meridian Process facilitates cooperation among governments on CII protection and provides participating countries with the opportunity to share best practices from around the world.

14 Cyber security controls are safeguards or counter measures to ensure the confidentiality, integrity, and availability of information assets, systems, or networks and mitigate the risk to those assets, systems, and networks.

15 For example, firewall, intrusion detection system/intrusion prevention system, and proxy server logs.

16 Capabilities include people, processes, and technologies that support cyber security objectives.

17 Policies include types of instruments such as strategies, standards, frameworks, guidelines, or other documents that establish, implement, guide, describe, or explain organizational responsibilities, authorities, actions, and procedures.

18 Unofficial English translation of the Critical Information Infrastructure Protection Law.

19 Ibid.

20 Ibid.

21 "Overview of Cybersecurity," International Telecommunication Union (ITU), ITU-T X.1205, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

ict QATAR