Ministry of Information and Communications Technology

National Information Assurance and Cyber Security Strategy (NIACSS)

2012

Acknowledgement

This document would not have been possible without the support of many people.

Document Review

Ver.	Type	Date	Comments
1.0	Draft	June 1st , 2011	Initiated by Minister of ICT, Eng. Atef Al Tell
2.0	Draft	July 26th, 2011	CNIP program is added by SPI Adv., NITC(Dr. Ahmed Otoom)
3.0	Draft	August 14th, 2011	Review by Minister of ICT, Eng. Atef Al Tell
4.0	Draft	August 15th, 2011	Review by Timothy Bloechl on V2.0
5.0	Draft	August 18th, 2011	Review by GM & SPI Adv., NITC
6.0	Draft	September 4th,2011	Review by PS Dir. & E-Gov Dir., MoICT
7.0	Draft	September 11th, 2011	Review by PS Dir., MoICT, SPI Adv., and GM, NITC
8.0	Final Draft	October 16th, 2011	Public Review
9.0	Final	July 30th, 2012	Review by Minister of ICT, Eng. Atef Al Tell
9.0	Approved	September 24th,2012	Approved by Cabinet

Point of Contact

Please direct inquiries about this strategy, if any, to the following point of contact

Organization: National Information Technology Center (NITC)
Name: Dr. Ahmed Otoom
Title: DG's Advisor for the Implementation of E-Gov. Information Strategies and Policies
Email: ahmad.o@nitc.gov.jo
Telephone: (+962 65300269)
Fax: (+962 65300277)

Table of Contents

1. EXECUTIVE SUMMARY

Jordanian Government organizations and private sector have different approaches to ensure the security of their information systems and critical information infrastructures. However, these approaches: are generally basic; not systematic; subjective; have no clear definition or boundaries, are not thorough; do not meet international standards; and do not deal effectively with threats emerging from cyberspace. Moreover, cyber security efforts across Jordanian Government organizations and private sector are not consolidated and risks are not addressed at the national level.

The revolution in information and communication technologies, powerful personal computers, high-bandwidth and wireless networking technologies, widespread use of the internet, and the high volume of information exchanged over the internet and local networks make it very difficult within currently adopted approaches to obtain and maintain the desired level of information security. The weaknesses in current approaches, coupled with rapid advancements in technology place national networks at higher risks. The nation needs secure and reliable national information infrastructures which are resilient to malicious attack or arbitrary disruption to maintain a high level of trust in these systems across government, with the private sector, and within the citizenry.

Government of Jordan recognizes the challenges posed by malevolent actors' access to cyberspace. Reports of cyber-attacks and their impact are a routine, daily occurrence around the world. Furthermore, while we know what is known from these reports, the high probability of unreported or unknown attacks or intrusions causes even greater concern. These challenges require coordinated and focused efforts from all government organizations and strong partnerships between the public and private sectors, and with our citizens. Meeting these challenges requires all information assurance and security plans and activities adhere to a nationwide strategy to guarantee consistency and successful implementation of a coordinated and effective cyber defense.

Information Assurance: technical and managerial measures designed to ensure the confidentiality, integrity, availability, authenticity, possession or control, and utility of information and information systems.

This National Information Assurance and Cyber Security Strategy (NIACSS) is not only intended to secure the Internet cyberspace, it should provide a secure and trusted computing environment for all IT-related infrastructure throughout all identified national priorities herein. The NIACSS should augment the overall National Security Strategy (NSS) for Jordan. The main purpose of the NIACSS is to give structure, involve, and empower all concerned organizations to more effectively secure computer networks they own, operate, control, or interact with.

The NIACSS aims to provide a strong foundation to secure the National IT Infrastructure and is not only confined to secure the Internet cyberspace

NIACSS identifies strategic objectives, national priorities, and an implementation road map. The strategic objectives support the Government's vision for the path ahead. This vision aims to improve information assurance and cyber security measures in Jordan. Supporting national information security priorities address the critical needs required to guarantee a successful and effective protection of the national cyberspace. The NIACSS also considers the following important areas: Organization, Technical, Legal, Capacity Building, and Partnerships. National cyber security priorities demand collaboration within the Government, and with international partners, the private sector, and the population. The implementation road map guides successful implementation of the identified priorities towards achieving the strategic objectives.

This document is organized as follows. Sections 2 and 3 list the Scope and the Strategic Objectives of (NIACSS), respectively. Section 4 lists National Information Security Priorities. Section 5 outlines the Strategy Implementation Road Map. Finally, Section 6 summarizes the overall strategy.

2. SCOPE

The National Information Assurance and Cyber Security Strategy applies to all information domains to achieve comprehensive information security in Jordan. Although the government is the developer of this strategy, a successful implementation requires collaboration among all involved parties: government, international partners, and the private sector. Efforts of involved parties must complement rather than conflict with each other. Strategies and policies developed by the private sector should augment, comply, and be consistent with this strategy.

3. STRATEGIC OBJECTIVES

3.1. Strengthen Jordan's National Security by Preventing Cyber Attacks to Critical Information Infrastructures.

3.2. Minimize Risks to Critical Information Infrastructures and Government Networks by Reducing Vulnerabilities.

3.3. Minimize Damage and Recovery Time from Cyber Attacks regardless of source or intent.

3.4. Enhance Jordan's Economy and improve National Prosperity by Increasing Confidence and Trust in Government, and by extension, Private Information Systems Security, thereby encouraging investment and creating opportunities for enhanced collaborative processes.

3.5. Increase Information Security Awareness and its importance to National Security through a National Information Security Awareness and Training Program.

4. NATIONAL INFORMATION SECURITY PRIORITIES

To achieve the National Strategic Objectives listed above (Section 3), Government of Jordan organizes its NIACSS across nine major national interdependent priorities, each priority demanding collaboration across Government, and with international partners, the private sector, and the citizenry. Taken as a whole, these priorities form the action lines of the NIACSS Implementation Roadmap. The nine priorities (not sorted in order of importance**)** are:

1) Risk Management Program
2) National Computer Emergency Response Team (JOCERT)
3) Security Awareness and Capacity Building Program
4) National Information Security Standards and Policies
5) Legal and Regulatory Regime
6) National Encryption System
7) International Information Security Cooperation Program
8) Securing National Information Systems/Networks
9) Critical National Infrastructure Protection (CNIP) Program

4.1. Risk Management Program

A Nation-Wide Risk Management Program will establish the needed framework for high level impact risk management on the national level. It will not address individual risks, for government entities and private sector, with little or no impact on the national level. Government organizations and private sector must address and manage their own risks. They must develop their own risk management programs or plans that are inline with the Nation-Wide Risk Management Program.

Government organizations and private sector will develop and maintain risk management programs that are inline with the nation-wide risk management program.

In cyberspace, risks can never be reduced to zero and there is no 100% secure system.

Therefore, understanding the magnitude and potential impact of these risks informs organizational prioritization against limited resources. Proper risk assessment and management in Government organizations will contribute to business continuity and mission success. Organizations should assess risk both qualitatively and quantitatively by identifying threats and vulnerabilities. The likelihood and impact of each risk should be evaluated against organization missions and assets to identify security gaps. These gaps then define the true nature of the potential risk faced by the organization against which leaders must decide either to accept the risk, or take action to minimize or reduce the potential threat.

As no system is risk-free, government organizations should maintain disaster recovery plans that are products of effective risk management programs. Successful disaster recovery plans ensure organizations are back in operation in a short time period after incidents occur. Government organizations must adapt to the following strategies, for responding to risks, where applicable: mitigation, transference, acceptance, and avoidance.

4.2. National Computer Emergency Response Team (JOCERT)

Information systems are targets for cyber-attack due to: 1) revolutionary growth of information and telecommunication technologies in government organizations and big business as well; 2) availability of Government E-services through the E-Government program; 3) increasing internet penetration rate and e-commerce usage, and; 4) the increasing number of connected systems and networks.

Government of Jordan will establish a National Computer Emergency Response Team (JOCERT)

Cyber-attacks increase the possibility of data disclosure, data manipulation, data loss, and systems sabotage. These factors trigger the urgent need for a National Computer Emergency Response Team (JOCERT). At its highest level, the JOCERT helps the nation prepare for, prevent, respond to, and recover from cyber incidents and attacks. The JOCERT, which will require management and/or operational assets at national and organizational levels, will enable Jordan to be better positioned to manage and respond to cyber-

attacks and incidents to achieve a higher level of efficiency and transparency in dealing across government, with citizens and the private sector.

The JOCERT will coordinate with regional and international emergency warning systems and should offer the following four kinds of capabilities/services: proactive, reactive, quality management, and training. JOCERT will deal with information system security incidents utilizing the following methodology: receiving alerts, analyzing incidents, responding to incidents, and announcing incidents, respectively.

4.3. Security Awareness and Capacity Building Program

Cyber Security and Information Assurance Awareness and Training Programs are a critical priority. Establishing and maintaining these programs empowers Government organizations and private sector and yields a great potential return on investment in terms of contributing to the protection of critical information resources. Organizations which continually train their workforce in security policy and role-based security responsibilities will have a higher rate of success in protecting critical information. Government of Jordan will develop these programs in cooperation with the private sector. These programs should have the following characteristics:

> Government of Jordan will design, develop, and implement CS&IA Awareness and Training Programs.

- Increases public awareness of cyberspace security issues and efforts.
- Addresses cyberspace security policy, tactics, techniques, and procedures including response plans in the event of cyber-attack.
- Expands the government information technology workforce especially those focused on cyberspace security.
- Involves and encourages academic and research institution efforts to improve Cyberspace security education, knowledge and capabilities.
- Include a strong and well-balanced On-the-Job Training (OJT).

4.4. Develop National Information Security Standards and Policies

An authorized government entity, National Information Assurance and Security Agency (NIACSA) (Section 5), will develop and or customize nationwide cyberspace security overarching standards considering current international standards, policies, and best practices, such as encryption algorithms, encryption keys management, software development, physical and logical access control, and networks security. NIACSA will develop the necessary guidelines and training programs to guarantee that related entities can implement such standards and policies

> The efforts of implementing nationwide overarching standards and policies will be assigned or managed by NIACSA (Section 5). NIACSA will also audit and evaluate the compliance with these standards and policies. NIACSA should have a flexible organizational structure in which development, review, evaluation and audit are assigned to responsible departments such that segregation of duties is maintained.

> Information Security Policy must be developed and enforced to meet optimum information security requirements for government organizations and private sector.

Individual government entities and private sector that have different security requirements will have the ability to develop their own security policies that do not contradict with the nationwide security policy. NIACSA, Government entities and private sector must co-operate to ensure that their policies augment, comply, and be consistent with the nationwide policies.

A nationwide policy should be developed, published and communicated to provide direction and support for information security per this strategy, relevant laws, regulations and international information security standards.

The resulting information security standards and policies should be reviewed at planned intervals to accommodate for the rapid change of the cyberspace environment to ensure currency and effectiveness. Standards and policies should have a single owner for development, review and evaluation. At national and organizational level, officials and any other necessary party will be designated to help develop, promulgate, and review standards and policies. There should be defined management review procedures. Reviews should provide recommended improvements or changes needed according to law, and organizational and technical environments. The reviews should also consider feedback from interested parties, status of preventive and corrective actions, trends related to threats and vulnerabilities, reported incidents and actions taken to respond and recover from these incidents. .

Information Security Policies should:

- Assign and define information security classification levels required for the Government organizations.
- Comply with Jordanian laws and adopted international standards.
- Define organizational roles and responsibilities.
- Define policy distribution, training, and implementation timelines.
- Provide compliance and certification procedures, and approval authorities.
- Provide procedures for corrective actions for non-compliance.

4.5. Legal and Regulatory Regime

The need for empowering laws and regulations to support and enforce the implementation of the strategy is a must. A specialized committee should be formed with members from the Ministry of Information and Communications Technology and Ministry of Justice experts to further explore this area and provide recommendations.

Government organizations and private sector need to develop their own internal regulations consistent and compliant with national laws to cover information security-related legal issues.

4.6. National Encryption System

A National Encryption Centre (NEC) will be established to manage, control, plan, monitor, and enforce the national strategic encryption policies and later on produce indigenous national algorithms and keys. Government organizations and involved parties will adhere to the encryption standards, policies, or strategic guidelines approved and or developed by the NEC. While the private sector will have the flexibility to use their own encryption solutions, these solutions should never violate the approved standards, policies, or strategic guidelines.

A National Encryption Centre should be established

Government organizations and private sector need to use encryption along with other security measures to protect classified sensitive and critical information assets. The following strategic needs list for Government organizations will ensure investment in encryption today delivers strategic value to national security efforts:

4.6.1 A national encryption policy will be developed, coordinated, and placed in force.
4.6.2 Applicable international standards and best practices should be considered for adoption for better encryption management.
4.6.3 Encryption should be applied to all data deemed sensitive or classified.
4.6.4 Encryption should be considered where necessary when data is stored, transmitted/disseminated and or processed.
4.6.5 Government organizations must ensure encryption is used in parallel with other necessary security measures (defense-in-depth).
4.6.6 Government organizations must continually monitor or audit all automated and manual actions and ensure procedures are in place to guarantee the integrity and security of encryption capabilities and associated logs.

4.7. International Information Security Cooperation Program

Jordan is connected to other countries through information networks. Cyber-attacks can cause serious problems for national security. Therefore, the government and all concerned must prepare to defend critical infrastructures and respond effectively. To do so requires international cooperation.

Jordan needs to be part of an international effort to raise awareness, develop and promote security standards and best practices, investigate and prosecute malevolent users across borders, and negotiate and conclude bilateral and multi-national agreements. The following actions support this priority:

4.7.1 Share and analyze information on vulnerabilities, threats and incidents.

4.7.2 Participate in, utilize, and get benefits from current international efforts, such as cyber war exercises and international cyber alarm initiatives.

4.7.3 Coordinate investigations of cyber-attacks and other potential computer-related crimes with international partners as required by law and agreement.

4.7.4 Promote research and development and encourage the application of internationally certified security technologies.

National information security cannot be achieved or strengthened to a required level without cooperating with other international governments, research centers, universities, organizations, and the private sector.

4.8. Securing National Information Systems and Networks

Securing national systems should not only prevent security breaches, but also detect and respond to possible attacks. Employing Defense-in-Depth multiple layers of protection methods is critical to securing government systems and networks. Defense-in-Depth is not limited to technical security methods and procedures. Defense-in-Depth should also be resilient to accommodate rapid change in the cyber environment. It also includes a close examination of personnel security, network setup and configuration, and operational procedures. Security vulnerabilities across personnel, technology, and operations must be considered throughout the system's life cycle.

> Employ Defense-in-Depth to protect national information systems

It is through the combination of people, technology and operations which provides the greatest cyber security posture. Tactics, techniques, and procedures must be developed in the following areas to ensure success:

4.8.1. **Personnel Security**

Government organizations and private sector must issue security clearances to users, system administrators, and any other parties using or accessing information systems. Security clearance validation and renewal requires appropriate management, background checks, and commitment of resources. Also, cleared personnel require a “need-to-know” and integration in physical security systems to ensure control and monitoring of man and machine in the government information systems. Private sector will manage personnel security issues under its control. Private sector still needs to cooperate with the authorized government organization(s) to fulfill personnel security requirements outside its authority.

4.8.2. **Physical Security**

Government organizations and private sector must employ all necessary measures to deter, delay, and detect attackers or potential insider threats from accessing a facility, resource, or information stored on physical media. When the physical environment is threatened, appropriate response options must be in place. Organizations should plan for this event, as well as natural disasters, manmade catastrophes, accidental damage and other various events which could damage the information infrastructure. These plans should be tested and exercised regularly to ensure response times and effectiveness.

4.8.3. **Network and Communication Security**

Government organizations and private sector must defend the communications networks, critical infrastructures, networks boundaries, and computing systems that they own through using proper COMSEC and TRANSEC technologies, protection paths and secure alternatives. National networks and communication infrastructures must be secure, reliable and available, they must maintain the trust of government, private sector and individuals, and should be resilient to malicious or arbitrary disruption and or deception.

4.8.4. **Software Security**

Government organizations and private sector must ensure software consistently exhibits required desirable properties even when the software comes under attack. It should minimize the numerous flaws and errors in software that are often located and exploited by attackers to compromise the software's security and other required properties. Software should be able to resist most attacks and tolerate the majority of those attacks it cannot resist. If neither resistance nor tolerance is possible and the software is compromised, it should be able to isolate itself from the attack source and

degrade gracefully. Resistance and tolerance are relatively ensured by having software manufactures a) adhere to software security development lifecycle and b) constant vulnerability assessment, analysis of perceived vulnerabilities, and rapid counter-measures or other configuration changes.

A certification and accreditation program should be established for all critical software that will be used in government entities and business entities that operate critical national infrastructure. Moreover, Government organizations and private sector will follow national guidelines, standards, rules and best practices needed to guarantee software acquisition, procurement, outsourcing, in-house developed software, and Commercially available Off-The-Shelf (COTS) components will deliver software that commit to the national security rules and do not yield security breaches.

4.8.5. **Procedural Security**

Government organizations and private sector must ensure information security related procedures are in place, well-understood, and successfully implemented. These procedures should meet the set of regulations, rules, best practices, national information security policies and standards that direct how an entity manages, protects its communications and distributes sensitive information.

4.8.6. **Electro-Magnetic Emissions (Radiations) Security**

Government organizations and private sector must ensure that sensitive information is not leaked through system electro-magnetic emissions (radiations). Organizations should take necessary measures to protect systems having sensitive information and prevent adversaries from exploiting this vulnerability utilizing Tempest Devices, shielding, Faraday caging and or any other necessary measures.

4.9. Critical National Infrastructure Protection (CNIP) Program

Government of Jordan will cooperate with the private sector to establish a program responsible for information assurance and cyber security related-issues for the Critical National Infrastructure (CNI) including SCADA systems. The CNI are those information assets or systems of critical value to Jordan. Examples include telecommunications, ISP providers, banking and finance, health institutions, electrical power grid, and water supply. CNI support economic, political and social life of Jordan such that any entire or partial loss or compromise of these systems may result in a serious impact on a national level; or may be of instant concern to the Government and people.

A CNIP program is needed to secure systems of critical value to Jordan

The government should regulate, co-operate and work closely with those parties who manage, own, or operate CNI. The government should engage with those parties in order to regulate and provide security guidance in both of physical and virtual domains to secure CNI.

5. IMPLEMENTATION ROAD MAP

Having an NIACSS represents only the first step towards achieving the expected objectives. Jordan Government is committed to a persistent implementation mechanism utilizing the appropriate resources to fulfill this strategy.

Due to the abstract high-level nature of NIACSS, it will be explored further by NIACSA that will be established. NIACSA will provide enough details in a supplementary document "**NIACSS Implementation Road Map**". The Road

A detailed NIACSS Implementation Road Map Document is required.

Map document will translate priorities and objectives listed in NIACSS into specific well-defined initiatives/projects. The implementation of these initiatives/projects will contribute to realizing the overall identified NIACSS objectives.

NIACSS calls for establishing a well-defined organization called National Information Assurance and Cyber Security Agency (NIACSA). NIACSA should be the focal point for all information assurance and Cyber Security related issues and assigned the following responsibilities:

5.1. Be the single point of reference and a coordination lead Agency for Jordan's information assurance and cyberspace security. NIACSA should act as regulatory and advisory body. NIACSA should develop and review all security-related strategies, standards, policies, laws, and champion required change in co-ordination with all stakeholders.

5.2. Manage and coordinate the efforts needed to implement the NIACSS related projects.

5.3. Manage the CNIP Program.

5.4. Manage Nation-Wide Risk Management Program

5.5. Audit all government's information systems and procedures to guarantee compliance with national security standards and policies. Hence, the NIACSA will be responsible for Compliance and Certification.

5.6. Establish and manage the operation of :

- National Cyberspace Security Operations Centre (CSOC).
- National Computer Emergency Response Team (JO-CERT).
- National Encryption Center (NEC).

5.7. Coordinate with all government entities (including Military, Public Security Department, Civil Defense Department, and General Intelligence Department) and private sector regarding information assurance and cyber security.

- Define Success criteria.
- Raise the concern of cyberspace security within these entities.
- Raise the visibility of cyberspace security within entities budgets.
- Provide technical assistance to public and private sectors to guarantee proper protection of information systems and networks.

- Provide proper training and awareness sessions to entities' employees to help them comply with national standards and policies and to facilitate the implementation of the CIACSS.
- Define stages for cyberspace security implementation and enforcement.

5.8. Provide crisis management in response to attacks on national critical information systems.
5.9. Coordinate with peer international agencies.
5.10. Organize and carry out evaluation attacks on national networks in order to measure their readiness.
5.11. Be fully prepared to carry out preemptive and reactive attacks on hostile networks and or systems.

6. CONCLUSION

Jordan Government realizes the threats imposed by the revolutionary changes in Information Technology and the cyberspace environment. NIACSS is presented as a result of the government's review of the current information security situation. Current approaches are basic, not systematic, subjective, have no clear definitions and boundaries, not thorough, do not follow international standards, and are not able to deal effectively with the threats especially those emerging from the cyberspace. Efforts in this field are not consolidated and risks are not addressed at the national level.

NIACSS presents the strategic objectives, national information security priorities, and the implementation road map required to ensure and maintain a resilient and trusted computing environment that supports national security, enhances the economy, and builds awareness and trust of citizens towards achieving national prosperity. The following nine major national information security priorities collectively contribute to achieving the strategic objectives and help to prevent, deter, and protect national infrastructures against damage or attacks and minimize damage and recovery time from attacks that do occur:

1) Risk Management Program
2) National Computer Emergency Response Team (JOCERT).

3) Security Awareness and Capacity Building Program
4) National Information Security Standards and Policies
5) Legal and Regulatory Regime
6) National Encryption System
7) International Information Security Cooperation Program
8) Securing National Information Systems/Networks
9) Critical National Infrastructure Protection (CNIP) Program

Those nine major national interdependent priorities demand collaboration within Government, with international partners, with the private sector, and with the citizenry of Jordan.

For implementation purposes, NIACSS calls for establishing a well-defined organization called National Information Assurance and Cyber Security Agency (NIACSA) that oversees the efforts required to implement the NIACSS and its related projects. NIACSA is foreseen as a central national entity for governmental and non-governmental organizations regarding all information assurance and cyber security related issues.