National Information Technology Center (NITC)

National Information Assurance and Cyber Security Strategy (NIACSS)

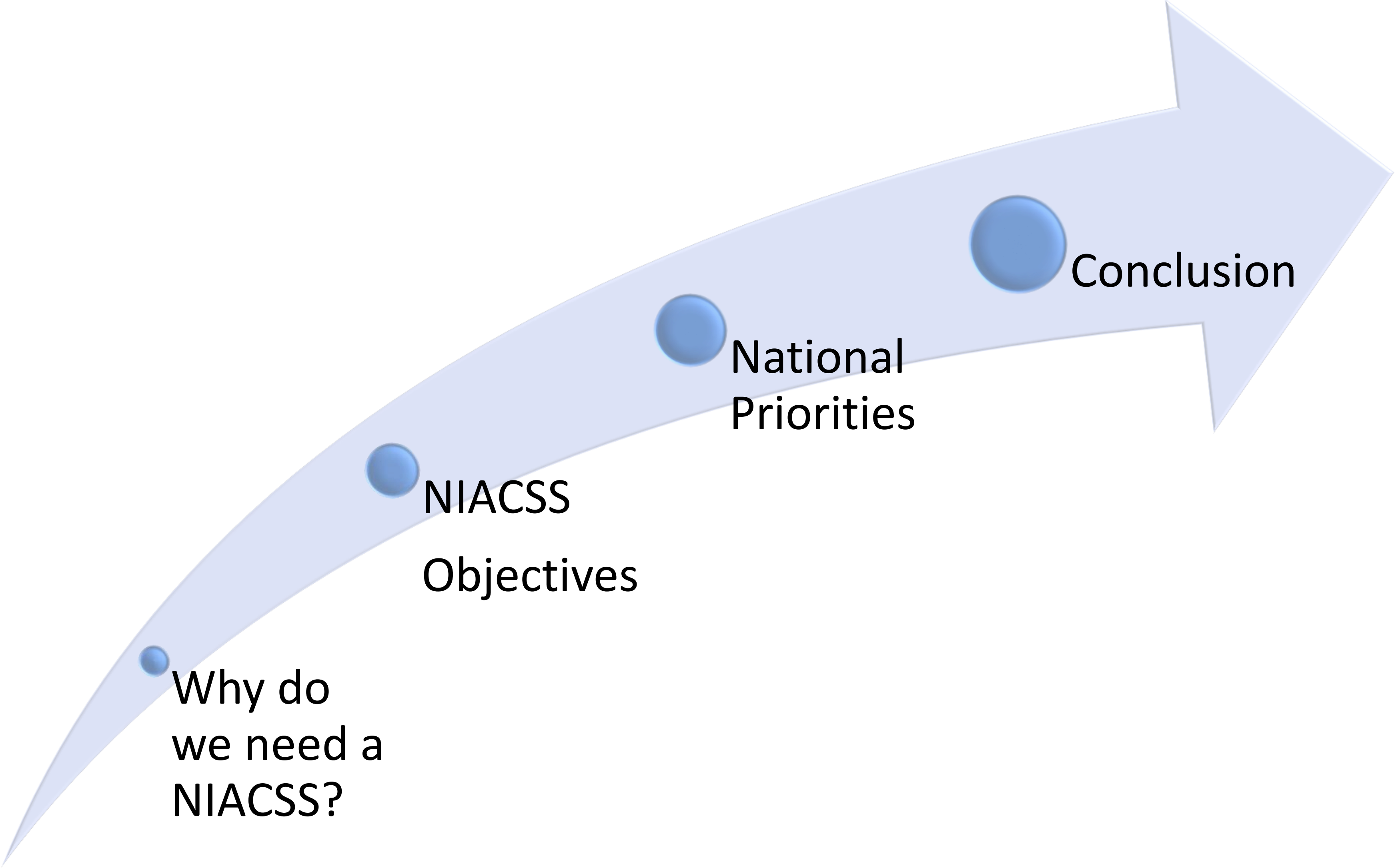
Jordan’s Approach to National CS&IA

Ahmed Otoom, Ph.D.

Disclaimer

“This presentation does not necessary represent the thoughts, intentions, plans or strategies of the National Information Technology Center (NITC), Jordan’s Ministry of Information and Communications Technology (MoICT), or any other Governmental or nongovernmental entity; it is solely the opinion of the author(s). The NITC, MoICT, and/or any other entity are not responsible for the accuracy of any of the information supplied herein”

Agenda



Why do we need a NIACSS?

NIACSS

Objectives

National Priorities

Conclusion

Why do we need a NIACSS?

Current approaches for CS&IA are relatively:

- Basic and Not systematic
- Subjective
- Not thorough, do not follow international standards
- Not consolidated and risks are not addressed at the national level
- Not able to deal with risks emerge from the cyberspace

We Need to consolidate, manage and coordinate National CS&IA efforts towards achieving our objectives (listed next)

NIACSS Objectives

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

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

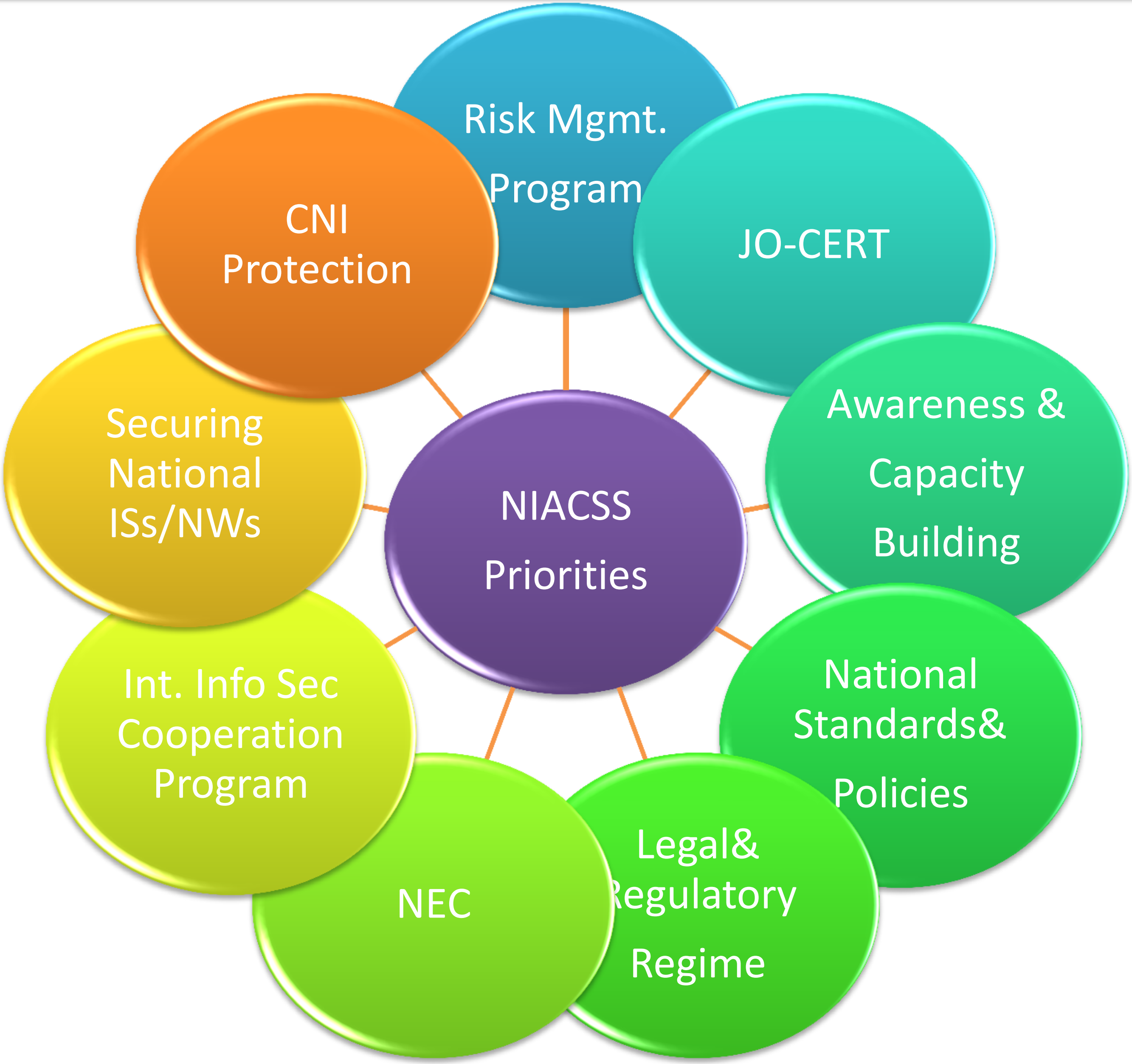
Minimize Damage and Recovery Time from Cyber Attacks regardless of source or intent.

NIACSS Objectives

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.

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

Priorities



NIACSS Priorities

Risk Mgmt. Program

JO-CERT

Awareness & Capacity Building

National Standards& Policies

Legal& Regulatory Regime

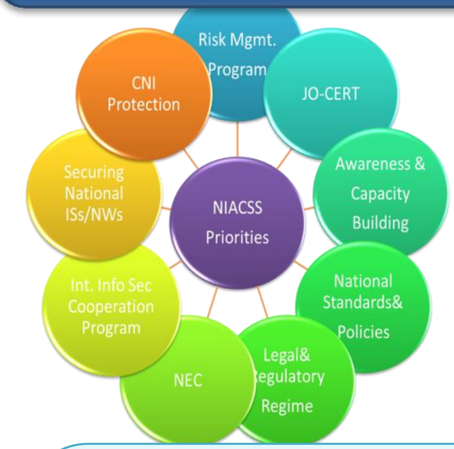
NEC

Int. Info Sec Cooperation Program

Securing National ISs/NWs

CNI Protection

Priorities: Risk Management Program

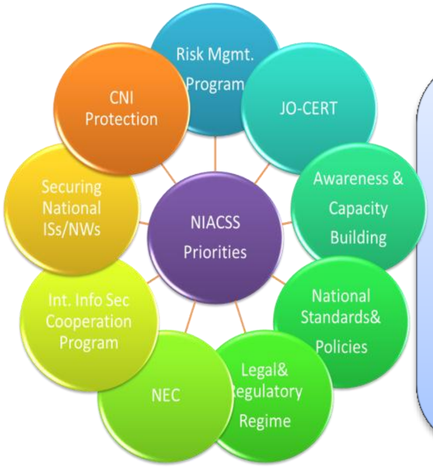

Risk Mgmt. Program
CNI Protection
JO-CERT
Securing National ISs/NWs
NIACSS Priorities
Awareness & Capacity Building
Int. Info Sec Cooperation Program
National Standards& Policies
NEC
Legal& egulatory Regime

A Nation-Wide Risk Management Program will establish the needed framework for high level impact risk management on the national level.

Risk management programs for National Entities must be inline with the nation-wide risk management program. Recovery plans will enable entities to get back in operation in a short period of time after an incident occurs.

National entities must consider the major risk management strategies, where applicable: mitigation, transference, acceptance, and avoidance.

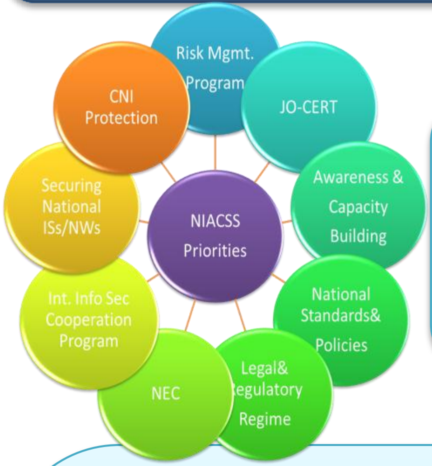
Priorities: JO-CERT


Risk Mgmt. Program
JO-CERT
Awareness & Capacity Building
National Standards& Policies
Legal& egulatory Regime
NEC
Int. Info Sec Cooperation Program
Securing National ISs/NWs
CNI Protection
NIACSS Priorities

The urgent need to manage and respond to cyber attacks made it a necessity to ***establish a National Computer Emergency Response Team(JOCERT)***

JO-CERT 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

Priorities: Security Awareness and Capacity Building

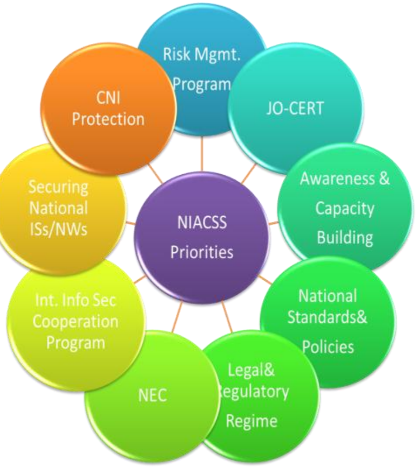

Risk Mgmt. Program
JO-CERT
Awareness & Capacity Building
National Standards& Policies
Legal& Regulatory Regime
NEC
Int. Info Sec Cooperation Program
Securing National ISs/NWs
CNI Protection
NIACSS Priorities

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

This program should have the following characteristics:

- ❑ 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).

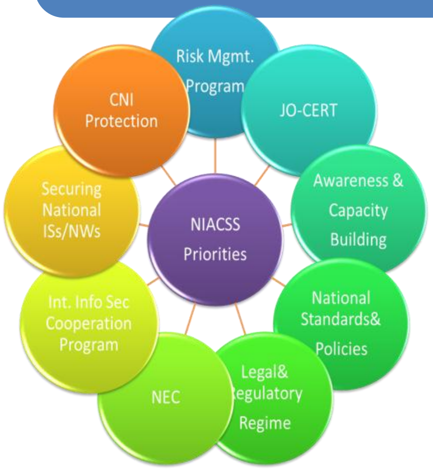
Priorities: National Information Security Standards and Policies


Risk Mgmt. Program
CNI Protection
JO-CERT
Securing National ISs/NWs
NIACSS Priorities
Awareness & Capacity Building
Int. Info Sec Cooperation Program
National Standards& Policies
Legal& Regulatory Regime
NEC

Information Security Policy must be developed and enforced to meet optimum information security requirements for government organizations and private sector utilizing international standards and best practices.

- ❑ The efforts of implementing nationwide overarching standards and policies will be assigned or managed by NIACSA.
- ❑ NIACSA will also audit and evaluate the compliance with these standards and policies given that segregation of duties is maintained.

Priorities: Legal and Regulatory Regime


Risk Mgmt. Program
CNI Protection
JO-CERT
Securing National ISs/NWs
NIACSS Priorities
Awareness & Capacity Building
Int. Info Sec Cooperation Program
National Standards& Policies
NEC
Legal& egulatory Regime

There is a need to review the related laws and regulations to support and enforce the implementation of this strategy.

Priorities: National Encryption Centre

A National Encryption Centre should be established to control, plan, monitor, and enforce the national strategic encryption policies.

Risk Mgmt. Program
JO-CERT
CNI Protection
Awareness & Capacity Building
Securing National ISs/NWs
NIACSS Priorities
National Standards& Policies
Int. Info Sec Cooperation Program
NEC
Legal& Regulatory Regime

Priorities: International Cooperation Program

National information security cannot be achieved or strengthened to a reasonable level without cooperating with related International Entities, especially in the following areas:

- ❑ Share and analyze information on vulnerabilities, threats and incidents.
- ❑ Participate in, utilize, and get benefits from current international efforts, such as cyber war exercises and international cyber alarm initiatives.
- ❑ Coordinate investigations of cyber-attacks and other potential computer-related crimes with international partners as required by law and agreement.
- ❑ Promote research and development and encourage the application of internationally certified security technologies.

NIACSS Priorities
Risk Mgmt. Program
JO-CERT
Awareness & Capacity Building
National Standards& Policies
Legal& Regulatory Regime
NEC
Int. Info Sec Cooperation Program
Securing National ISs/NWs
CNI Protection

Priorities: Securing National Information Systems and Networks

Employing Defense-in-Depth multiple layers of protection methods is critical to securing national systems and networks

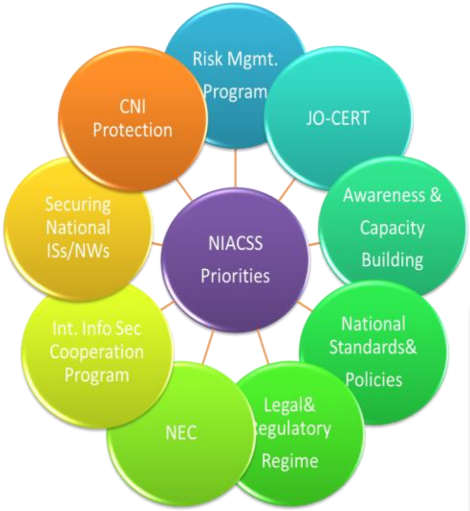
Manage security vulnerabilities in personnel, technology systems, and all operations that occur during the system's life cycle.

Securing information systems should consider achieving information assurance and security by three primary elements: people, technology and operations.

National entities must take care of personnel Security and physical security within the overall comprehensive information security solution.

National entities must defend the communications networks, critical infrastructures, networks boundaries, and computing systems that they own.

Priorities: Critical National Infrastructure (CNI) Protection Program


Risk Mgmt. Program
CNI Protection
JO-CERT
Securing National ISs/NWs
NIACSS Priorities
Awareness & Capacity Building
National Standards& Policies
Int. Info Sec Cooperation Program
NEC
Legal& Regulatory Regime

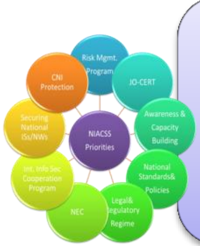
A CNI protection program is needed to secure systems of critical value to Jordan including SCADA Systems

Examples of CNI systems include telecommunications, ISP providers, banking and finance, health institutions, electrical power grid, and water supply

The government should co-operate and work closely with those parties who manage, own, or operate CNI.

Conclusion

NIACSS is just the first step; a commitment is needed to implement the NIACSS in order to achieve strategic objectives.


NIACSS Priorities
Risk Mgmt. Program
JO-CERT
Awareness & Capacity Building
National Standards& Policies
Legal& Regulatory Regime
NEC
Int. Info Sec Cooperation Program
Securing National ISs/NWs
CNI Protection

The identified Priorities should be considered as a whole.

NIACSA is needed to act as a focal point for all CS&IA related issues.

NIACSA should be empowered by law and enough resources.

Thank You

Ahmad.o@nitc.gov.jo