



INS

International Nuclear Security  
Reducing Risk of Nuclear Terrorism

# Managing Cyber Risks For Nuclear

Outline of Events for the Middle East  
North Africa Regional Meeting

Proposal For Consideration

October 2023






# Managing Cyber Risks for Nuclear

## Topic: A Proposed Workshop

### | INTRODUCTION

A photograph of a security guard in a dark uniform with 'SECURITY' written on the back, wearing a cap and holding a walkie-talkie. He is in a control room with several computer monitors displaying data in the background.

Nuclear security, operations, and safety systems are a complex integrated network that are composed of and utilize a myriad of technologies. Digital technologies, components, and protocols are increasingly becoming the backbone for these nuclear systems. While these technologies have enhanced system performance and improved efficiencies, they have also changed risk profiles. **The purpose of this workshop is to highlight those changed risks.**

#### CHANGES TO RISK PROFILE

Changes in the risk profile come in the form of vulnerabilities that a threat actor could potentially discover and exploit to negatively impact performance of a nuclear system.

Negative impacts could range from disruption of nuclear operations to compromise of safety systems. Vectors for exploiting vulnerabilities and leveraging these risks can come from a variety of sources from insider, supply-chain, as well as outsider based attacks.

There is a global need for nuclear security programs to adjust their evaluation methods and account for these risk profiles changes and take effective steps to prevent, detect, respond, and recover from new adversary tactics, techniques, and procedures.

#### WORKSHOP OVERVIEW

INS proposes to host and execute a workshop to discuss risks changes due to cyber and ways to manage the risk. The workshop topics range from introduction to common digital dependencies in a modern nuclear security, operational and safety systems, challenges that arise from those dependencies, and methods for addressing potential risks.

The workshop is designed as a forum where cross functional experts discuss systems essential for nuclear operations and vulnerabilities that result from these digital dependencies.

The workshop consists of formal presentations, demonstrations, and joint exercises. All activities will be designed to foster discussion to increase understanding and identify resources to assist in discovering more information. No prior cyber experience is necessary.



# Managing Cyber Risks for Nuclear

## Topic: A Proposed Workshop

### | OBJECTIVES & STRUCTURE

#### FORUM OBJECTIVES

The primary purpose of the forum is to engage a variety of nuclear personnel and cyber security experts in a technical exchange of ideas, challenges, and solutions on cyber risks. All proposed activities are designed to create a shared experience where participants work together and discover how cyber risks impact nuclear security.

#### FORUM OUTCOMES

This workshop proposal is designed to illicit 3 conclusions from the participant:

1. recognize cyber security is a vital element to a nuclear program;
2. describe current threat trends and applications to nuclear security; and
3. identify resources (people, organizations, and information sources) that can help strengthen cyber security regimes.

#### FORUM STRUCTURE

The primary objective is to create a platform that fosters collaboration and collective discussion on cyber risks. Therefore, the majority of activities in this engagement are focused on group work and discussions.

The activities are broken into 3 key security topics. For each topic, there are 3 central activities denoted by A, B, C in the agenda.

- A. kickoff **Presentation** that introduces the topic.
- B. **exercise / Demonstration** geared towards generating discussion in groups and as a class as a whole.
- C. **interactive Discussion** where a segment of the topic is discussed in detail.

The focus of each activity is based around the question: **“HOW DOES THIS TOPIC IMPACT ME?”**

### | FORUM TOPICS



#### Systems Analysis & Operations

In this session we will discuss the goals, functions, and systems used to establish a modern and sustainable nuclear security and safety program using digital & analog components. Consequence & Systems Analysis is the focus.



#### Threat Trends & Analysis

In this session we will discuss impacts of recent threat actor trends and relevancy to nuclear systems and performance metrics. This includes vulnerability analysis and translating them into risk prioritized actions.



#### Cyber Risks & Solutions

In this session we will discuss approaches evaluating and treating (mitigating and remediating) cyber risks inherent in a modern nuclear system from an outsider and insider perspective.



# Managing Cyber Risks for Nuclear

## Topic: A Proposed Workshop

### FORUM AGENDA

Session	Day 1 - INTROs	Day 2 - SYSTEMS	Day 3 -THREAT	Day 4 - RISKS & RESPONSE	Day 5 - EVALUATE
Morning	Welcome: Opening Remarks and Course Introduction	Welcome & Cyber Challenge	Welcome & Cyber Challenge	Welcome & Cyber Challenge	Welcome & Cyber Challenge
	Cyber Challenge: Group activity designed to illustrate course objectives and meet participants.	Presentation: Threat Tactics and Techniques	Presentation: Cyber Supply Chain Risk Management	Presentation: Incident Response	Exercise: Data Requirements for Incident Response & Recovery
	<i>Break</i>	<i>Break</i>	<i>Break</i>	<i>Break</i>	<i>Break</i>
	Demonstration: Cyber-Attack Identification of how cyber-attacks work and potential consequences.	Demonstration: Ransomware	Exercise: Supply Chain Risks	Exercise: Incident Response	Open Discussion
	Presentation: Cyber Risk at Nuclear Facilities	Presentation: Threat Trends & Considerations	Presentation: Defensive Architecture	Exercise: Cybersecurity & Insider Threat Management	Summary
<i>Lunch</i>	<i>Lunch</i>	<i>Lunch</i>	<i>Lunch</i>	<i>Lunch</i>	<i>Close of Workshop @ 1200</i>
Afternoon	Exercise: Industrial Control Systems	Exercise: Vulnerabilities & Exploits (Attack Life Cycle)	Exercise: Exploiting Vulnerabilities & the Kill Chain (Part 1)	Exercise: Phishing For Information	
	Presentation: Asset Characterization & Consequence Analysis	Presentation: Managing Cyber Risks	Exercise: Exploiting Vulnerabilities & the Kill Chain (Part 2)	Exercise: Resource Planning for Cyber Vulnerability Mitigations	
	<i>Break</i>	<i>Break</i>	<i>Break</i>	<i>Break</i>	
	Exercise: Identifying Assets & Assessing Consequence	Exercise: Assessing & Prioritizing Risks	Presentation: Mitigating Risk & Cybersecurity Solutions (Administrative & Physical)	Discussion: Cyber foundations & building a cyber program.	
	Presentation: Cybersecurity Plan & Risk Management	Discussion: Threat Profiles & Threat Sharing Information	Exercise: Security Controls (Part 1)	Exercise: Cyber Hygiene	
	Questions & Adjourn @ 1700	Questions & Adjourn @ 1700	Questions & Adjourn @ 1700	Questions & Adjourn @ 1700	