IAEA Nuclear Security Programme

Computer Security at Nuclear Facilities
Eurosafe - Paris 2008 - A. Cavina (IAEA-NSNS)
Structure of the presentation

1. Who we are & what we do
2. The Nuclear Security Series
3. Computer security
IAEA and Nuclear Security

• The Nuclear Security programme has seen one of the fastest recent growth within the IAEA
• Office of Nuclear Security unit responsible for cross-organizational coordination of activities
  • ~50 staff
  • Budget 2007 ~15M€
• Strong interactions with Safety
• Commonalities with Safeguards (Science, Ill. Tr.)
• Programme existed since the early 80s but started vigorously expanding since 2002
  • Almost entirely (90%) funded through voluntary contributions
Interplay within Nuclear Security

NUCLEAR SECURITY FRAMEWORK
- Conventions
- Laws & regulations
- Regulatory bodies
- Law enforcement
- Threat assessment
- Accounting and control
- Guidance
- Prevention
- Detection/response
- Coordination
- Security culture

TARGETS
- Nuclear weapons
- Nuclear material
- Radioactive material
- Nuclear facilities
- Transports
- Transits
- Technology
- Cyberspace
- Sensitive information

THREATS
- Terrorists
- Criminal organizations
- Non-state factions
IAEA - Improving Nuclear Security

- Promoting international instruments and their implementation
- Developing recommendations and guidelines
- Providing evaluation and advisory services
- Providing education and training – human resource development
- Providing technical improvements and upgrades
- Coordinating Member States and the global effort towards Nuclear Security
Nuclear Security Series

Scope of the Series:
• internationally accepted baseline for nuclear security
• “guidance” not “standards”
• provide links to safety and safeguards
• different levels of documents
• rigorous review process involving Member States
• starting point for other activities

• Anticipate 20-30 publications in next few years
• 9 documents published to date
• Benchmarks for States and the IAEA
#1: Technical and Functional Specifications for Border Monitoring Equipment
#2: Nuclear Forensics Support
#3: Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators
#4: Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage
#5: Identification of Radioactive Sources and Devices
#6: Combating Illicit Trafficking in Nuclear & Other Radioactive Material
Published - Continued

- #7 - Nuclear Security Culture
- #8 - Preventive and Protective Measures Against Insider Threats
- #9 - Security in the Transport of Radioactive Material

Final Stage Prior to Publication:

- Nuclear Security at Major public events
- Security of Radioactive Sources
- Development and Maintenance of a Design Basis Threat
- Identification of Vital Areas at Nuclear Facilities
- INPRO Manual on Physical Protection
- Computer Security at Nuclear Facilities

Ready to be sent for comment for 120 days:

- Protection and Confidentiality of Nuclear Security Information
NUCLEAR SECURITY SERIES FRAMEWORK

**Recommendations**

- Nuclear Security Culture
  - Confidentiality of Nuclear Security Sensitive Information
- Development and Maintenance of a Design Basis Threat
  - Protection Against Sabotage
  - Security of Radioactive Sources
  - Protection Against an Insider Threat
  - Radioactive Waste Security
  - Security During the Transport of Radioactive Material
  - Physical Protection of Nuclear Material During Transport
- Recommendations for the physical protection of nuclear material and nuclear facilities being also revision 5 of INFCIRC225.
- Recommendations for the physical protection of radioactive materials and associated facilities

**Implementing Guides**

- Nuclear Security at Major Public Events

**Technical Guidance:**

- Nuclear Security Glossary
- Model Regulations for Security of Nuclear and other Radioactive Material and Associated Nuclear Facilities
- Educational Programmes for Nuclear Security
- Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage - No. 4
- Identification of Vital Areas at Nuclear Facilities
- INPRO Manual on Physical Protection
- Physical Protection of Research Reactors and Associated Facilities
- Security of Information and Instrumentation & Control Systems at Nuclear Facilities
- Nuclear Material Accountancy Systems at Facilities
- Nuclear Forensics Support - No. 2
- Technical and Functional Specifications for Border Monitoring Equipment – No. 1
- Monitoring for Radioactive Material in International Mail – No. 3
- Identification of Radioactive Sources and Devices – No. 5
- Combating Illicit Trafficking in Nuclear and Other Radioactive Material – No. 6
- Detection and Response for Radioactive Material at Seaports
Developing recommendations and guidelines

- Maximizes strengths of IAEA:
  - Outreach (145 MSs and growing...)
  - Access to expertise
  - External to political/industrial influence

- Creates knowledge:
  - More than the sum of its parts
  - International forum for reflecting on experience

- Linked to the implementation of obligations contained in the international (legal) instruments

- Widespread long-term impact:
  - Availability
  - Visibility - Awareness raising - Benchmarking
  - May be incorporated in national legislation/guidance
Computer Security at Nuclear Facilities

The history:

• Work started in 2003!!
• Has been the object of 4 CMs and 1 TM
• Is now available for Member States comments (120 days, ending Dec. 15th)
• Will be published early 2009
Why an IAEA CompSec document?

Global reasons:

• Attackers focus on critical infrastructure (existing examples of sabotage / extortion), new attention to SCADA systems as targets
• Relevant legislation and regulations of the field are lagging behind
• Not all national infrastructures have recognized and standardized the issue
• Existing international guidance is not industry specific and fails to capture some of the key issues
• No existing IAEA document specifically addresses the field
Why an IAEA CompSec document?

Technological reasons:
- Increased presence of digital I&C systems in the design of new (and old) NPPs and the corresponding introduction of new and unknown vulnerabilities
- Increased interconnection and reliance of Physical Protection systems on computerized systems (alarms, access control,...)
- Increased request for connection of Extranet, Intranet (Business) and Control networks
• **computers** and **computer systems** refer to the computation, communication, instrumentation and controls devices that make up functional elements of the nuclear facility. This includes components such as embedded systems and PLCs. In essence all components that may be susceptible to electronic compromise.

• the term **computer security** will be used to cover the security of all computers as defined above and all interconnected systems and networks. The terms **IT security** and **cyber security** are, considered synonyms.
Document: Objectives

• create **awareness** of the importance of incorporating **computer security** as a fundamental part of the **overall security plan**

• highlight concerns, requirements and strategies for implementing a computer security programme

• bring **focus** on **issues specific to nuclear facilities**:

• provide advice on evaluating existing programmes
Nuclear security and computer security objectives

Computer security objectives:
• are commonly defined as protecting the confidentiality, integrity, availability attributes of electronic data or computer systems
• must address the protection of those computers, networks and other digital systems that are critical for the safe and secure operation of the facility and for preventing theft, sabotage and other malicious acts
Computer based **malicious acts** may be grouped as:

- information gathering attacks
- attacks disabling or compromising of computers crucial to facility security or safety;
- compromise of computers **combined** with other concurrent modes of attack, such as physical intrusion to target locations.
Legislative and Regulatory considerations

• State legislation to be continuously reviewed and updated to include provisions for new and emerging criminal activities and other potential threats to computer security

• State regulatory authorities to issue requirements for computer security as part of the requirements for the Site Security Plan
SITE SECURITY FRAMEWORK

- Computer security is a cross-cutting discipline that has the potential to affect all areas of security.
- It is management’s responsibility to ensure proper coordination of the various disciplines of security and integration of computer security at the appropriate level.
Threat identification and characterization

• Threats of either stand alone attacks using/against computer systems or coordinated attacks including the use of computer systems should be incorporated into DBT scenarios

• An adequate process of intelligence gathering is required to ensure the completeness and relevance of each facility’s attacker matrix

• Likewise sensitive assets and their vulnerabilities should be identified and assessed
• The security of CS to be based on a graded approach
• The assignment of CS to different levels and zones should be based on their relevance to safety and security
• The risk assessment process should be allowed to feed back into and influence the graded approach
Special considerations for Nuclear Facilities

- Facility lifetime phases and modes of operation
- Differences between IT systems and control systems
- Demand for additional connectivity and related consequences
- Considerations on software updates/patching
- Secure design and specifications for computer Systems.
- Third party/vendor access control procedure
Next step: HRD + Assessment

- First pilot “Computer Security for Nuclear Security practitioners” course specific for nuclear facilities – September ‘08, Romania
  - **4-5 courses** planned for 2009
- Putting together, upon invitation, a first draft for an assessment mission to review I&C security in an NPP
- Parallel development of “Protection of Nuclear Security Information” document
With many thanks...

Andrea Cavina  
Office of Nuclear Security  
International Atomic Energy Agency  
A.Cavina@iaea.org  
+43-1-2600-26637  

http://www-ns.iaea.org/security/