41\textsuperscript{st} Meeting of the Radiation Safety Standards Committee
21 – 24 November 2016

Agenda Item: R7.3
NST045 Computer security for nuclear security (Implementing Guide)

Mr Mike Rowland
Objective: Provide guidance on developing, implementing and integrating computer security as a key component of nuclear security covering NSS 13, NSS 14, and NSS 15.

Contents:
1. INTRODUCTION
2. CONCEPTS AND CONTEXT
3. ROLES AND RESPONSIBILITIES OF THE STATE
4. ROLES AND RESPONSIBILITIES OF RELEVANT ENTITIES
5. ESTABLISHING THE COMPUTER SECURITY STRATEGY
6. IMPLEMENTING THE COMPUTER SECURITY STRATEGY
7. DEVELOPING A COMPUTER SECURITY PLAN
8. SUSTAINING COMPUTER SECURITY
APPENDIX I: CONSIDERATIONS FOR INTERFACES WITH THE SAFETY DOMAIN
ANNEX I. CYBER THREAT PROFILES
ANNEX II. ASSIGNMENT OF RESPONSIBILITIES TO RELEVANT ENTITIES
ANNEX III. ILLUSTRATION OF A FRAMEWORK OF COMPETENCES AND LEVELS OF CAPABILITY
Document History

• DPP approved – June 2014 (5th NSGC)
• Consultancy Meetings (5) - Nov 2014, Jan 2015, Aug 2015, Jan 2016, May 2016
• Technical Meeting (1) – Jun 2016

Development was in close coordination with NST057 (recommendations level guidance WM) and NST047
NSS 20 Objective and essential of a State’s nuclear security regime

NSS 13 Nuclear Material and Nuclear Facilities

NSS 14 - Radioactive Material and Associated Facilities

NSS 15 Nuclear and other Radioactive MORC


NSS Computer Security Implementing Guides


NST045 (2017 est) - Computer Security for Nuclear Security (proposed for 120 day MS review)

NSS Computer Security Technical Guides

 NSS 17 - Computer Security Nuclear Facilities (2011)

NSS 17 - Computer Security Nuclear Facilities (2011)

Application in Grade Approach

Application in Grade Approach

Application in Grade Approach


NST036 (Completed – Print 2016) Computer Security for I&C Systems at Nuclear Facilities

Documents Outside Nuclear Security Series

Conducting Computer Security Assessments (2016)

Incident Response Planning for Computer Security Events (2016)

Note: NSS 17 is planned to ultimately be replaced by NST045 and NST047.
**Sensitive information assets** are defined [NSS20] as any equipment or components that are used to store, process, control or transmit sensitive information.

The term **sensitive digital assets (SDAs)** is used in this publication to identify those sensitive information assets that are computer-based and need computer security measures for their protection.
Defining CS Responsibilities

All organizations are bound by the State's legislation.

Organizations that have assigned roles and responsibilities to deliver the State's computer security strategy.

Organizations whose requirements are not derived from regulatory requirements.

State
- Legislative framework
- National Strategy
  - Roles and Responsibilities

Competent authorities
- Recommendations, requirements and standards

Competent authority for computer security
- Certification standards

Regulatory bodies
- Regulatory requirements

Operators
- Licence holders, Operators, Shippers and Carriers
- Contractual requirements

Contractors, Vendors, Suppliers
- Contractual requirements

Providers of goods and services
Comments provided by:

• France
• Finland
• Australia
• Iraq
• Japan
• Ukraine

Comment Resolution:

• Total Comments: 65
• Accepted/Accepted with Modification: 56
• Rejected: 7
<table>
<thead>
<tr>
<th>Comment No.</th>
<th>Para/Line No.</th>
<th>Proposed new text</th>
<th>Reason</th>
<th>Reason for modification/rejection</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRAQ-2</td>
<td>1.01/line 5</td>
<td>… including maintaining physical protection system. All such computer systems therefore need to be secured …</td>
<td>Terms of the nuclear security series, IAEA</td>
<td>(semantics) Physical Protection is the objective and not a system.</td>
</tr>
<tr>
<td>JP-NUSC-1</td>
<td>2.09</td>
<td>Followings should be added after para. 2.9. While digital asset itself has no potential impact on nuclear safety and security, this digital asset should be identified as the SDA if this digital asset communicates with the SDA through data communication.</td>
<td>Cyber-attacks may affect to the SDA from the non SDA via data communication lines, all digital assets communicate with the SDA by data communication, these digital assets should be identified as the SDA.</td>
<td>This proposed sentence is too loose. How many data hops does communication detail. Does this mean we must ultimately make the entire network or even internet an SDA? The communication and interconnectivity between SDAs and digital assets should be closely considered in assessing what level of protection is required for digital assets.</td>
</tr>
<tr>
<td>Comment No.</td>
<td>Para/Line No.</td>
<td>Proposed new text</td>
<td>Reason</td>
<td>Reason for modification/rejection</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>------------------</td>
<td>--------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>UKR-3</td>
<td>2.39-2.43 (pages 11-13)</td>
<td>It is reasonable to define the criteria for determining the computer security levels for SDAs and computer-based systems</td>
<td>To clarify the approaches for determining the computer security levels</td>
<td>This is a very good point, but as many Member States may have different approaches which all may be valid, this topic will be addressed in NST047 (Technical Guidance).</td>
</tr>
<tr>
<td>JP-NUSC-3</td>
<td>3.05</td>
<td>Para. 3.5 states as follows; “The State should identify all the competent authorities and operators with roles and responsibilities relating to computer security in the nuclear security regime and ….” Does the State directly identify operators’ role and responsibility on computer security?</td>
<td>Clarification</td>
<td>The State should identify these roles and require such organizations to implement computer security plans.</td>
</tr>
<tr>
<td>JP-NUSC-5</td>
<td>3.24.-3.26. and 3.29.-3.36.</td>
<td>Move the following paragraphs to chapter 4. Paras 3.24. – 3.26. Paras 3.29. – 3.36.</td>
<td>The contents of these paragraphs deemed to be the activities conducted not by the State, but by operators.</td>
<td>This section looks at interfaces with computer security, and can be applied to both operators and CAs.</td>
</tr>
<tr>
<td>Comment No.</td>
<td>Para/Line No.</td>
<td>Proposed new text</td>
<td>Reason</td>
<td>Reason for modification/rejection</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>--------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>JP-NUSC-6</td>
<td>4.00</td>
<td>The most of the practices described in section 4 are common practices conducted by competent authorities and operators. It is ambiguous which one is the practice that competent authorities should perform and which one is the practice of operator. Suggested to separate the descriptions into the practices of competent authorities and the practices of operator.</td>
<td>Previously this was split, but the decision was made to create one section that identified practices for both. Unfortunately, these are NOT always common practices performed by either CAs or Operators.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JP-1</td>
<td>5.13 Line 16 to 19 and Page 30/Line 1 to 2</td>
<td>Delete this para 5.13 and Fig.6.</td>
<td>Since the detailed description about DBT should be described at not this guide but the guide developed separately, i.e., NST058&quot;Development, use and maintenance of threat assessment and design basis threat (Revision of NSS No. 10)&quot;; it is not necessary to describe this paragraph at this guide. We are concerned about it becoming complicated that leaving this paragraph takes consistency with NST058 under development.</td>
<td>This paragraph is fully is meant to emphasize the guidance in NSS10 and the future guidance in the revision. This section is important, because it applies NSS10 principles to computer security where no such guidance currently exists. NST058 drafting is incomplete and NST045 will likely be published in advance of the update to NSS10. NST058 is being developed in collaboration with NST045</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NSGC Recommendation

- NSGC approval NST045 to forward for 120-day Member State Review
Thank you!