Nuclear Safety Standards Committee
36th Meeting
16 – 18 October 2013

Agenda item 3.1, 3.2
DPP NST045 Nuclear Security Recommendations for Computer Security
DPP NST046 Computer Security Systems and Measures for Nuclear Facilities

Donald Dudenhoeffer, NSNS
Comment Review

The comments noted in this presentation and in the listing of combined comments include those received under the NUSSC review, but also those received thru 3 October for the upcoming NSGC meeting.

The focus of this briefing are those comments specifically for NUSSC.
Document Objective:

- The objective of this document is to establish the high level recommendations to guide the development of computer security programmes in Member States, to include State, competent authority, and facility level operations.

- The high level guidance presented in this document will have applicability toward nuclear and other radioactive material, associated facilities and activities, and the detection of such material out of regulatory control and response to threats involving such material.
Comments combined from NUSSC and NSGC pre-meeting input:

Total Comments: 17

Accepted: 4 (mainly for clarity)

Accepted with modification: 5

Rejected: 5

No Action Required (commentary, not editorial or for NSGC discussion): 3

Comments from:

- Canada
- France
- Russian Federation
- Finland
<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>NUSC-CA-1</td>
<td>Section 1. /Proposed Title</td>
<td>(Change the title to:) Nuclear Security Recommendations for Computer Security at Nuclear Facilities</td>
<td>This document addresses computer security for all nuclear facilities.</td>
<td>This guidance is applicable toward facilities out of regulatory control also.</td>
</tr>
<tr>
<td>NUSC-CA-5</td>
<td>6 (page 6 of 8)</td>
<td>3.z Secure Development Environment</td>
<td>For a stronger security of the software development environment. It will be appropriate to put it between sections 3.5 and 3.6</td>
<td>While important, this is too granular for the Recommendations level and will be addressed in implementing guidance.</td>
</tr>
<tr>
<td>NUSC-CA-7</td>
<td>6 and sub-section 3.9y (page 6 of 8)</td>
<td>3.9y Procurement and Qualified Suppliers</td>
<td>A sub-section dealing with procurement control and supplier qualification should be addressed here. It will be appropriate to put it after the section 3.93 and then rearrange other section numbers accordingly.</td>
<td>While important, this is too granular for the Recommendations level and will be addressed in implementing guidance.</td>
</tr>
</tbody>
</table>
While the overall consensus from Member States is that additional guidance at the Recommendations level is needed, different opinions exist as to how to implement such guidance.

The possible options presented and to be discussed at the NSGC meeting in October include:

1. Development of a dedicated Recommendations level document

2. Implement guidance as a update to the current Recommendations documents (NNS13, NSS14, and NSS15)

3. Develop an interim Annex on Computer Security for the current Recommendations documents until such time as the document could be updated.
Document Objective:

- The objective of this document is to establish implementation guidelines for developing and integrating computer security as a fundamental part of the overall nuclear security plan for nuclear facilities.

- This implementing guide is intended for a wide audience that includes policy makers, nuclear security regulators, facility management, staff with security responsibilities, technical staff, vendors and contractors.

- The focus of this guide is nuclear facilities and associated operations, which have the strongest dependence on complex computer systems, and which could lead to the greatest potential consequences if a cyber-attack were successful. However, the document could be applicable to other radioactive material facilities and operations as applied in a graded approach.
Comments combined from NUSSC and NSGC pre-meeting input:

Total Comments: 18

Accepted: 11

Accepted with modification: 4

Rejected: 3

Comments from:
• Canada
• France
• Russian Federation
• Finland
<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>NUSSC-CA-7</td>
<td>Section 6/A possible Table of Content:</td>
<td>(create a new sub-section) 5.6 lifecycle management of cyber assets.</td>
<td>Life Cycle Management is one of important topics for computer security program. The subsections from 7.2 to 7.6 can be moved into this new section.</td>
<td>These areas may need separate sections. To be further evaluated during the CM and document development.</td>
</tr>
<tr>
<td>NUSSC-FR-1</td>
<td>Para 6</td>
<td>7. SPECIAL CONSIDERATIONS FOR NUCLEAR FACILITIES 7.1 Facility Lifetime Phases and Modes of Operation 7.2 Safety classification, Connectivity and Related Consequences 7.3 Considerations on Software Updates and Hardware Modification 7.4 Secure Design and Specifications for Computer Systems 7.5 Third-Party/Vendor Access and Control 7.6 Security Testing</td>
<td>Safety classification should be mentioned. This can also interface with “Computer system classification” (it may not be clear which classification purpose (safety and/or security) is addressed</td>
<td>Safety classified systems will be addressed, but a specific heading is not needed.</td>
</tr>
</tbody>
</table>