Energy
A Security Plan for the remote monitoring networks

Johan Stronkhorst
Paris, 15/11/2016
The EURATOM Treaty (1957)

Chapter VII – Safeguards

Executive tasks are given to the Commission for all related areas:

- declaration of basic technical characteristics to the EC (Art. 78)
- provision of accountancy declarations to EC (Art. 79, Regulation no. 302/2005)
- send inspectors to nuclear installations and verify declarations (Art. 81-82)
- initiate infringement procedures (Art. 82-83)
- fulfil obligations undertaken by the Euratom Community in agreements with international organizations and Third States (Art. 77 b)
EURATOM Safeguards

• Apply to all nuclear material and installations in the EU, except nuclear material and installations used for defense purposes in the Nuclear Weapon States (NWS)

From a practical point of view this means that:

• no difference can be made by the Commission (EC) between safeguards applied in NWS and in Non-NWS (Art. 77a and 84), and
• at the same, safeguards is applied in a way that the EC makes sure that all agreements with third parties are complied with (the main party in this respect being the IAEA), Art. 77b

The joint EURATOM / IAEA remote monitoring network is one of the results of the cooperation with the IAEA...
Data handling

Data handling in NPP & Lux/Vienna HQ

- No formal classification, but treated as sensitive information
- Onsite storage of data for about 6…8 months – backup for VPN black out
- Review networks separated in technical and safeguards review

EURATOM & IAEA automate data transfer via VPN

- To make the data transfer much more secured
- To have daily feedback about proper system operation - less redundancy
- To save inspector and operator effort for additional inspections

Nothing new you would say….
Why....

a Security Plan?
But the word ‘internet’ is mentioned. No change in data handling since 1957, so what’s the point?
What can be found in a Security Plan?

**Explanations**

- The technical details of the remote monitoring network
- The dataflow from the NPP to Luxembourg and Vienna

**Assessment of the security requirements & risks**

- Clarify the security requirements of all connected systems & data
- Compare the old and new situation
- Give an inventory of security measures vs. threats

**More explanations**

- Related procedures, like incident handling
- Data handling and its relation to privacy
Into details...

EC Headquarter secure data room

Joint RM system
- ADSL router
- Netscreen SSG-20

Collect Server

Storage Server EC

Data collect server PULLS the data from remote site and PUSHES it to both storage server EC and IAEA

VPN to LUX

INTERNET cloud

VPN to VIENNA

DMZ RMS

IAEA Collect Server

Storage Server SG (Safeguards)

IAEA Headquarter

Nuclear Plant

Surveillance system or Data Acquisition
- ADSL router
- Netscreen 5-GT

ADSL link

INTERNET cloud

Firewall + Encryption + Router

Common sealed

Common sealed
Into details...
A risk based approach

Clarify the security requirements (chapter 3)

- It is not only about confidentiality !!!
- The highest risk may be something completely different.

Assess the threats and security measures (chapter 4 & 5)

- Is your biggest fear realistic?
- Every stakeholder has its own agenda…..

How to make ends meet….. (Chapter 6, 7, conclusion)

- Assess related subjects, like incident handling & privacy
- Implement the solution that meet the requirements.
What if?

**Incident notification scheme**

<table>
<thead>
<tr>
<th>Required incident action</th>
<th>Stakeholder</th>
<th>Contact</th>
<th>Tel no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment (Power) Reset</td>
<td>Operator (for help)</td>
<td>RO, FO, TFO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Euratom (to initiate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment replacement</td>
<td>Operator (for help)</td>
<td>RO, FO, TFO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Euratom (to initiate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broken seals</td>
<td>Operator (for help)</td>
<td>EURATOM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(to initiate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damaged or missing files</td>
<td>Operator (for help)</td>
<td>EURATOM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(to initiate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td>EURATOM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Encryption Failure</td>
<td>EURATOM (to replace device)</td>
<td>RO, FO, TFO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EURATOM (Certificates)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera Encryption Failure</td>
<td>EURATOM (to change camera)</td>
<td>RO, FO, TFO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator (for help)</td>
<td>EURATOM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(to initiate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data leak</td>
<td>Operator</td>
<td>EURATOM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EURATOM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Abbreviations:**
- RO: EURATOM Review Officer
- FO: EURATOM Facility Officer
- TFO: EURATOM Technical Facility Officer

---

**Chart:**
- **Detection of an incident**
- **Notification scheme in place**
- **Initial assessment of the incident**
- **Periodic review & improvement**
- **Producing annual security incident summary to stakeholder**
- **End**
- **Notify all stakeholders**
- **Is there a cross-border element of the incident?**
- **Notify the direct concerned stakeholder**
- **Is disclosure of the incident in the public interest?**
- **Supervisory authority informs the public**
- **End**

- **Detected by a potential security incident via:**
  - External
  - Internal
  - Manual inspection

- **Within 24 hours after becoming aware of the breach:**
The context...

Energy IMS

QMS
Continuous improvement
Customer focus
Process approach

ICS
Evaluation
Communication
Documentation
Reporting

Risk Management
Budgetary Management
Financial Management
Activity Based Management

Security plan – 15/11/2016 13
The context...

Documents types identified within the Directorate of NUCLEAR SAFEGUARDS

- **Internal documents**
  - document issued within the Integrated Management System of the ENER/DDG2.E NUCLEAR SAFEGUARDS

- **Documents of external origin**
  - documents that do not originate within the Directorate, but are necessary for ensuring quality and meeting requirements. These documents are issued outside the Directorate

- Security Plan RM Network
- One for each conn. site

- Commission Guidelines on Security Plans
- Commission Guidelines on Asset Classification
- Commission standard on Cryptography and PKI
- Commission standard on Security Risk Management
Questions?

Johan Stronkhorst
johan@stronghorse.nl