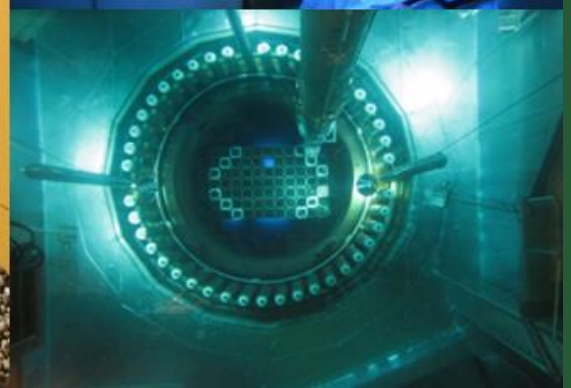


Authority for Nuclear Safety and Radiation Protection

"Information protection / Confidentiality in the Netherlands"

Marco Schraver

Nuclear Security Policy Coordinator/ Security Officer

Authority for Nuclear Safety and Radiation Protection (ANVS)

Wednesday, May 11, 2016, 16:30 - 17:30

Unclassified Information

Outline presentation

- Security approach Authority Nuclear Safety and Radiation Protection
- Annual reports 2015 Intelligence and Security Services
- Legal framework classification of information
- Classification Structure
- After the classification of information, the elaboration and implementation measures
- Design Basis Threat Cyber Security
- Lessons Learned – Best Practises

Authority Nuclear Safety and Radiation Protection (ANVS)

Reasons for the establishment of the ANVS:

- Be compliance with the intent of IAEA and Euratom rules for an independent nuclear authority.
  - Adopted solution: ANVS = independent administrative authority

- Boost the robustness and effectiveness of the former organisation(s).
  - Adopted solution: combining existing knowledge and expertise

ANVS's task areas

- Nuclear safety
- Radiation protection (medical, transport, industry)
- Emergency preparedness and response
- Security
- Safeguards
- Waste

ANVS's powers

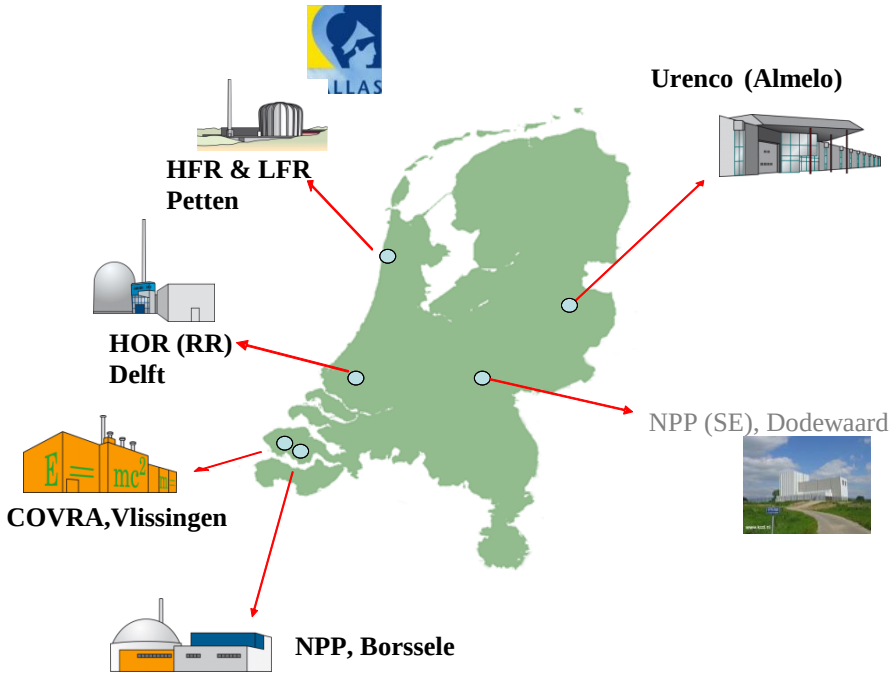
- Preparation policy, legislation and regulations
- Issues licences, exemptions, etc.
- Inspection, supervision and enforcement
- Information
- International cooperation
- Research
- Knowledge support for other national bodies
- ANVS transferred to the Ministry of Infrastructure and the Environment, but it exercises its powers independently

ANVS approach

- ANVS approach:
  - Security is a statutory duty, this also applies to Safety and Safeguards
  - Security is part of the (wider) safety concept: 3-S-approach
    - Integrated way regarding looking at 3-S-issues
    - In the near future joint inspections (Safety/Security): coherent and simultaneous inspections on site

Intro: Nuclear Installations in the Netherlands

- NPP Borssele (2 loop PWR, 510 MW_e)
- NPP Dodewaard shutdown (BWR, safe enclosure)
- Research Reactor HFR Petten (50 MW_{th})
- Research Reactor LFR Petten (30 kW_{th}), shutdown
- University Reactor HOR Delft (3 MW_{th})
- Ultra Centrifuge Enrichment Plant URENCO (UNL)
- Interim Waste Storage Facility (COVRA)



Annual Reports 2015 Intelligence and Security Service (AIVD-MIVD) *(open source)*

- The threat of digital espionage is becoming increasingly aggressive and sophisticated.
- Some non-Western countries with large military ambitions are guilty of cyber infiltration and espionage.
- Some states with very considerable resources are trying to steal unprecedented large quantities of data.
- The international business is a favorite target of foreign espionage.
- The intelligence activities of foreign intelligence services were strongly in 2015 aimed at gathering economic, political and technological information.
- There is a trend that affected the functionality of systems such as Industrial Control Systems and SCADA systems.
- Most used attack are spear phishing and watering holes (infection of visitors to websites).

Legal framework in the Netherlands

- Government Information Security Decree - Specific Information (VIR-BI 2013)
  - Basis for government measures in the field of managing (special) information
  - Decree specifies:
    - Security classification regarding information
    - Mandatory requirements for protection and handling

- Executive Order on the Security of Nuclear Facilities
  - DBT Cyber Security

- Non-disclosure Decree license holders Nuclear Energy Act (Nea).

Classification Structure

- Levels of classification (VIR-BI):
  - Departmental Confidential (Dept-C) (damage to departments / government)
  - State Secret - Confidential (Ss-C) (damage to the State / allies)
  - State Secret - Secret (Ss-S) (serious damage to the State / allies)
  - State Secret - Very Secret (Ss-VS) (very severe damage to the State / allies)
- Other markings have no legal status (not in VIR-BI):
  - Trade secret-Confidential
  - Personal - Confidential

Factors classification (selection)

Category	Dept-C	Ss-C	Ss-S	Ss-VS
Public trust	Loss of public respect	Public outcry	Loss of confidence	Structurally loss of confidence
Damage to critical processes	Loss guarantee continuity	Temporary loss of continuity	Lengthy loss of continuity	Permanent failure of the process
Breach of privacy	Privacy-sensitive information people	Privacy-sensitive information public figures	Privacy-sensitive information people / info Royal Family	Information about Royal family
Financial damage	> 50 million	> 500 million	> 5 billion	> 50 billion

Elaborations of factors (selection)

	Dep C	Ss C	Ss C	Ss VS
Each document must have at least by provided with classification level, duration classification, page numbering and total number of pages that make up the document;	V	V	V	V
Each document is provided with a copy number		V	V	V
Each document must have a Copy number, Author, Receiver.		V	V	V
Creating, updating, modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available and destroy specific information is recorded.			V	V

Who defines level of classification?

- Author (or supervisor) of the note
  or
- Classification level of information/sources used in the writing process
  or
- Advice from the Classification Officer in the organization.

Key factors process of consideration

- Knowledge / understanding of the consequences of abuse of classified material is crucial.
- Knowledge / understanding of the obligations arising from use of classified material is crucial.

After the classification…the follow-up

- When the employees knows what kind of classified information is used, further provisions must be taken regarding:

  - Internal procedures (e.g. clean desk, visitors policy, processing method within organization in the field of sensitive information, security measures outside office hours)

  - Vetting people/trustworthiness

  - Security infrastructure (physical and cyber: safes, detectors, sensors, key- and access management, protected areas)

  - Strengthening and maintenance awareness at all levels

Design Basis Threat Cyber Security - I

- Focus DBT Cyber Security:
  - Nuclear material (theft/sabotage)
  - ICS (sabotage/influencing)
  - Nuclear information (theft/sabotage)

- Cooperation between all relevant public and private stakeholders (including Plant Security managers and CIO's).

- DBT is approved by Minister of Infrastructure and Environment and Minister of Security and Justice (= National Counter Terrorism Coordinator (NCTV) + National Cyber Expert Centre (NCSC)).

- Written agreement of Directors of the National Police (Cyber Crime Unit) and AIVD (General Intelligence Security Service).

DBT Cyber Security - II

- First version adopted in 2014 - based on IAEA-NSS-publications.
- Evaluation / adjustment in 2016 (focus on integration DBT Physical Security (e.g. Blended Attacks, state of the art detection facilities)).
- Evaluation every two years (in case of serious incidents interim adjustment).
- Licensees are going to report predefined cyber incidents to the Regulatory Body ANVS + National Cyber Security Centre on a mandatory basis.
- National Cyber Security Centre assists to neutralize cyber incidents and analyze who penetrates cyber systems.

Lessons Learned – Best Practices

- Information protection / Confidentiality is a responsibility of all relevant public and private stakeholders: “Same goals - different responsibilities”.
- Human factor is the key factor regarding information protection.
- Focus should primary be on raising the security awareness among management and staff.
- This focus must be permanently maintained and reinforced at all levels – be transparent in terms of necessity and follow-up actions.

- Thank you for your attention!

Marco Schraver
Nuclear Security Policy Coordinator
Authority for Nuclear Safety and Radiation Protection (ANVS)
Marco.schraver@anvs.nl