Thomas HAUTESSERRES
Sectorial coordinator, energy and nuclear power
French cyberdefense agency (ANSSI)

Overview of the French cybersecurity approach & application to nuclear cybersecurity

Agenda

- ANSSI in a nutshell
- French approach to Critical Information Infrastructure Protection (CIIP)
- Application to nuclear facilities

ANSSI in a nutshell

- ANSSI
  - French cybersecurity and cyberdefense agency and authority
  - Reports to Prime minister
  - Created in 2009, 500+ people
- Scope
  - Originally government and critical infrastructures operators
  - Extending to SME, citizens
- Fields of action
  - Operational matters (CERT-FR)
  - Expertise, R&D
  - Secure information systems
  - Evaluation, certification, regulation, training
- Current priorities
  - Critical Information Infrastructure Protection (CIIP) law (« LPM* »)
  - Cybersecurity industry policy

*LPM: French Military Planning Law, includes CIIP articles.

The French CIP approach

- CIP: critical infrastructure protection
  - Defense and national security approach
- Key concept: **critical infrastructure operators***
  - “*An operator whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation*”
  - Approx. 250 CI operators: 40% public, 60% private designated since 2006
  - 12 sectors: health, water, defense, **energy (incl. nuclear power)**, transportation, finance, etc.

Power

Food

Finance

Public

Telco

Health

Industrie

Defense

Transport

Water

Space & Research

Justice

*OIV in French, standing for operators of vital importance

The French CIIP approach

- CIIP: critical information infrastructure protection
  - Complete the CIP approach with a focus on IT systems
- Key concept: **critical information system***
  - “*An information system [belonging to a CI operator] that, if its security or availability were compromised, could strongly threaten the economical or military potential, the security or the resilience of the Nation, or present a danger to the population.*”
  - The cybersecurity law is only applicable to critical IT systems of critical infrastructure operators.

*SIIV in French, standing for information system of vital importance

CIIP law – 4 main CIIP measures

Mandatory security rules: organisational and technical

- 20 rules, adapted but mostly similar across business sectors
- Examples: IT security policy, documentation, network segregation, patching, etc.
- Prescribe the use of qualified providers (audit, detection, response)

Incident notifications to ANSSI

- Great importance of trust and confidentiality

Inspections of critical IT systems

- ANSSI can mandate audits, executed by ANSSI or qualified auditors

Major crisis

- ANSSI can mandate measures in case of crisis

*LPM: French Military Planning Law, includes CIIP articles.

Application to nuclear facilities

- Cyber threat assessment
  - Adapt protection to known attack vectors & tactics + defense in depth
  - CIIP rules enforce good practices protecting against common IT threats
- Nuclear facilities specific?
  - CIIP rules are mostly similar across business sectors
  - CIIP is complementary to nuclear-specific security laws (nuclear material laws, physical security) and design basis threat
- Regulation or incitation?
  - CIIP law forces good practices and inspections on critical IT systems of operators of critical infrastructures only.
  - Regulation in force in the nuclear sector since April 2017.

Thank you