Information security as part of nuclear security and safety in Finland

Paula Karhu/STUK/Nuclear Security
paula.karhu@stuk.fi

3rd International Regulator's Conference on Nuclear Security
Marrakech, 1 – 4 October 2019

[20191003 PKa]

Information security

- Confidentiality
- Integrity
- Availability
- During the whole lifecycle of the information

Information

- Written on paper
- In people's minds
- In electronic format, in information systems (cyber)
  - ITC systems
  - nuclear security systems
  - I&C/ICS systems
  - including programmable digital systems
  - including those in NF and in the use of radiation (e.g. in hospitals)

Case Finland: State level

- Act on the opennes of government activities (621/1999)
  - What is public
  - What is classified
- Goverment Decree on information security in Central Government (681/2010)
  - How to protect classified information
- Also: KATAKRI – Information security audit tool for authorities (2015)

Regulation for NF and RM

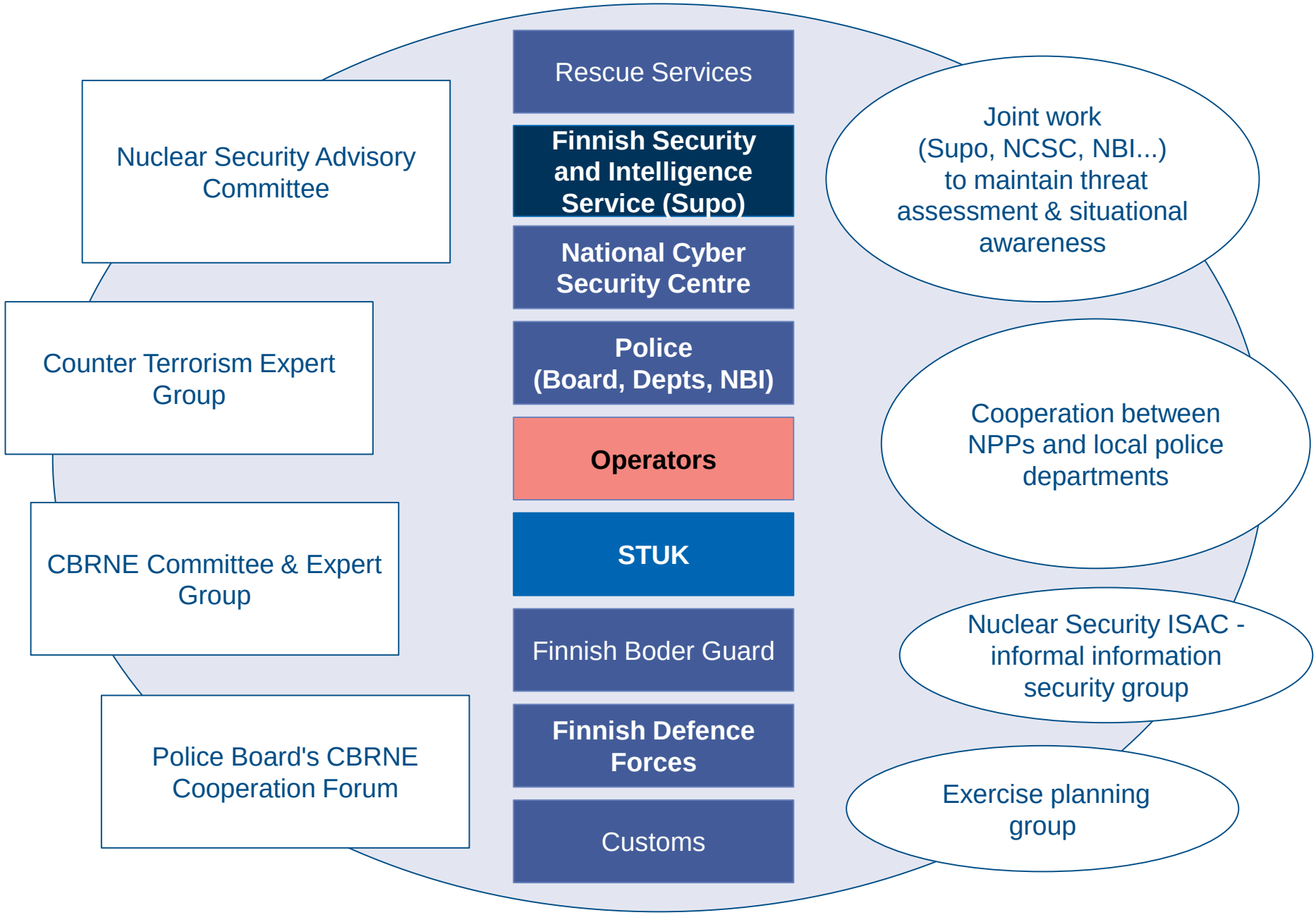
- STUK regulation on nuclear security in the use of nuclear energy (Y/3/2016)
  - General requirements, principles of protection
  - Detection of and response to anomalies/irregularities/events
- DBT includes cyber and other information security threats
- STUK regulatory guide A.12: information management system for a NF
- STUK regulation on security of radioactive sources (S/3/2018)

Some principles of STUK guide A.12

- Roots in ISO/IEC 27 000 series
- Focus on information security management system, which is part of the organization's integrated management system
- Risk-informed, risk management approach
  - Indentification of assets
  - Evaluation of their significance to overall nuclear safety and security
  - Application of security controls according to the significance
    - Such as access management, how systems interact, which may be connected to others and how, methods for detecting and responding to anomalies /irregularities/events, testing, exercises… (however, in regulation and guide the approach is more risk-informed, performance based than prescriptive)
- Evaluation of effectiveness of the ISMS
  - Internal assessments, external, independent assessments
  - STUK inspection programme

Interfaces

- Physical security and information security are interdependent
- Both are interfaced with safety
- For example:
  - Design of hard-to-hack systems, including I&C/ICS systems
  - Secure and efficient information transmission in cases of response to accidents and to nuclear security events, including MORC incidents
  - Availability and integrity of information needed in emergency response, for example in a NF


Nuclear Security Advisory Committee
Counter Terrorism Expert Group
CBRNE Committee & Expert Group
Police Board's CBRNE Cooperation Forum
Rescue Services
Finnish Security and Intelligence Service (Supo)
National Cyber Security Centre
Police (Board, Depts, NBI)
Operators
STUK
Finnish Boder Guard
Finnish Defence Forces
Customs
Joint work (Supo, NCSC, NBI...) to maintain threat assessment & situational awareness
Cooperation between NPPs and local police departments
Nuclear Security ISAC - informal information security group
Exercise planning group

Thank you