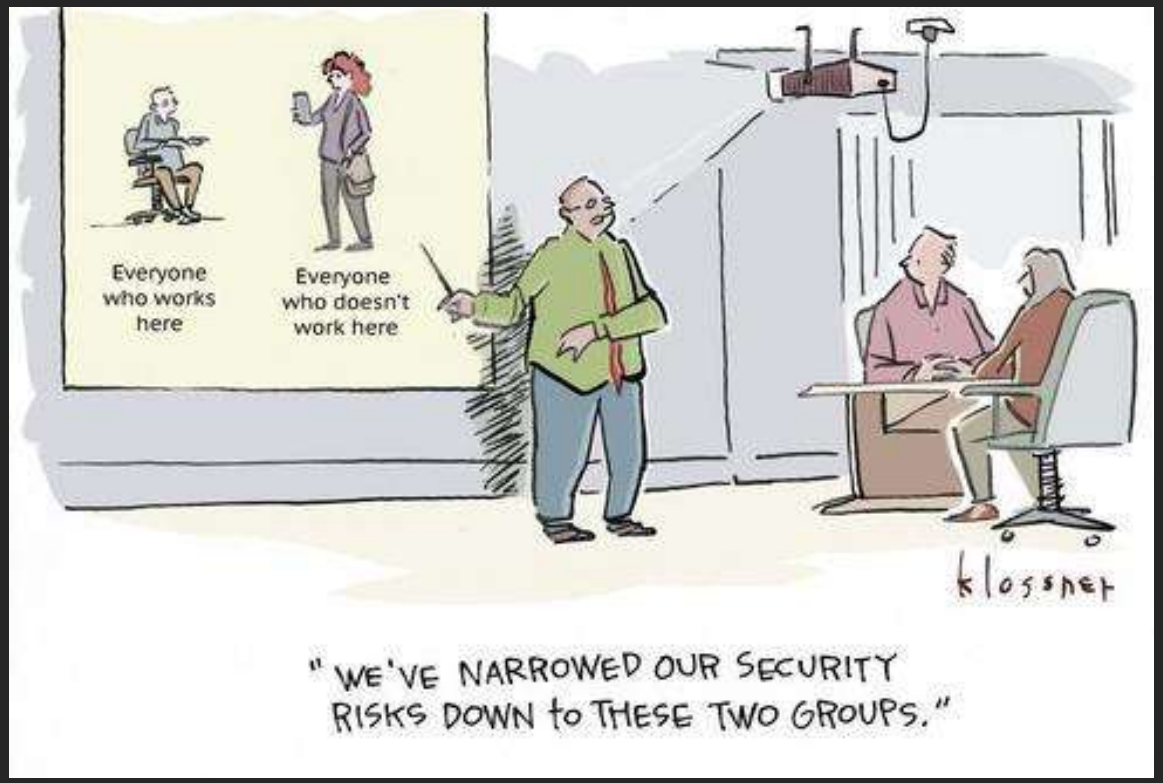
Supervision and Incident notification
SK approach

Rastislav Janota
Director
National CERT of the Slovak Republic
National Security Authority

SK NBÚ CERT

CYBERSECURITY IS TOPIC FOR?

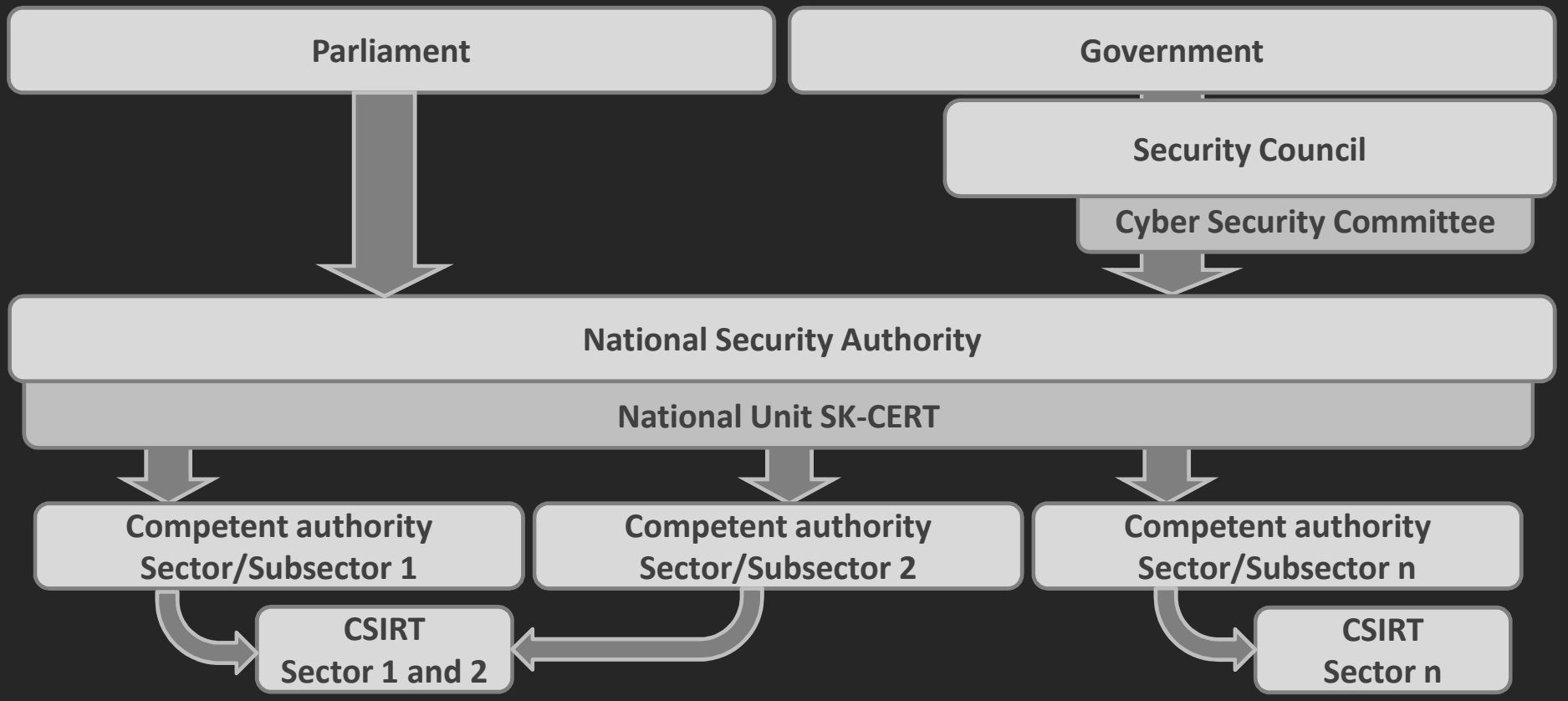


Cybersecurity is topic for everyone. It is responsibility of everybody.

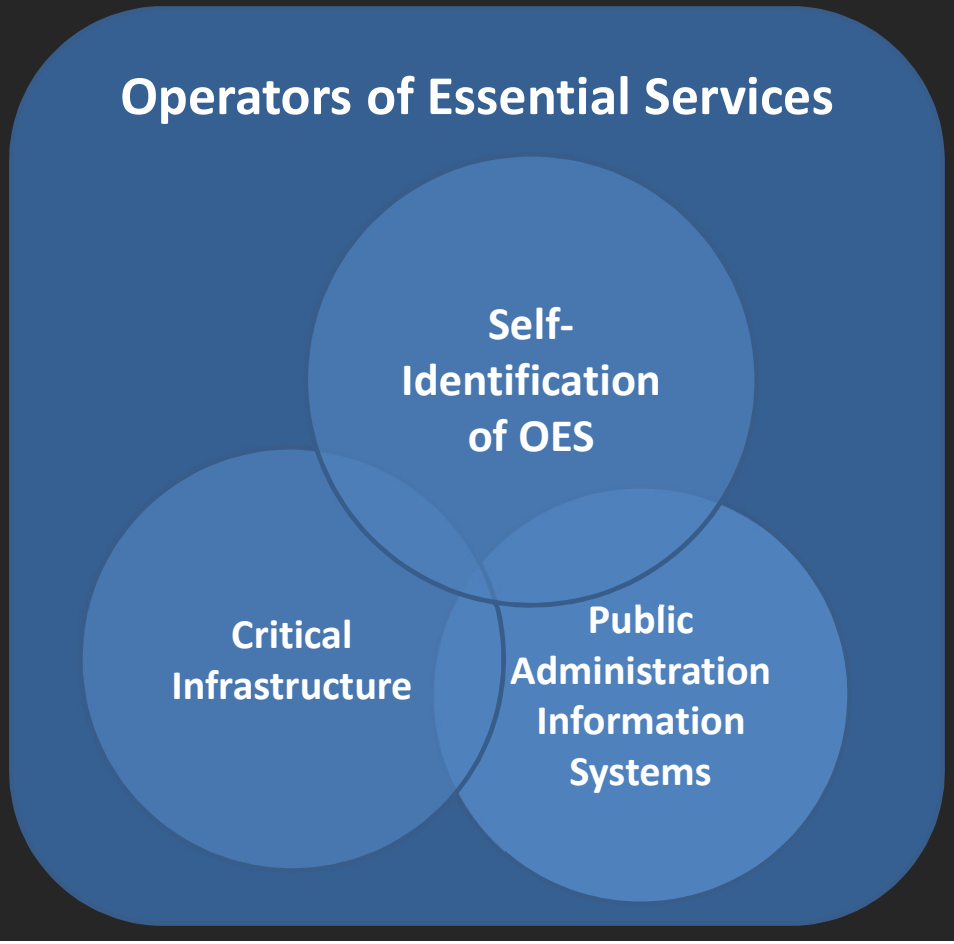
Everyone is responsible for own data and own services.

Everyone should be aware of any kind of problem/incident/attack from anyone (inside or outside own organization).

CYBERSECURITY GOVERNANCE IN SLOVAKIA



CYBERSECURITY LAW PRINCIPLES IN SLOVAKIA



- OES origins from three groups:
  - Public Administration Information Systems
  - Critical infrastructure Elements
  - Self-Identification - Subject from sectors/subsectors (based on specific and impact criteria)
- Alignment with Critical Infrastructure Protection (sectors, competent bodies)
- So current situation is:
  - 11 sectors with 28 subsectors
  - 11 Competent authorities (Big ones and small ones)
  - Today only 3 sectorial CSIRTs (incl national CERT)

IDENTIFICATION CRITERIA – EXAMPLES (BANKING)

SK CERT

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Credit institutions whose business is to receive deposits or other repayable funds from the public and to provide loans on their own account	a) Number of clients exceeding 25 000. b) Market share exceeding 1% of the balance sheet total.	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss exceeding 0,1 % of GDP. 4. Economic loss or material damage to at least one user exceeding 250 000 EUR. 5. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

IDENTIFICATION CRITERIA – EXAMPLES (DIGITAL INFRASTRUCTURE)

SK CERT

Service provider (Annex No. 1 to the Act)	**Specific sector criteria** (individually)	**Impact criteria** (individually) Impact of the cybersecurity incident in the information system or network, on the functioning of which depends service operation, may cause:
Internet exchange point service provider for switching networks that are technically and organizationally separate.	Organization administers an autonomous system (AS) or operates data lines in the Internet network, where these interconnect the AS with two and more other AS in the overall transmission capacity of network interfaces of at least 2 Gbps. For these purposes an AS is considered only an AS with a public AS number (public ASN), not an AS	1. Threatening availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided or available through these networks and information systems, affecting more than 25 000 persons. 2. Limitation or disruption of operation of other essential service or critical infrastructure element. 3. Economic loss or material damage to at least one user exceeding 250 000 EUR. 4. Disruption of public order, public security, emergency or distress requiring carrying out of rescue work or execution of activities and measures related with providing help in distress.

DEFINITION OF SECTORS AND SUBSECTORS FOR OES

SK CERT

Sector	Subsector	Competent Authority	CIP	NIS	CiiP
Banking		Ministry of Finance		☑	☑
Transport	Air transport	Ministry of Transport and Construction	☑	☑	☑
	Rail transport		☑	☑	☑
	Water transport		☑	☑	☑
	Road transport		☑	☑	☑
Digital Infrastructure		National Security Authority		☑	☑
Electronic Communication	Satellite communication	Ministry of Transport and Construction	☑		☑
	Electronic communications networks and electronic communications services		☑		☑
Financial market infrastructures		Ministry of Finance		☑	☑

DEFINITION OF SECTORS AND SUBSECTORS FOR OES

SK CERT

Sector	Subsector	Competent Authority	CIP	NIS	CIIP
Postal services		Ministry of Trans & Const	☑		☑
Energy	Mining	Ministry of Economy	☑		☑
	Electricity		☑	☑	☑
	Oil		☑	☑	☑
	Gas		☑	☑	☑
	Heat-power				☑
Other Industries	Pharmaceutical	Ministry of Economy	☑		☑
	Metallurgical		☑		☑
	Chemical		☑		☑
	Intelligent Industry (4.0)				☑
Health	All medical facilities (incl. Hospitals and private clinics)	Ministry of Health	☑	☑	☑

DEFINITION OF SECTORS AND SUBSECTORS FOR OES

SK CERT

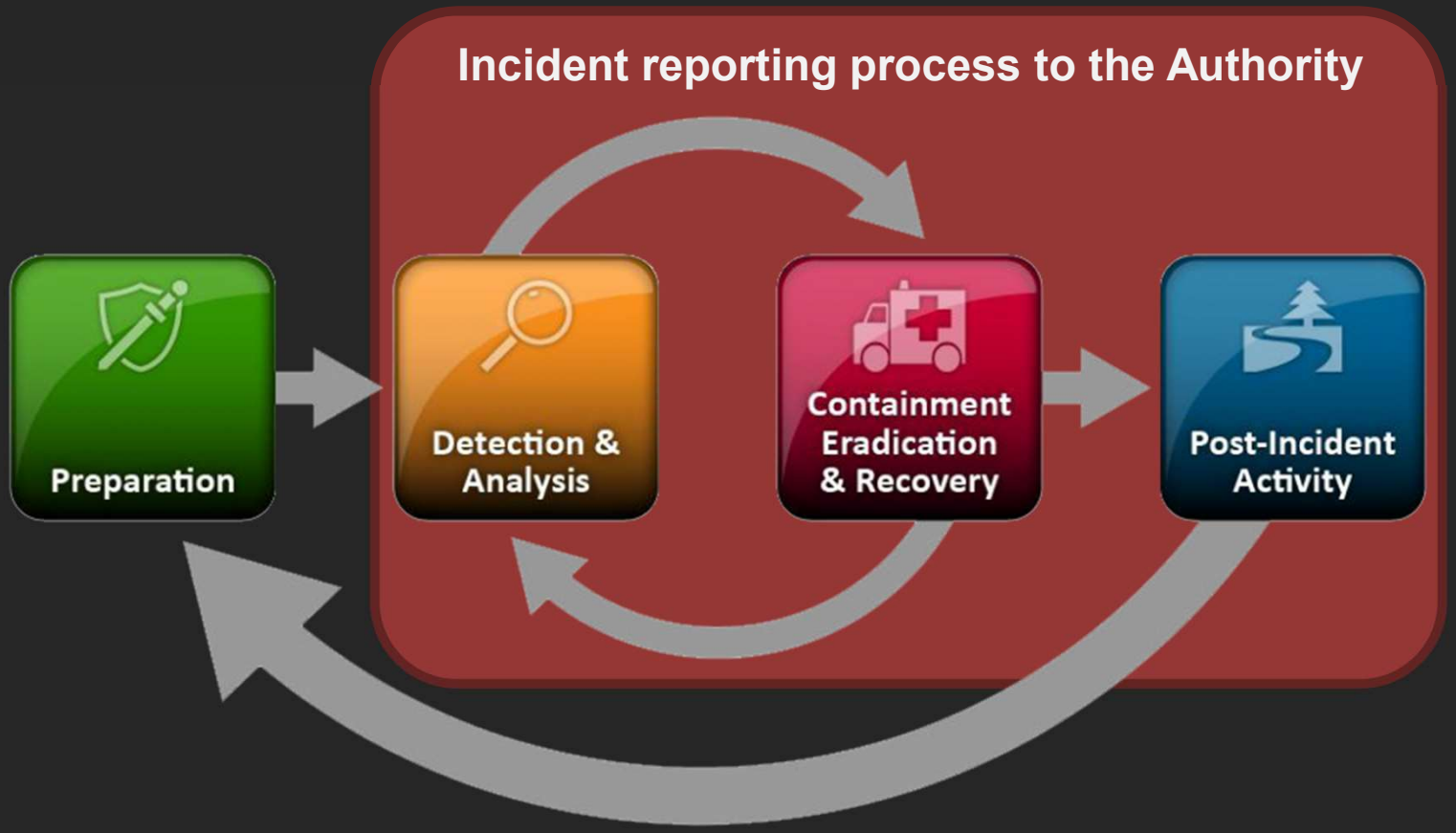
Sector	Subsector	Competent Authority	CIP	NIS	CIIP
Water and Atmosphere	Weather service	Ministry of the Environment	☑		☑
	Water works		☑		☑
	Drinking water supply and distribution		☑	☑	☑
Public Administration	Public order and security	Ministry of Interior			☑
	Information systems of public administration	Deputy Prime Minister's Office for Investments and Informatization	☑		☑
	Defense	Ministry of Defense			☑
	Intelligence services	Intelligence services			☑
	Classified Information Protection	National Security Authority			☑

BASIC DUTIES FOR OES FROM CYBER SECURITY ACT / NIS

SK CERT

- Two important group of duties for Operators of Essential Services
- Preventive duties
  - Follow minimum security baselines defined by law
  - Do proper management of supply chain including telco services
- Reactive duties
  - Report cybersecurity incident to Cybersecurity Authority (National Unit SK-CERT)
  - Handle cybersecurity incidents
  - Cooperate with the Cybersecurity Authority and the competent body (sectoral authority) when handling the reported cybersecurity incident
  - Inform the law enforcement authority or the Police

INCIDENT RESPONSE LIFECYCLE



NIST SP 800-61 R2 Foundation

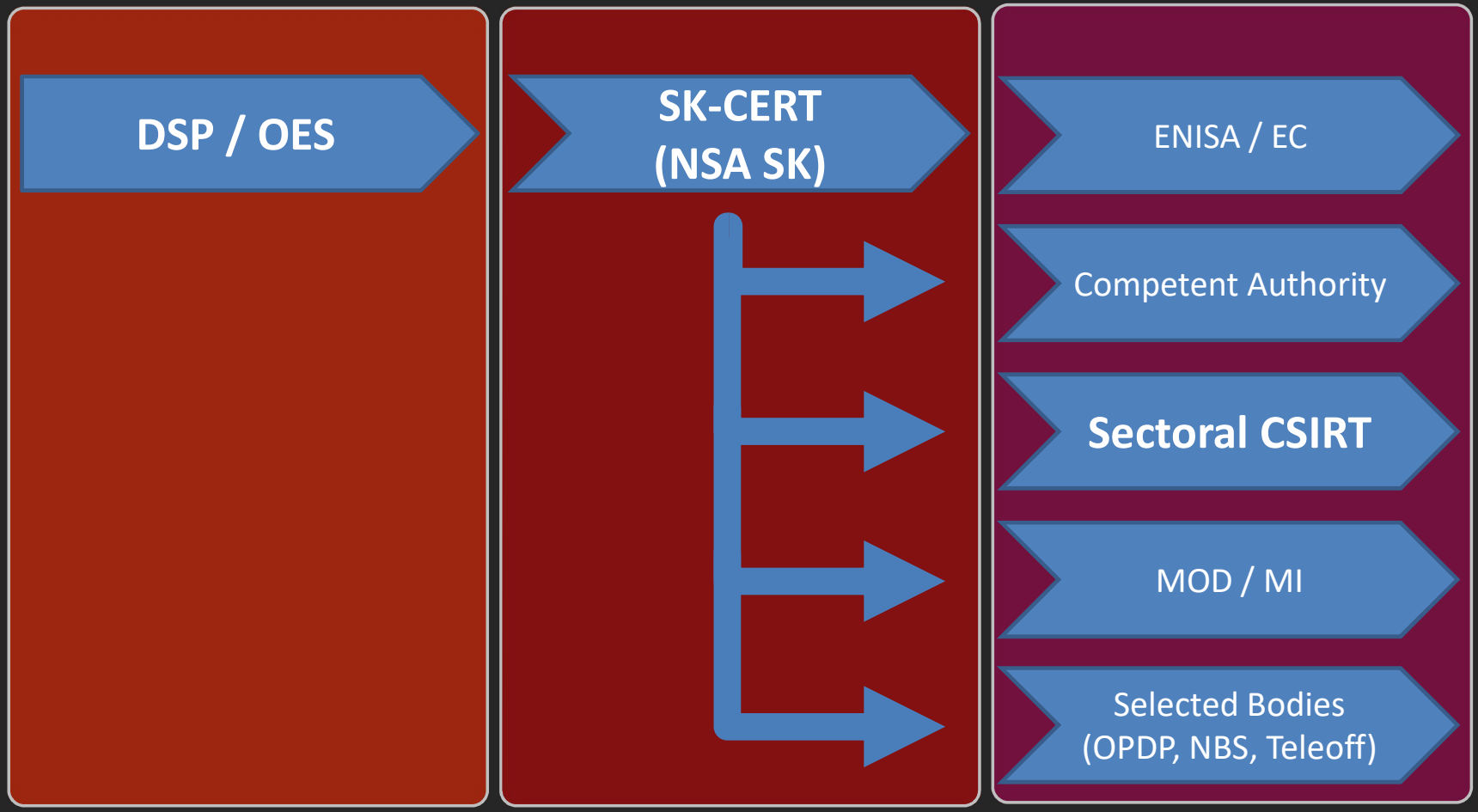
REPORTING OPTIONS

SK CERT

- **Standard reporting**
  - Web GUI
  - API to Reporting system
- **Optional reporting**
  - Based on agreement with NSA SK (SK-CERT) (Cyber Security Act 69/2018 Article 24 section 6)
  - Raw data from different equipment (sensors, FWs, WAFs, DNSs, proxy servers, routers etc.)

CYBERSECURITY REPORTING SYSTEM

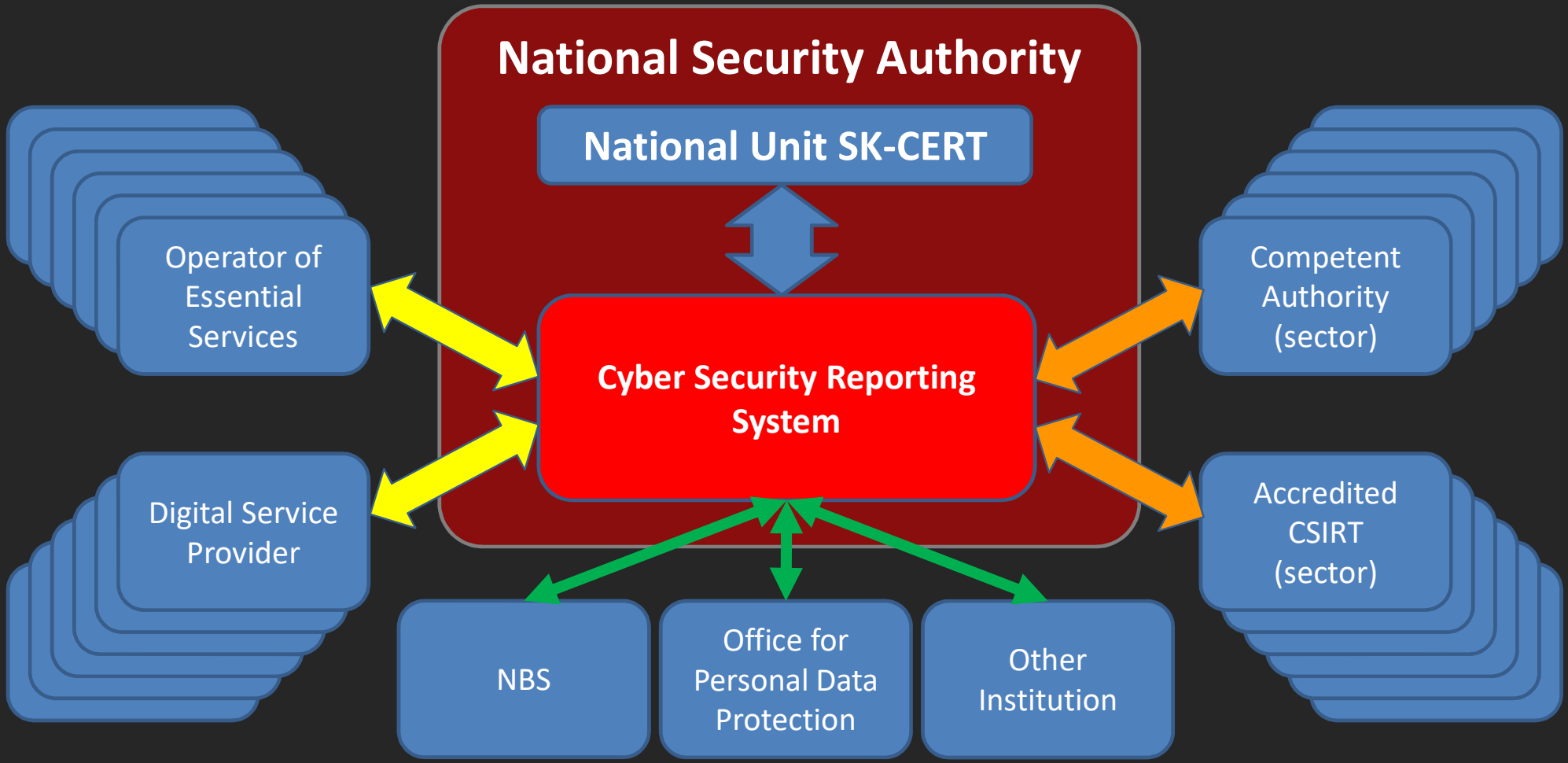
SK CERT



NATIONAL SECURITY AUTHORITY

CYBERSECURITY REPORTING SYSTEM

SK CERT



NATIONAL SECURITY AUTHORITY

INCIDENT HANDLING

SK CERT

- Sectorial CSIRTs should do
  - Coordination of real incidents within the sector
  - Incident Handling with Reporter from their sector

- National CSIRT responsibility is
  - Doing correlation of incidents across Slovak internet space
  - Comparison with list of actual IOC
  - Creating warnings to organizations without incident based on known problems in the SK internet space

NATIONAL SECURITY AUTHORITY

THANK YOU

rastislav.janota@nbu.gov.sk

SK NBÚ CERT