



Critical Information Infrastructure Protection Slovak Approach

Rastislav Janota

Director

National CERT of the Slovak Republic

National Security Authority

Europe Region
Cyberdrill

26-30 November 2018
Limassol, Cyprus





Motto:

Who should take care on
Cybersecurity?

WE ALL DO!

Everyone is responsible for own data
and own services...

- **2011 - Critical Infrastructure Protection**
 - Law build mostly around physical protection
 - Limited sector reach (many important areas was not covered)

- **April 2018 - Cybersecurity law**
 - Law prepared as Critical Information Infrastructure Protection Law
 - Many new sectors and subsectors included
 - Alignment with CIP Law
 - Build around European Cybersecurity Directive - NIS

- **General Data Protection Regulation (GDPR) – 2016/679**
 - To strengthen and unify data protection for all individuals within the European Union (EU)
 - Regulator – Office for Personal Data Protection of the Slovak Republic
- **Payment Services Directive (PSD2) – 2015/2366**
 - To regulate payment services and payment service providers throughout the European Union (EU)
 - Regulator – National Bank of Slovakia
- **Regulatory framework for electronic communications – Telecoms Package (2009)**
 - To create a common set of regulations for the telecoms industry across all 27 EU states
 - Regulator – Regulatory Authority for Electronic Communication and Postal Services
- **Network and Information Security Directive 2016/1148**
 - To force companies and organizations to protect their systems/data from cyber-attacks
 - Regulator – National Security Authority

- Minimum regulations approach used
- Practical approach to incident handling
- Opening voluntary 'win-win' cooperation with the market instead of mandatory duties

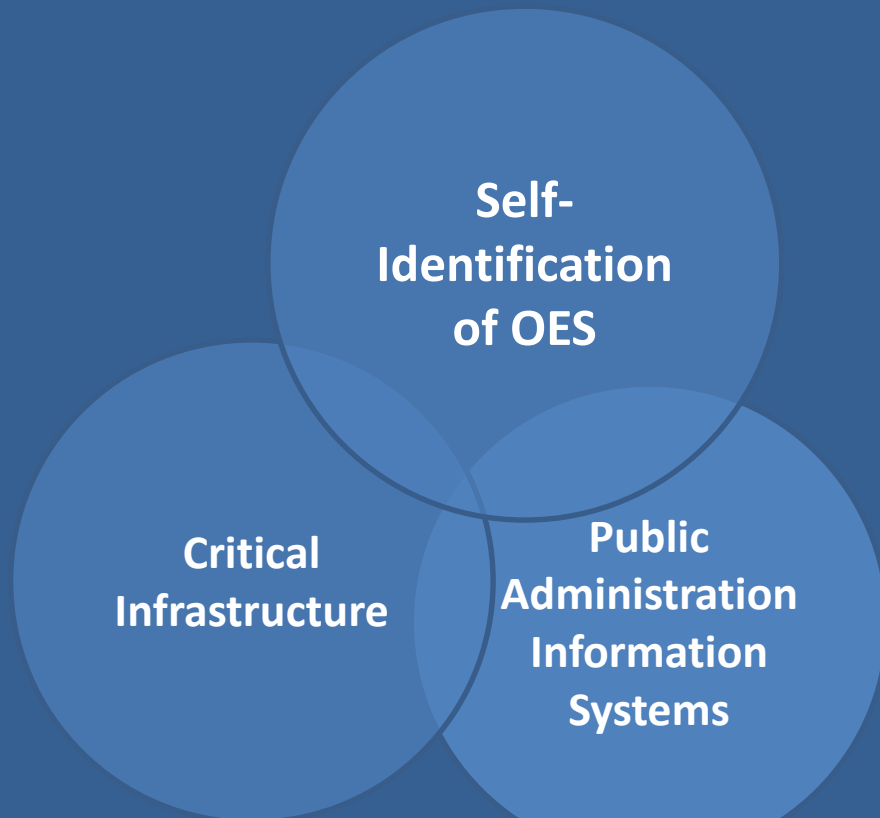
- Alignment with Critical Infrastructure Protection legislation
- Alignment with Intelligent Industry 4.0 government approach
- Definitions of sectors and subsectors for OES incl. competent bodies and their duties
 - (11 Sectors, 27+1 Sub Sectors, 11 Competent Authorities)

- Mandatory government CSIRTs for sectorial competent bodies, government outsourcing and last-resort option



- 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

Operators of Essential Services



- OES consist of 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)
- Definitions of sectors and subsectors for OES

Sector	Subsector	Competent authority	CIP	NIS	CiiP
Banking		Ministry of Finance		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transport	Air transport	Ministry of transport and construction	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Rail transport		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Water transport		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Road transport		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Digital Infrastructure		National Security Authority		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Electronic Communication	Satellite communication	Ministry of transport and construction	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Electronic communications networks and electronic communications services		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Financial market infrastructures		Ministry of Finance		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



Sector	Subsector	Competent authority	CIP	NIS	CIIP
Postal services		Ministry of trans & const	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Energy	Mining	Ministry of Economy	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Electricity		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Oil		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Gas		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Heat-power				<input checked="" type="checkbox"/>
Other Industries	Pharmaceutical	Ministry of Economy	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Metallurgical		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Chemical		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Intelligent Industry (4.0)				<input checked="" type="checkbox"/>
Health	All medical facilities (incl. Hospitals and private clinics)	Ministry of Health	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



Sector	Subsector	Competent authority	CIP	NIS	CIIP
Water and Atmosphere	Weather service	Ministry of the environment	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Water works		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Drinking water supply and distribution		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public Administration	Public order and security	Ministry of interior			<input checked="" type="checkbox"/>
	Information systems of public administration	Deputy Prime Minister's Office for Investments and Informatization	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
	Defense	Ministry of defense			<input checked="" type="checkbox"/>
	Intelligence services	Intelligence services			<input checked="" type="checkbox"/>
	Classified Information Protection	National Security Authority			<input checked="" type="checkbox"/>



NATIONAL
SECURITY
AUTHORITY

THANK YOU

rastislav.janota@nbu.gov.sk



Europe Region
Cyberdrill
26-30 November 2018
Limassol, Cyprus

