Impact of the Cybesecurity Law on the Czech Entities

Kharkiv
September 26, 2019

Jan Dienstbier

Vicepresident of the Czech Institute of CyberSecurity Managers
Jan.Dienstbier@cimib.cz

Motto

**„Cyber security is not a question of law,
it is a question of instinct for survival"**

existing Legal environment helps

ČIMIB

Relevant Laws

- 240/2000 Col., On crisis management and change of some laws
- 365/2000 Col., On information systems of the public sector
- 480/2004 Col., On some services of the information society
- 127/2005 Col., On electronic communications
- 412/2005 Col., On the protection of secret information and on the security capability, as amended in later provisions
- **181/2014 Col., on cyber security and change of some laws (Cyber Security Act)**

ČIMIB

Government Desrees & Regulations

- **432/2010 - On Identification Criteria of Critical Infrastructure**
- **315/2014 - Broadening 432/2010**
- **317/2014 - On Important Information Systems and Their Identification Criteria**
- 205/2017 - On the establishment of The National Cyber and Information Security Agency (NCISA) as a coordinator of the issues of cyber security and also the national authority in this area
- **82/2018 - On Security Measures, Cyber Security Incidents, Reactive Measures and Reporting Guidelines in the Area of Cyber Security (Decree on Cyber Security)**

ČIMIB

Act on Cyber Security
The English translation can be downloaded here.

- Focused mainly on Public Administration and Critical Infrastructure

  - Protection of the State

  - External liabilities

  - Protection of individuals

- Creates 2 CERTs (Govermental, National)

  - Government CERT (GovCERT.CZ) and other CSIRT teams play a key role in safeguarding the critical information infrastructure. Each country having its critical systems connected to the internet has to be able to effectively face security challenges, react on the incidents, coordinate actions to solve them and effectively prevent them. The task of these teams is to provide the security information and assistance to the state bodies, private entities and citizens. It plays a key role in enhancing the knowledge about internet security.

- Compliant with EU Cyber Security Strategy

  - Complient with NIS directive

ČIMIB

- **NIS - Directive on security of network and information systems**

- GDPR – General Data Protection Regulation
  - The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

- eIDAS Regulation
  - Regulation for the electronic identification and trust services for electronic transactions

- CNB Recomendations (for banking sector, not public)

The National Cyber and Information Security Agency (NCISA) is the central body of state administration for cyber security, including the protection of classified information in the area of information and communication systems and cryptographic protection. It is also in charge of the public regulated service of the Galileo satellite system. It was created on August 1, 2017 on the basis of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Act).

Main areas of activity of NCISA:

- operates the Government CERT (GovCERT.CZ)
- cooperation with other Czech CERT® teams and CSIRTs
- cooperation with international CERT® teams and CSIRTs
- drafting of security standards for information system CII/IIS
- support of education in the field of cyber security
- research and development in the area of cyber security
- protection of classified information in the field of information and communication systems
- cryptographic protection
- operates National PRS helpdesk - one of the services of European satellite system Galileo (NCPRS)

ČIMIB

- Main principles
  - Minimizing interference with the rights of private entities
  - Individual responsibility for ICT security – data security, responsibility for own networks & systems

- Defines
  - Security measures (standardization)
  - Obligation to report cyber security incidents
  - Obligation to take (counter)measure
  - Obligatory roles (Cybersecurity Committee, Cybersecurity Manager, Architect, Auditor)

ČIMIB

- Critical Information infrastructure (both public&private)
- Important Information System (just public)
- Basic Service (both public&private based on NIS - being implemented this year)
- Digital Service (eshops included coming out of NIS - being implemented this year)

- COMPULSORY SUBJECTS
  - Electronic communications service providers and entities providing electronic communications networks
  - Entities providing significant network
  - Operators of Important Information Systems
  - Operators of communication systems included in the Critical Information Infrastructure
  - Operators of information systems included in the Critical Information Infrastructure
  - Utilities
  - Transport …

SECURITY MEASURES

- Organisational
  - risk management, security policy, acquisition policy, maintenance, business continuity management, incident management, control and audit ...
- Technical
  - physical security, identity management, access rights, antivirus, detection, defense and analytical tools, application security, cryptography ...
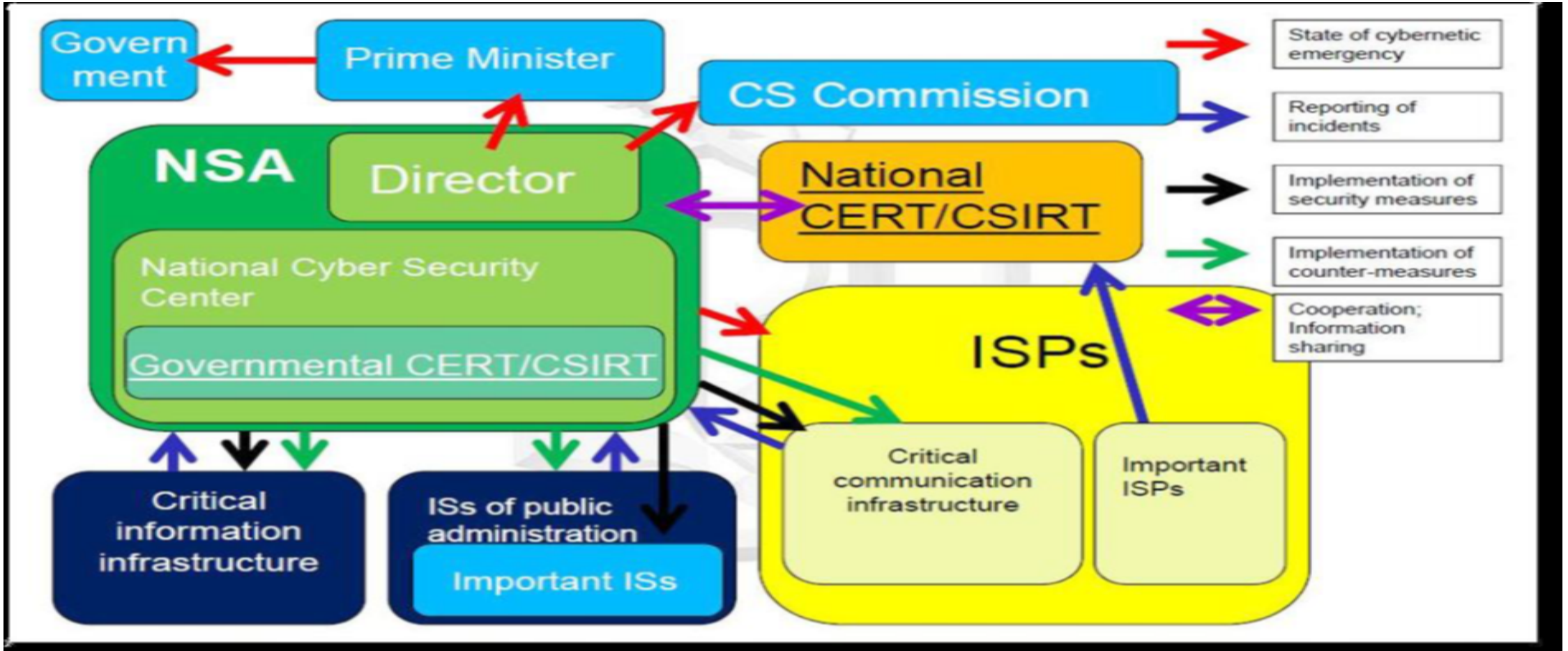- Security Documentation

ISO / IEC 27001 compliant

INPECTION & PENALTIES

- NÚKIB/NCISA

  - Request for corrective actions within a defined period

  - Define how to eliminate

  - Can prohibit an use of the system or until fix

  - Penalties for

    - Non-implementation of security measures

    - Non-reporting of cyber security incident
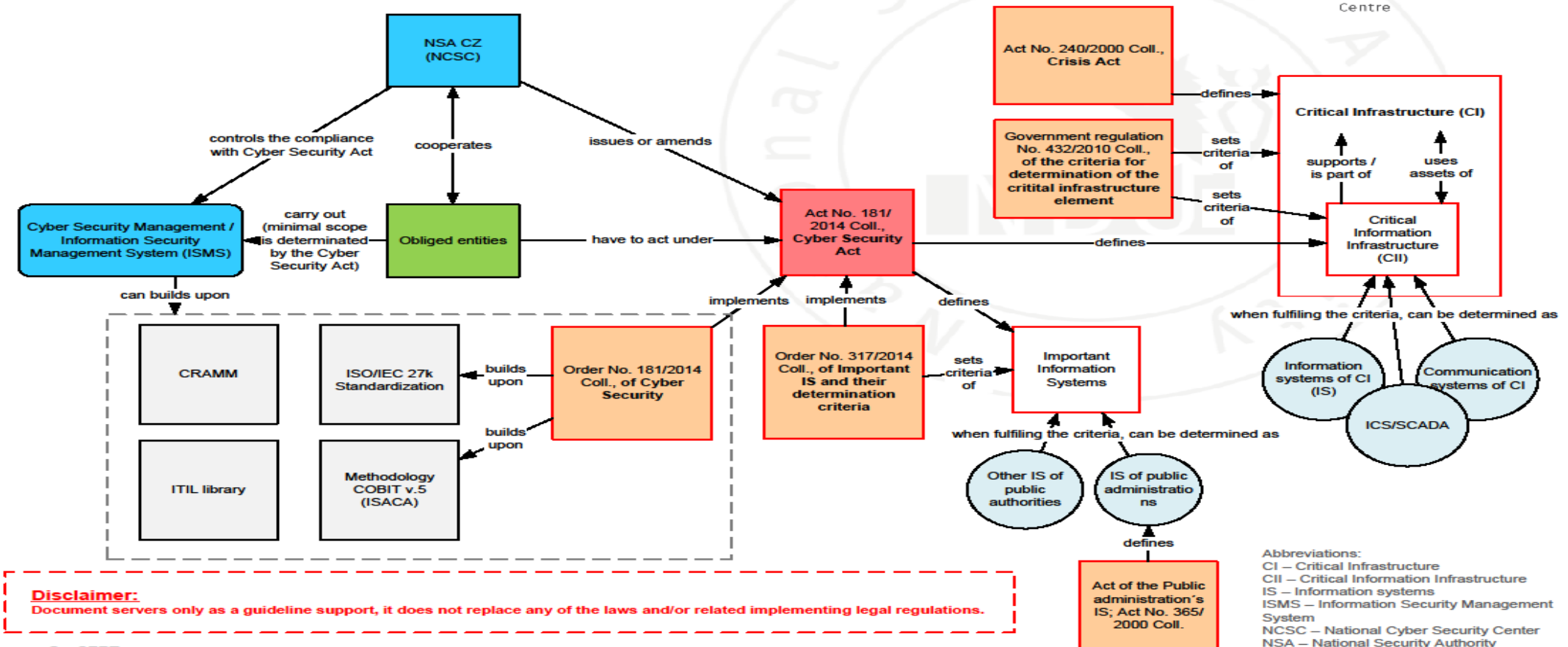
    - Up to 10M CZK

More info on **www.govcert.cz/en/**

ČIMIB

Currently cca

- 100 Critical Systems
- >200 Significant/Important Systems
- and determination still going on (Basic Services …)
- Huge increase in 2018

Thank you

Questions?

Jan.Dienstbier@cimib.cz