Security Conference

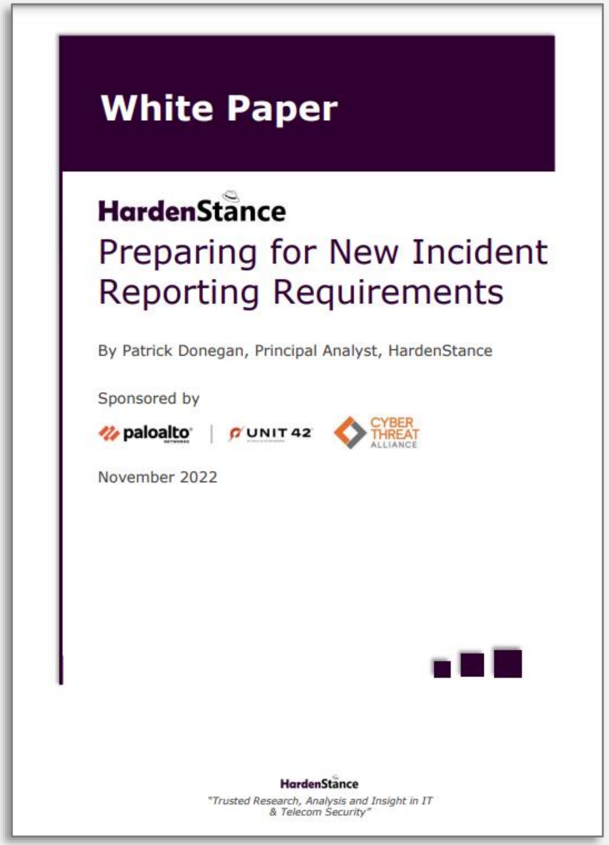
Global Cybersecurity Regulation

Presented by: Patrick Donegan, Principal Analyst

HardenStance

15/10/2023

Regulation & Policy



White Paper

HardenStance

Preparing for New Incident Reporting Requirements

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

paloalto | UNIT 42 CYBER THREAT ALLIANCE

November 2022

HardenStance
"Trusted Research, Analysis and Insight in IT & Telecom Security"

White Paper

HardenStance

Aligning Spectrum Policy with Cybersecurity Goals

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

ctia

May 2023

HardenStance
"Trusted Research, Analysis and Insight in IT & Telecom Security"

TTIS Telecom Threat Intelligence Summit 2023

TWO-DAY VIRTUAL EVENT 6 - 7 JUNE 2023 HOSTED BY HardenStance

The event dedicated to improving cyber security outcomes for the telecom sector and its customers through threat intelligence sharing.

REGISTER TODAY

SPONSORS ENEA AdaptiveMobile Security NOKIA FORTINET NETSCOUT

PARTICIPATING COMPANIES FIRST MITRE Dataplane.org CYBER THREAT ALLIANCE GSMA Telefónica

THE END OF LAISSEZ-FAIRE IN TELECOM CYBER SECURITY REGULATION

WEBINAR HOSTED BY HardenStance

A discussion with
Gerry McQuaid, Ofcom
Peter Haigh, NCSC
Nils Ahrlich, Nokia
Patrick Donegan, HardenStance

20 APRIL 2023
14:30 GMT | 15:30 CET | 9:30 EST

REGISTER TODAY

SPONSORED BY NOKIA

PARTICIPATING ORGANISATIONS Ofcom National Cyber Security Centre

Aligning with the NIS2 Directive:
Cybersecurity Guidelines for Europe's Telecom Operators

WEBINAR

NILS AHRLICH
Global Head of Security Consulting, Nokia

8 NOVEMBER 2023
15:00 Paris | 14:00 London | 9:30 New York

REGISTER TODAY

ORGANISED BY HardenStance

SPONSORED BY NOKIA

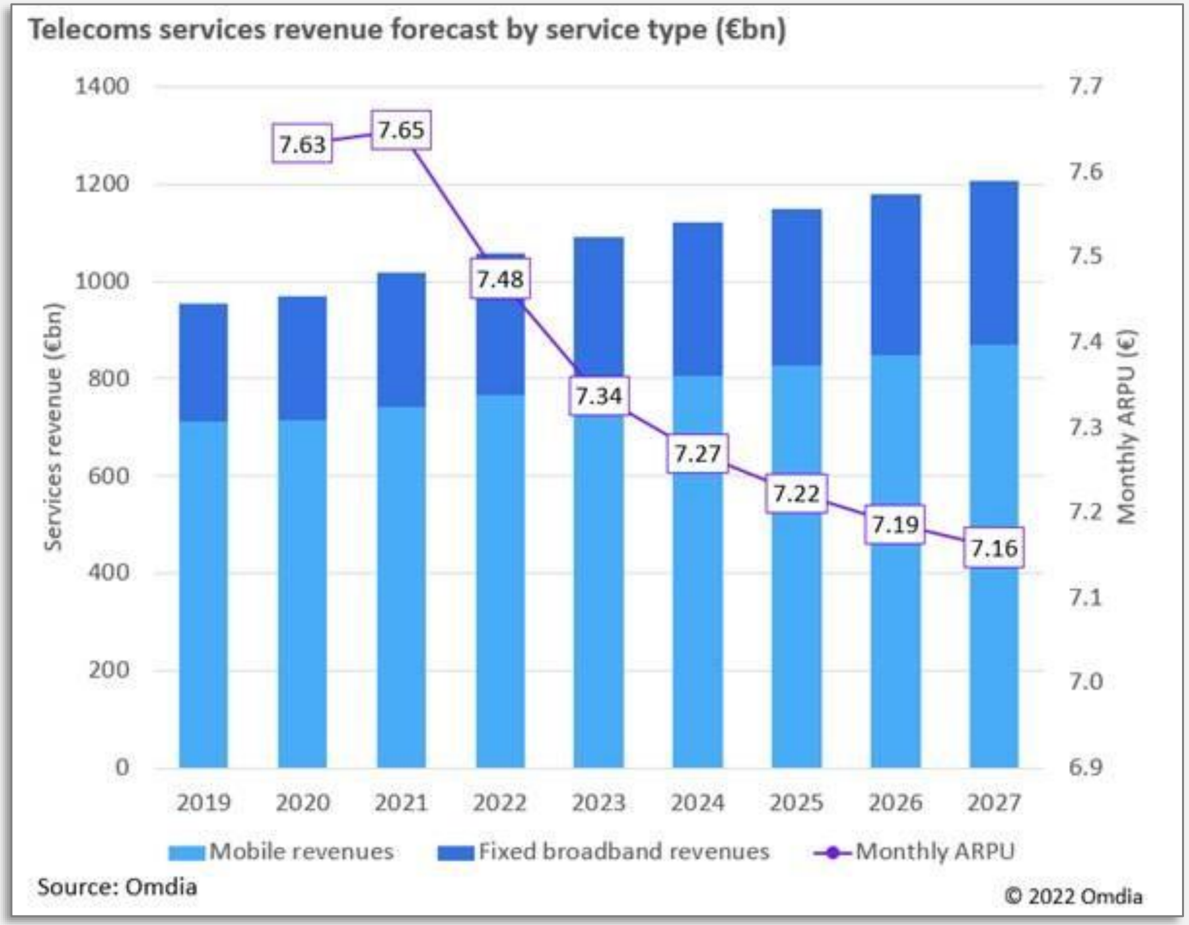
FEATURING CYBER THREAT ALLIANCE

Agenda

1. The commercial context
2. General trends in cybersecurity regulation of telecoms.
3. National and regional examples.
4. (Some of) The regulator’s priorities
5. Summary and recommendations

1. The commercial context

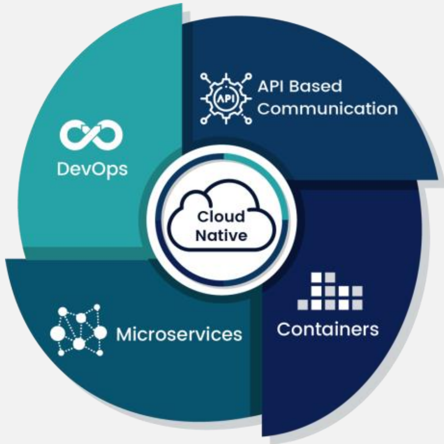
The commercial context



Telecoms services revenue forecast by service type (€bn)

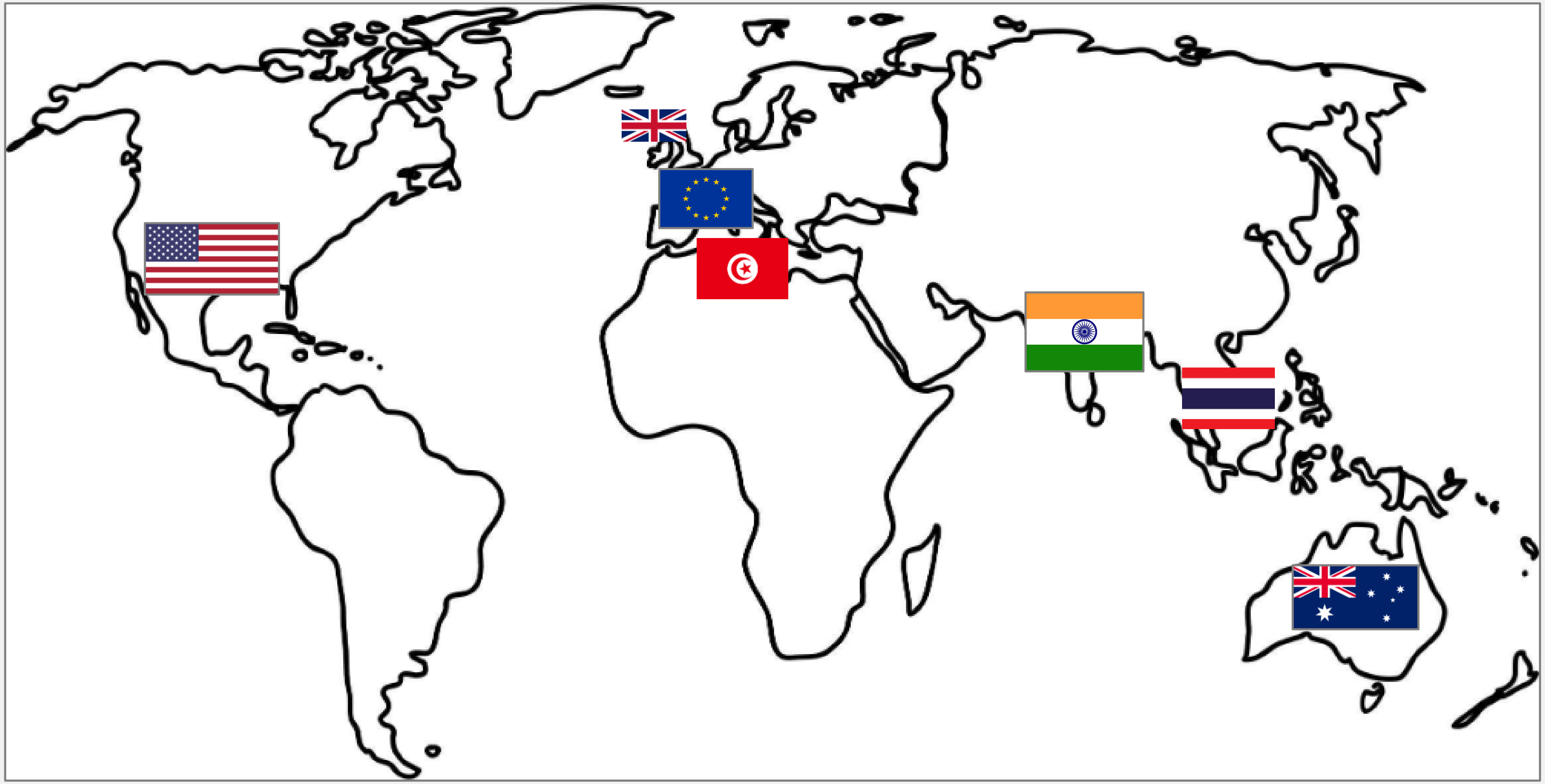
Source: Omdia

© 2022 Omdia

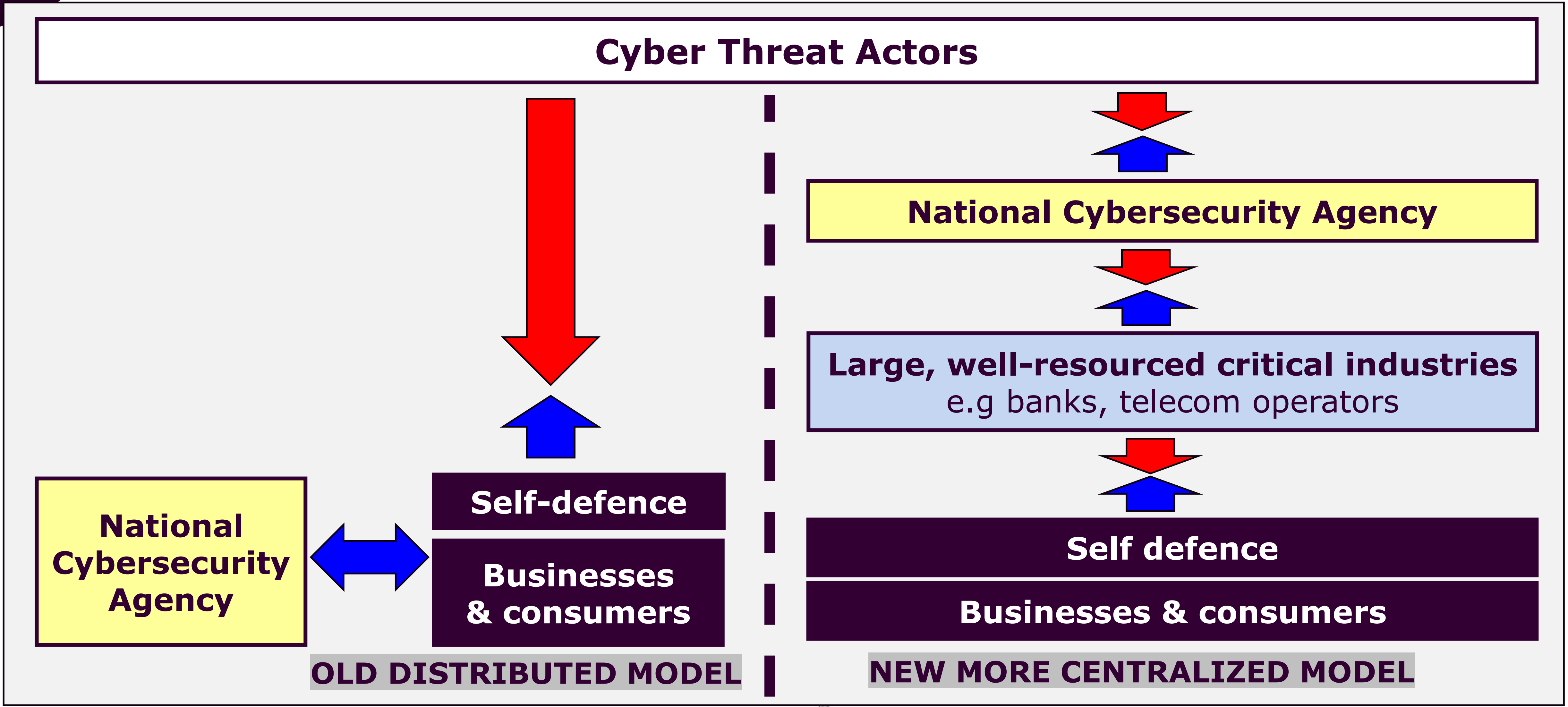


2. Trends in cybersecurity regulation of telecoms

Cybersecurity regulation is trending



The trend in cybersecurity regulation



Cyber Threat Actors
National Cybersecurity Agency
Self-defence
Businesses & consumers
OLD DISTRIBUTED MODEL
National Cybersecurity Agency
Large, well-resourced critical industries
e.g banks, telecom operators
Self defence
Businesses & consumers
NEW MORE CENTRALIZED MODEL

HardenStance

There’s a heavier burden to be borne

HardenStance

3. Regional and national examples

A new start in Australia

Clare O'Neil, Minister for Home Affairs & Minister for Cybersecurity

" **The old school way of thinking about cybersecurity is that events like those at Optus and others are about private events, affecting individuals and companies**.

But when you run systems of national significance, or when you hold personal information about literally half [your] population, that's not just of interest to the company itself or to individual customers. It's also of national interest. "

" Cybersecurity is not a problem we're going to resolve by teaching every teenager and grandmother what 2FA is. There are lots of risks that people can't manage themselves.

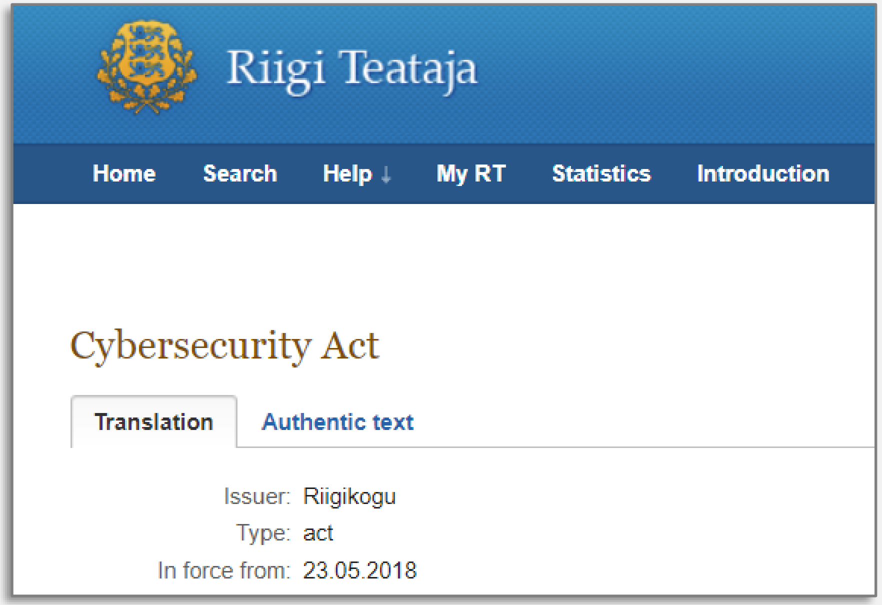
One of the principles driving our cybersecurity strategy is to push responsibilities for cyber protection onto the actors in the economy that can most manage them.

"These companies have a lot more power and control over these problems than the customers they serve. We should be forcing them to take more responsibility for what goes on on their networks from a cybersecurity perspective. "

*Comments made in the July 27 2023 edition of the 'Risky Business' podcast

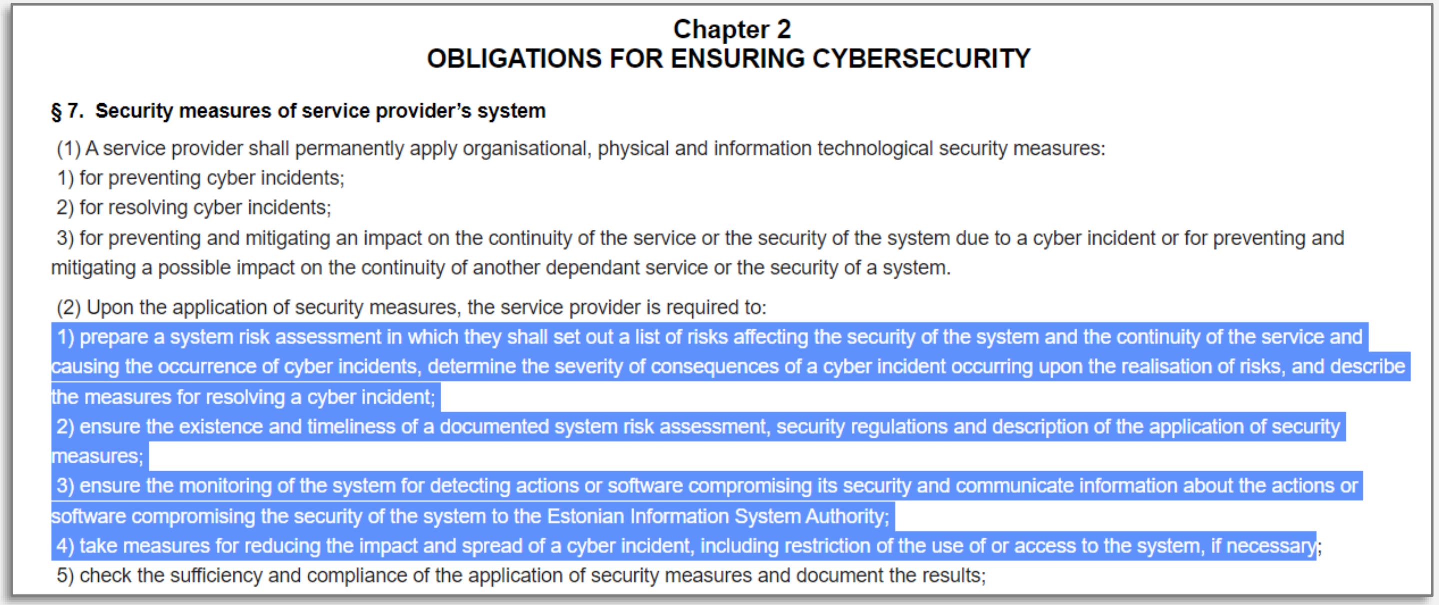
Estonia’s Cybersecurity Act of 2018

(Implements EECC)



Cybersecurity Act

Issuer: Riigikogu
Type: act
In force from: 23.05.2018



Chapter 2
OBLIGATIONS FOR ENSURING CYBERSECURITY

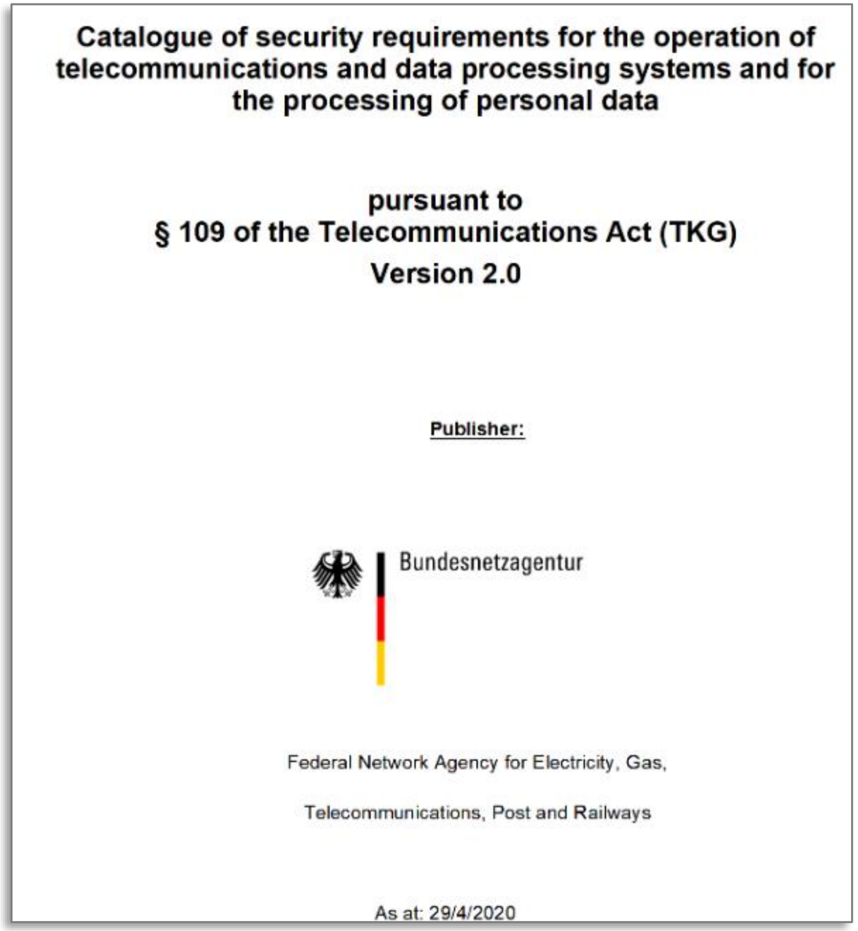
§ 7. Security measures of service provider’s system

(1) A service provider shall permanently apply organisational, physical and information technological security measures:
1) for preventing cyber incidents;
2) for resolving cyber incidents;
3) for preventing and mitigating an impact on the continuity of the service or the security of the system due to a cyber incident or for preventing and mitigating a possible impact on the continuity of another dependant service or the security of a system.

(2) Upon the application of security measures, the service provider is required to:
1) prepare a system risk assessment in which they shall set out a list of risks affecting the security of the system and the continuity of the service and causing the occurrence of cyber incidents, determine the severity of consequences of a cyber incident occurring upon the realisation of risks, and describe the measures for resolving a cyber incident;
2) ensure the existence and timeliness of a documented system risk assessment, security regulations and description of the application of security measures;
3) ensure the monitoring of the system for detecting actions or software compromising its security and communicate information about the actions or software compromising the security of the system to the Estonian Information System Authority;
4) take measures for reducing the impact and spread of a cyber incident, including restriction of the use of or access to the system, if necessary;
5) check the sufficiency and compliance of the application of security measures and document the results;

Germany’s TKMoG* of 2020

*Telekommunikationsmodernisierungsgesetz (implements EECC)



Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data

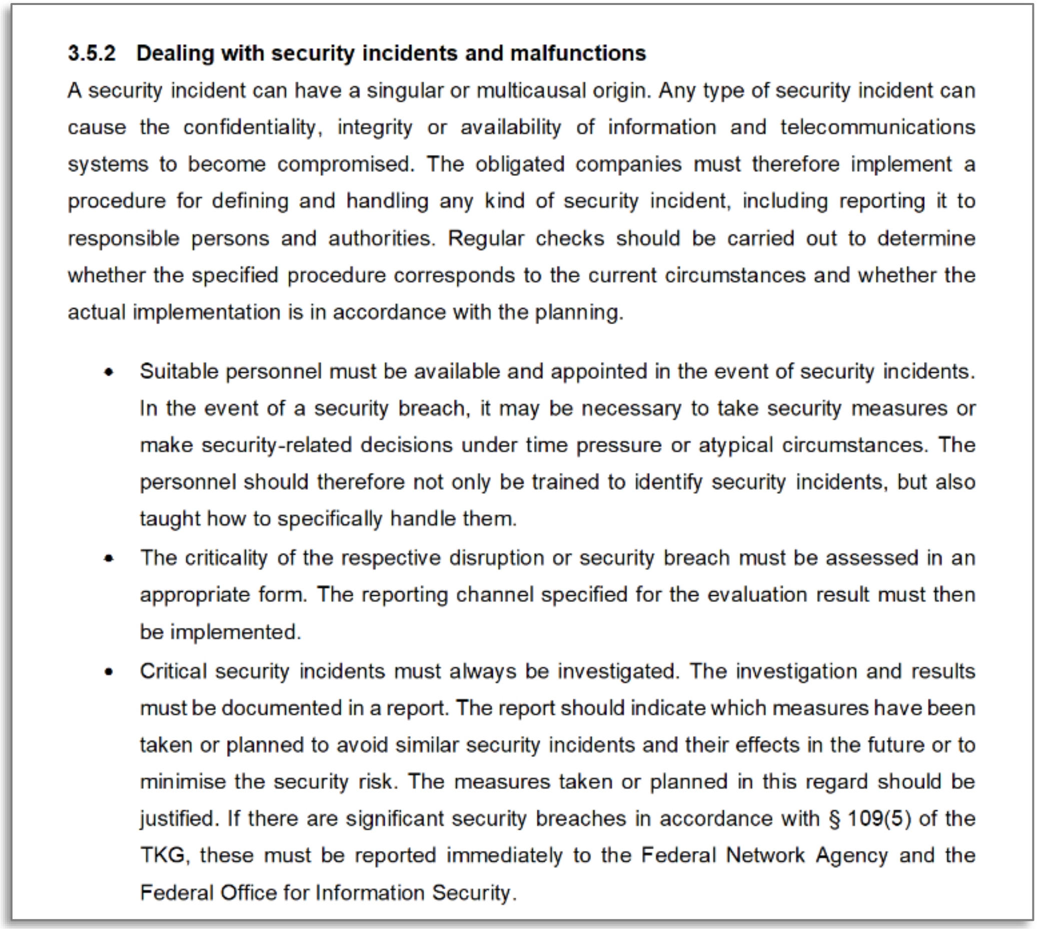
pursuant to
§ 109 of the Telecommunications Act (TKG)
Version 2.0

Publisher:

Bundesnetzagentur

Federal Network Agency for Electricity, Gas,
Telecommunications, Post and Railways

As at: 29/4/2020



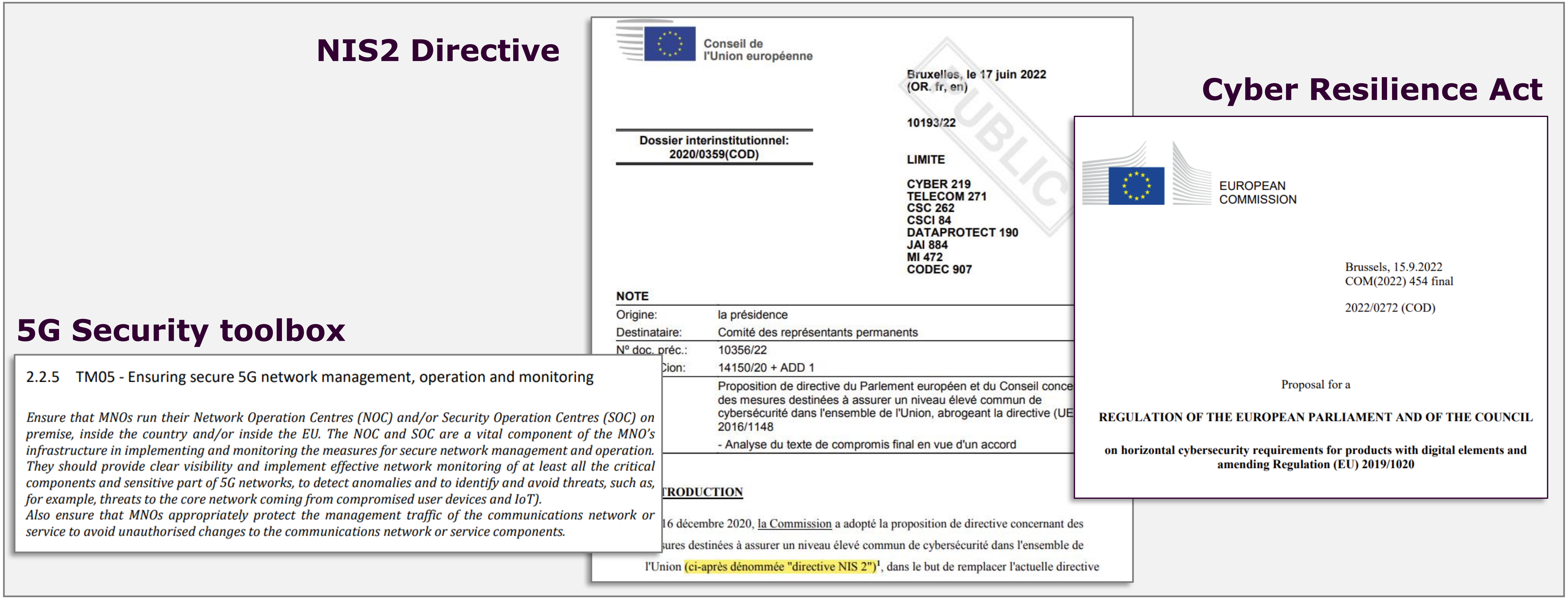
3.5.2 Dealing with security incidents and malfunctions

A security incident can have a singular or multicausal origin. Any type of security incident can cause the confidentiality, integrity or availability of information and telecommunications systems to become compromised. The obligated companies must therefore implement a procedure for defining and handling any kind of security incident, including reporting it to responsible persons and authorities. Regular checks should be carried out to determine whether the specified procedure corresponds to the current circumstances and whether the actual implementation is in accordance with the planning.

- Suitable personnel must be available and appointed in the event of security incidents. In the event of a security breach, it may be necessary to take security measures or make security-related decisions under time pressure or atypical circumstances. The personnel should therefore not only be trained to identify security incidents, but also taught how to specifically handle them.
- The criticality of the respective disruption or security breach must be assessed in an appropriate form. The reporting channel specified for the evaluation result must then be implemented.
- Critical security incidents must always be investigated. The investigation and results must be documented in a report. The report should indicate which measures have been taken or planned to avoid similar security incidents and their effects in the future or to minimise the security risk. The measures taken or planned in this regard should be justified. If there are significant security breaches in accordance with § 109(5) of the TKG, these must be reported immediately to the Federal Network Agency and the Federal Office for Information Security.

HardenStance

EU Regulation and Legislation



NIS2 Directive

Conseil de
l'Union européenne

Bruxelles, le 17 juin 2022
(OR. fr, en)

10193/22

LIMITE

CYBER 219
TELECOM 271
CSC 262
CSCI 84
DATAPROTECT 190
JAI 884
MI 472
CODEC 907

Dossier interinstitutionnel:
2020/0359(COD)

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents
N° doc. préc.:	10356/22
...ion:	14150/20 + ADD 1
	Proposition de directive du Parlement européen et du Conseil conce... des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 - Analyse du texte de compromis final en vue d'un accord

...TRODUCTION

...16 décembre 2020, la Commission a adopté la proposition de directive concernant des ...ures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (ci-après dénommée "directive NIS 2")[1], dans le but de remplacer l'actuelle directive

Cyber Resilience Act

EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

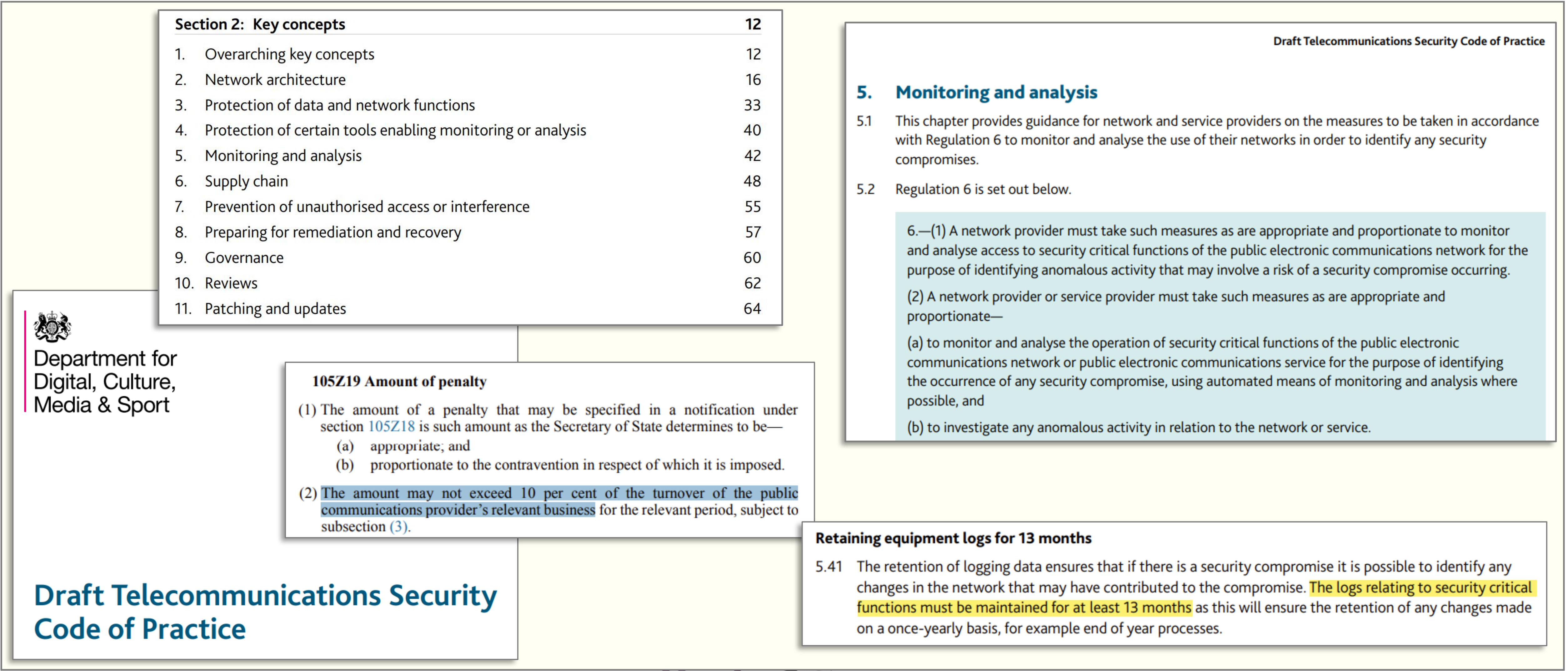
on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

5G Security toolbox

2.2.5 TM05 - Ensuring secure 5G network management, operation and monitoring

Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU. The NOC and SOC are a vital component of the MNO's infrastructure in implementing and monitoring the measures for secure network management and operation. They should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and IoT).
Also ensure that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components.

The Telecom (Security) Act



Department for
Digital, Culture,
Media & Sport

Draft Telecommunications Security Code of Practice

105Z19 Amount of penalty

(1) The amount of a penalty that may be specified in a notification under section 105Z18 is such amount as the Secretary of State determines to be—

(a) appropriate; and

(b) proportionate to the contravention in respect of which it is imposed.

(2) The amount may not exceed 10 per cent of the turnover of the public communications provider's relevant business for the relevant period, subject to subsection (3).

Draft Telecommunications Security Code of Practice

5. Monitoring and analysis

5.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 6 to monitor and analyse the use of their networks in order to identify any security compromises.

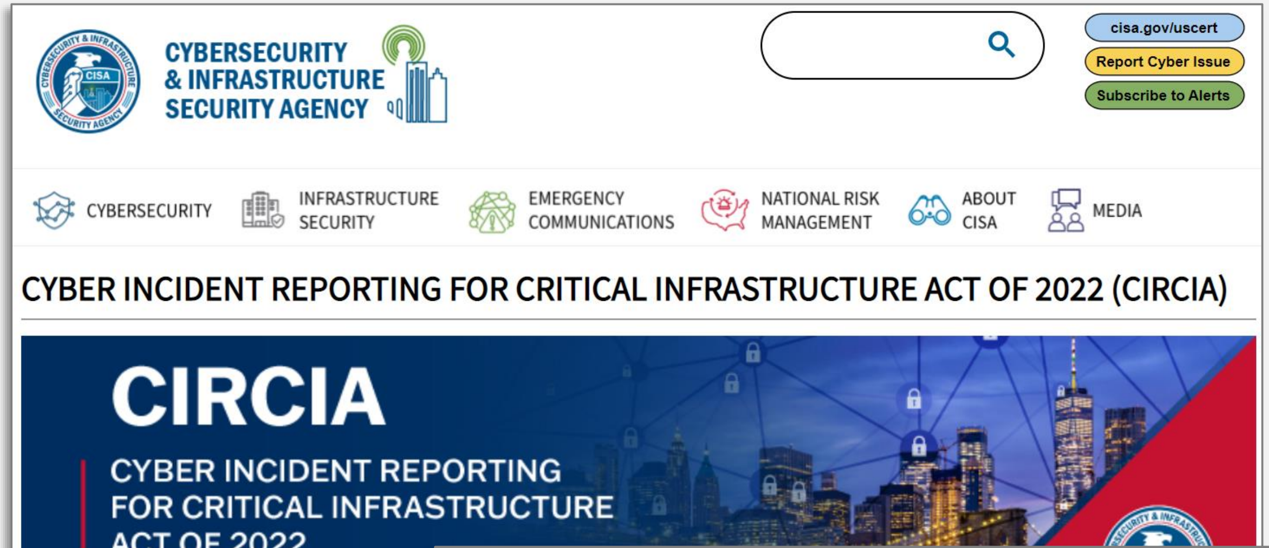
5.2 Regulation 6 is set out below.

> 6.—(1) A network provider must take such measures as are appropriate and proportionate to monitor and analyse access to security critical functions of the public electronic communications network for the purpose of identifying anomalous activity that may involve a risk of a security compromise occurring.
>
> (2) A network provider or service provider must take such measures as are appropriate and proportionate—
>
> (a) to monitor and analyse the operation of security critical functions of the public electronic communications network or public electronic communications service for the purpose of identifying the occurrence of any security compromise, using automated means of monitoring and analysis where possible, and
>
> (b) to investigate any anomalous activity in relation to the network or service.

Retaining equipment logs for 13 months

5.41 The retention of logging data ensures that if there is a security compromise it is possible to identify any changes in the network that may have contributed to the compromise. The logs relating to security critical functions must be maintained for at least 13 months as this will ensure the retention of any changes made on a once-yearly basis, for example end of year processes.

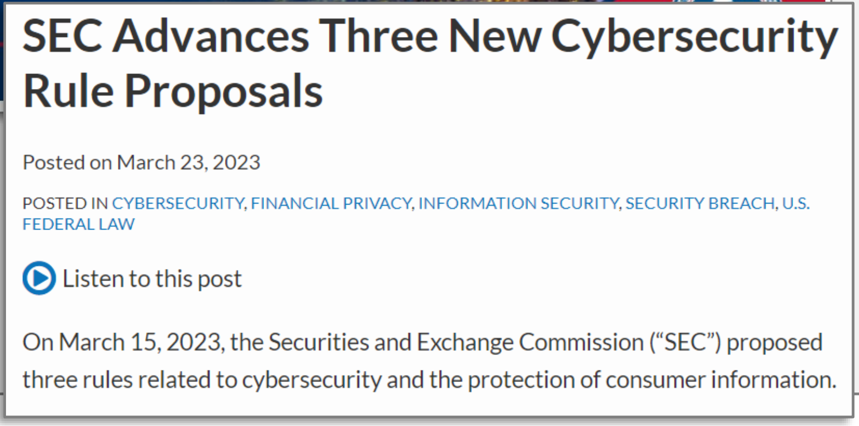
Even in America…



CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA)

CIRCIA

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

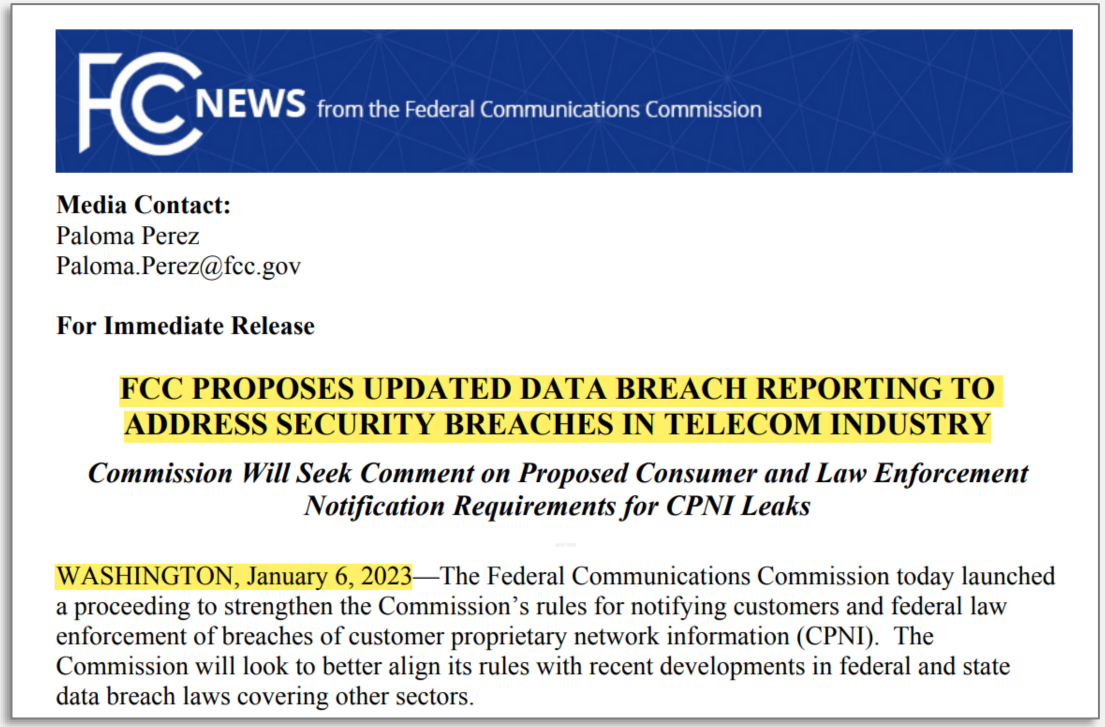


SEC Advances Three New Cybersecurity Rule Proposals

Posted on March 23, 2023

POSTED IN CYBERSECURITY, FINANCIAL PRIVACY, INFORMATION SECURITY, SECURITY BREACH, U.S. FEDERAL LAW

On March 15, 2023, the Securities and Exchange Commission ("SEC") proposed three rules related to cybersecurity and the protection of consumer information.



Media Contact:
Paloma Perez
Paloma.Perez@fcc.gov

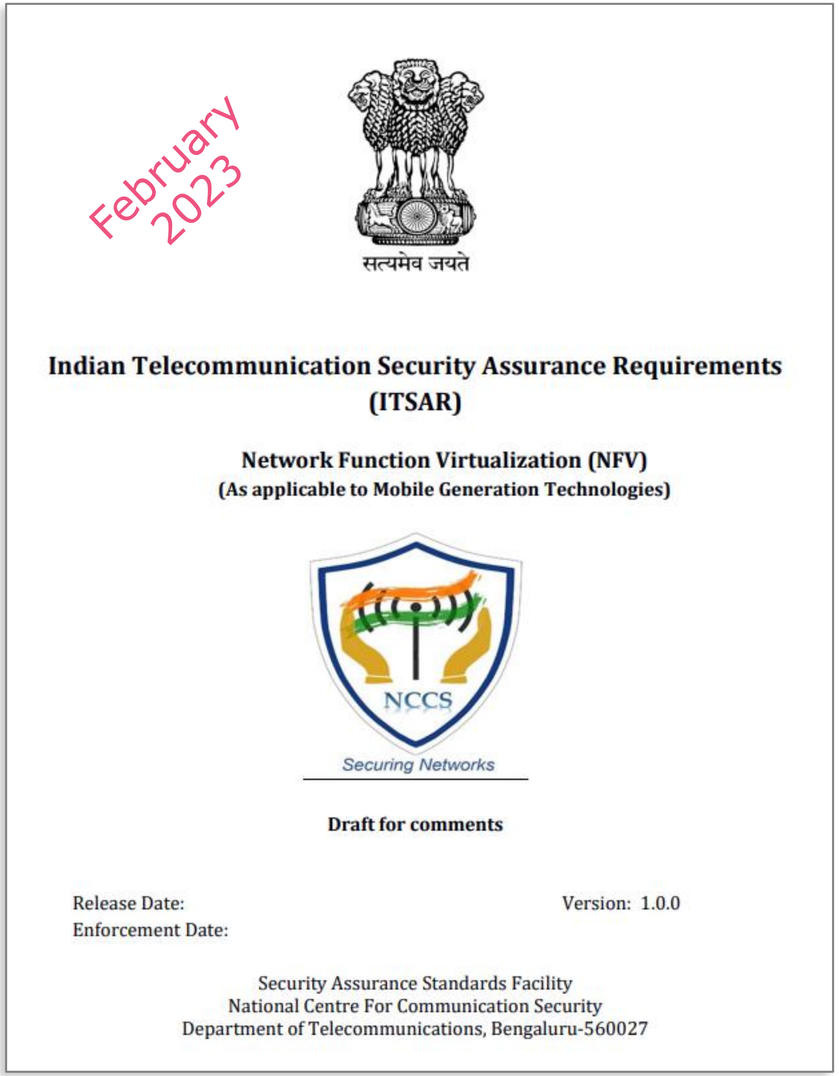
For Immediate Release

FCC PROPOSES UPDATED DATA BREACH REPORTING TO ADDRESS SECURITY BREACHES IN TELECOM INDUSTRY

Commission Will Seek Comment on Proposed Consumer and Law Enforcement Notification Requirements for CPNI Leaks

WASHINGTON, January 6, 2023—The Federal Communications Commission today launched a proceeding to strengthen the Commission's rules for notifying customers and federal law enforcement of breaches of customer proprietary network information (CPNI). The Commission will look to better align its rules with recent developments in federal and state data breach laws covering other sectors.

The ITSARs of India's DoT



February 2023

सत्यमेव जयते

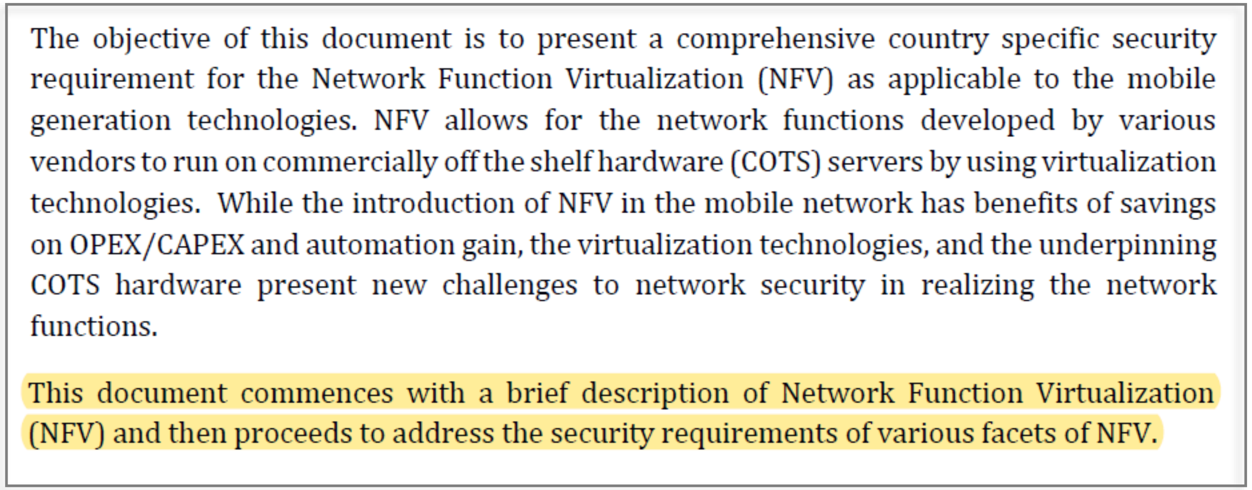
Indian Telecommunication Security Assurance Requirements (ITSAR)

Network Function Virtualization (NFV)
(As applicable to Mobile Generation Technologies)

Draft for comments

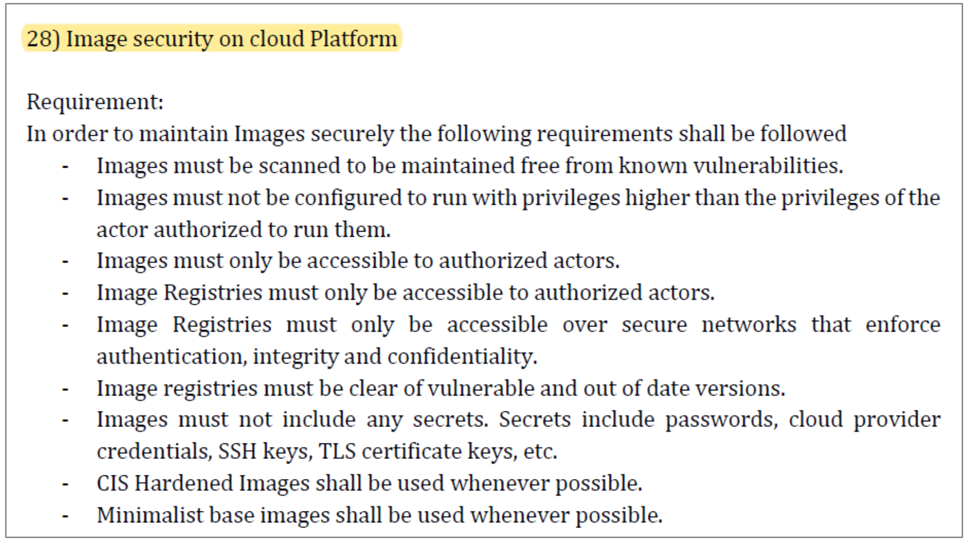
Release Date: Version: 1.0.0
Enforcement Date:

Security Assurance Standards Facility
National Centre For Communication Security
Department of Telecommunications, Bengaluru-560027



The objective of this document is to present a comprehensive country specific security requirement for the Network Function Virtualization (NFV) as applicable to the mobile generation technologies. NFV allows for the network functions developed by various vendors to run on commercially off the shelf hardware (COTS) servers by using virtualization technologies. While the introduction of NFV in the mobile network has benefits of savings on OPEX/CAPEX and automation gain, the virtualization technologies, and the underpinning COTS hardware present new challenges to network security in realizing the network functions.

This document commences with a brief description of Network Function Virtualization (NFV) and then proceeds to address the security requirements of various facets of NFV.



28) Image security on cloud Platform

Requirement:
In order to maintain Images securely the following requirements shall be followed

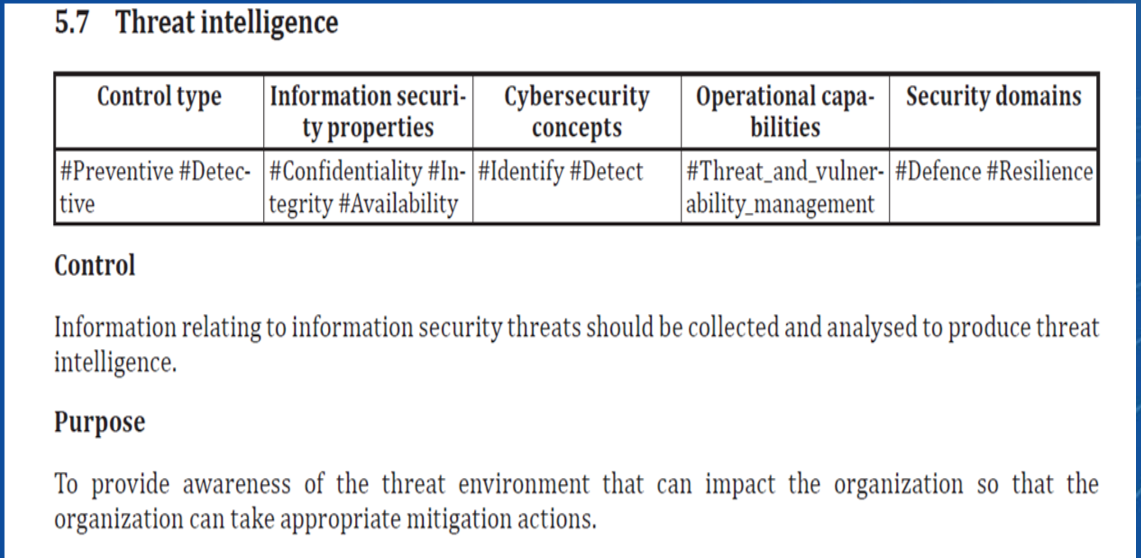
- Images must be scanned to be maintained free from known vulnerabilities.
- Images must not be configured to run with privileges higher than the privileges of the actor authorized to run them.
- Images must only be accessible to authorized actors.
- Image Registries must only be accessible to authorized actors.
- Image Registries must only be accessible over secure networks that enforce authentication, integrity and confidentiality.
- Image registries must be clear of vulnerable and out of date versions.
- Images must not include any secrets. Secrets include passwords, cloud provider credentials, SSH keys, TLS certificate keys, etc.
- CIS Hardened Images shall be used whenever possible.
- Minimalist base images shall be used whenever possible.

HardenStance

Threat Intelligence in Standards and Regulation

ISO/IOC DIS 27002

Information security, cybersecurity and privacy protection — Information security controls



5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Detect	#Threat_and_vulnerability_management	#Defence #Resilience

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose

To provide awareness of the threat environment that can impact the organization so that the organization can take appropriate mitigation actions.

Decree-Law No. 2023-17 of March 11, 2023, relating to cybersecurity

Art. 18 - Within the framework of response to cybernetic emergencies, the National Agency of Cyber Security carries out the following missions:

- Develop and apply the national cyber emergency response plan **in collaboration with public and private sector cyber emergency response centres**.
- **Put in place the technical procedures necessary for the early detection of cybernetic incidents and attacks that threaten the national cybernetic space.**
- **Set up and operate reporting channels for cyber incidents and attacks.**
- Reduce the impact of cyber incidents and attacks and ensure business continuity and rapid recovery from their effects.
- **Alert institutions, administrations and individuals, strengthen information systems, manage incidents, organize and coordinate efforts to remedy weaknesses, study them, analyze them and plan appropriate solutions**.

Art. 20 - The organizations mentioned in article 6 of the decree-law herein **shall immediately inform the national contact point for the response to cyber emergencies or the cyber emergency response center of cyber incidents and attacks and must comply with the urgent measures adopted by these**.

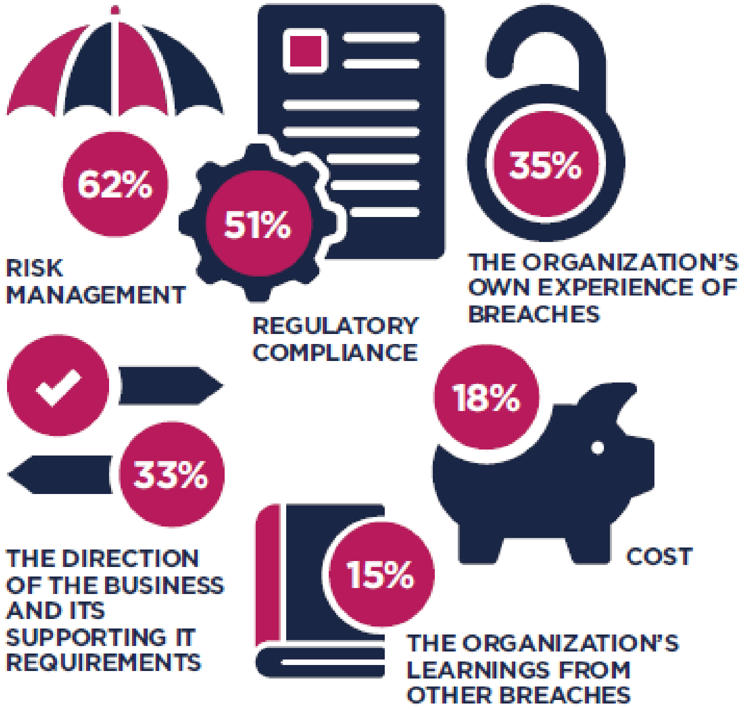
4. (Some of) The Regulator’s priorities

The regulator’s priorities

#1 Cyber risk management

- Central to the NIS2 Directive
- Compliance > Compliance+ >Risk Management
- New regulation a driver but nevertheless subordinate (TM Forum survey research)

Most important factors in prioritizing security spending



TM Forum, 2023

The regulator’s priorities

#2 Incident Reporting

Core Transport RAN UE

Visibility Threat Monitoring Detection & Response

Legislation/Regulation

Enforcement

“24/72 hours” “30 days”

The regulator’s priorities
#3 Better cyber threat intelligence sharing

Challenges

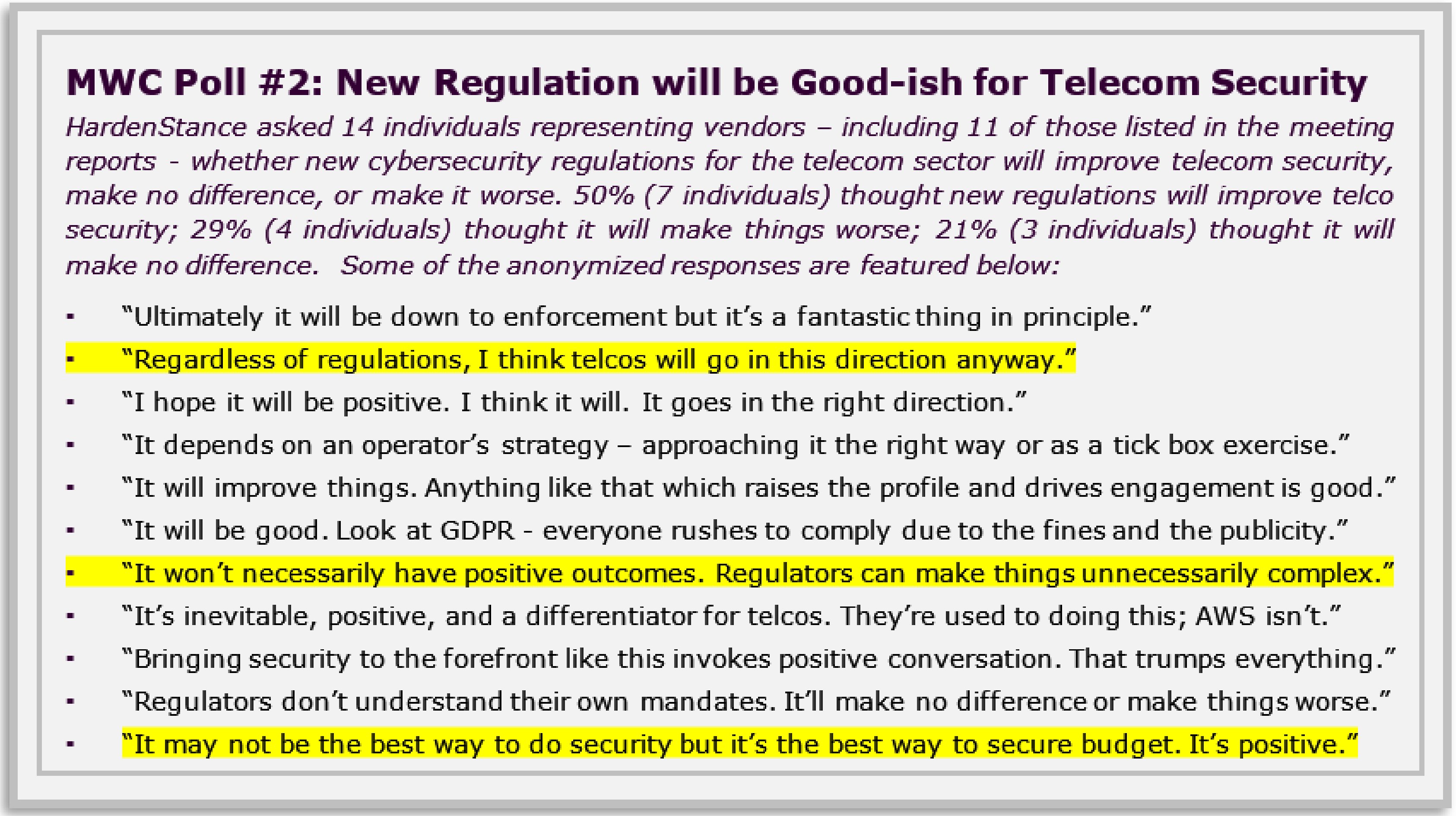
- Common nomenclature and formatting.
- Privacy regulations.
- ‘Trust’.
- Automation

Positive developments

- MITRE’s 5G FiGHT Framework.
- GSMA’s FASG.
- ETSI and GSMA CVD programmes.

5. Summary and Recommendations

An informal ‘poll’ from MWC 2023



MWC Poll #2: New Regulation will be Good-ish for Telecom Security

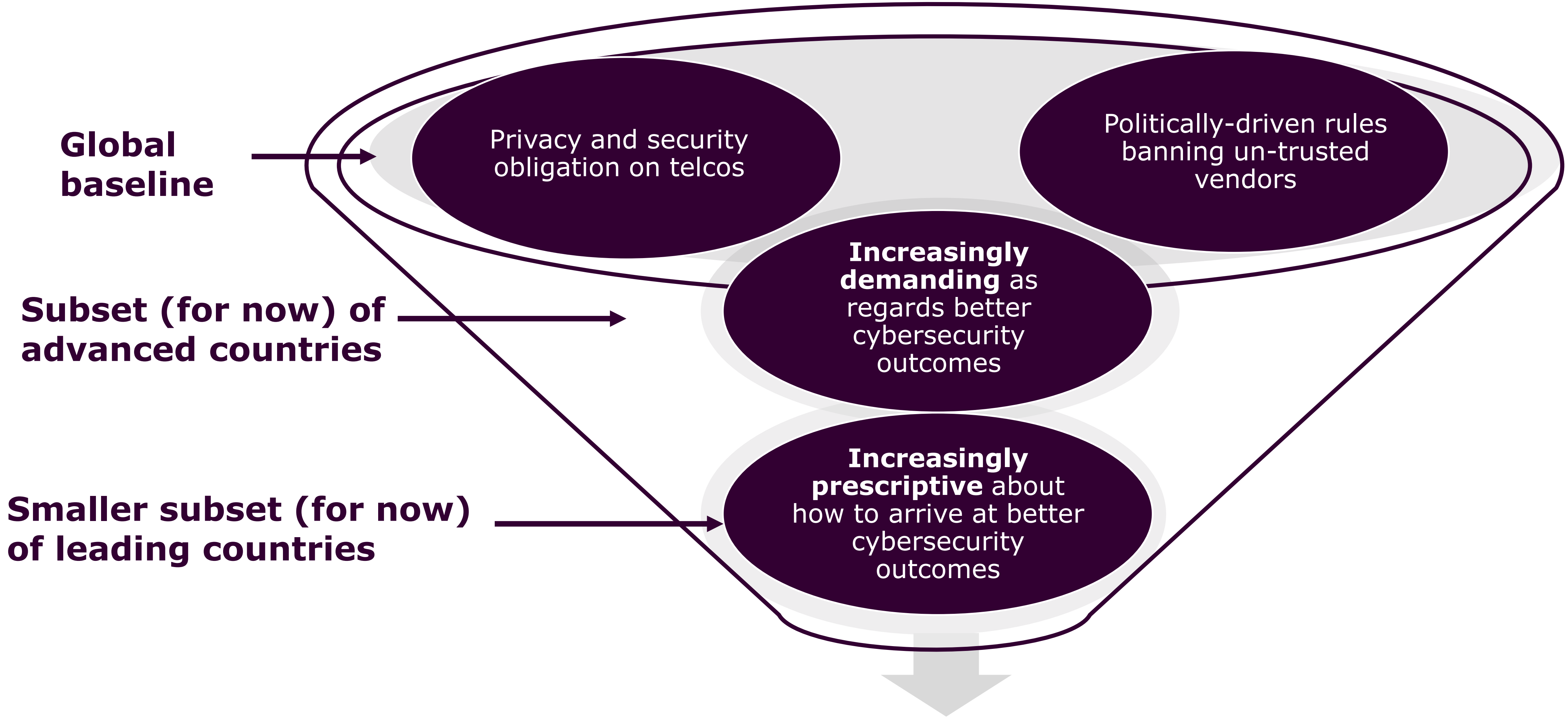
HardenStance asked 14 individuals representing vendors – including 11 of those listed in the meeting reports - whether new cybersecurity regulations for the telecom sector will improve telecom security, make no difference, or make it worse. 50% (7 individuals) thought new regulations will improve telco security; 29% (4 individuals) thought it will make things worse; 21% (3 individuals) thought it will make no difference. Some of the anonymized responses are featured below:

- “Ultimately it will be down to enforcement but it’s a fantastic thing in principle.”
- “Regardless of regulations, I think telcos will go in this direction anyway.”
- “I hope it will be positive. I think it will. It goes in the right direction.”
- “It depends on an operator’s strategy – approaching it the right way or as a tick box exercise.”
- “It will improve things. Anything like that which raises the profile and drives engagement is good.”
- “It will be good. Look at GDPR - everyone rushes to comply due to the fines and the publicity.”
- “It won’t necessarily have positive outcomes. Regulators can make things unnecessarily complex.”
- “It’s inevitable, positive, and a differentiator for telcos. They’re used to doing this; AWS isn’t.”
- “Bringing security to the forefront like this invokes positive conversation. That trumps everything.”
- “Regulators don’t understand their own mandates. It’ll make no difference or make things worse.”
- “It may not be the best way to do security but it’s the best way to secure budget. It’s positive.”

Taken from “MWC23: Taking Stock of Telco Security” (www.hardenstance.com)

HardenStance

Telco Security Re- Regulation 2.0



Global baseline

Subset (for now) of advanced countries

Smaller subset (for now) of leading countries

Privacy and security obligation on telcos

Politically-driven rules banning un-trusted vendors

Increasingly demanding as regards better cybersecurity outcomes

Increasingly prescriptive about how to arrive at better cybersecurity outcomes

HardenStance

Recommendations for telcos and their regulators

Regulators

- Maintain ‘engagement discipline’.
- Practise risk management yourselves.
- Prescribe with flexibility.
- Enforce with flexibility.
- Staff up.

Telcos

- Commit appropriately
- Engage with people as well as processes.
- “Yes” ? No!
- Collaborate – internally and externally.
- Invest.

Conclusion

Many requirements are new and challenging…

…Engagement, expertise and investment are all needed…

… in equal measure….and on all sides

patrick.donegan@hardenstance.com