Working Document of the NPC Study
Dynamic Delivery –
America's Evolving Oil and Natural Gas Transportation Infrastructure
Made Available December 12, 2019

Topic Paper #4-13

EUROPENA UNION CYBERSECURITY RESPONSE TO ATTACKS ON CRITICAL INFRASTRUCTURE

Prepared for the

Technology Advancement and Deployment Task Group

On December 12, 2019 the National Petroleum Council (NPC) in approving its report, *Dynamic Delivery – America's Evolving Oil and Natural Gas Transportation Infrastructure*, also approved the making available of certain materials used in the study process, including detailed, specific subject matter papers prepared or used by the study's Permitting, Siting, and Community Engagement for Infrastructure Development Task Group. These Topic Papers were working documents that were part of the analyses that led to development of the summary results presented in the report's Executive Summary and Chapters.

These Topic Papers represent the views and conclusions of the authors. The National Petroleum Council has not endorsed or approved the statements and conclusions contained in these documents, but approved the publication of these materials as part of the study process.

The NPC believes that these papers will be of interest to the readers of the report and will help them better understand the results. These materials are being made available in the interest of transparency.

The attached paper is one of 26 such working documents used in the study analyses. Appendix C of the final NPC report provides a complete list of the 26 Topic Papers. The full papers can be viewed and downloaded from the report section of the NPC website (www.npc.org).

This page is intentionally left blank.

Topic Paper

(Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure)

4-13	**European Union Cybersecurity Response to Attacks on Critical Infrastructure**
Author(s)	**Jason Haward-Grau (PAS Global, LLC)**
Reviewers	**Al Lindseth (Plains All American Pipeline)** **Doug Sauer (Phillips 66 Company)** **Wesley Malaby (Phillips 66 Company)** **Marty Willhoite (Miller Consulting Services)**
Date: October 31, 2019	**Revision:** Final

SUMMARY

The United States has not experienced direct cybersecurity attacks on industrial control system networks that have resulted in confirmed material disruption of service. However, there have been several attacks on power and utility networks in other countries such as Ukraine. These attacks have resulted in the accelerated development of European Union cybersecurity policies, which in turn have established a legal directive on cybersecurity for the protection of critical infrastructure. This topic paper addresses the relevance to the United States of attacks on European critical infrastructure and the applicability of EU cybersecurity approaches to the United States.

European Union Cybersecurity Response and Policy Actions to Attacks on Critical Infrastructure

The initial cyberattack on Ukraine's power grid in 2015 left 230,000 people without power. The cyberattack prompted the European Union to accelerate cybersecurity legislation, including implementing the legislation as a directive rather than as a 'regulation.'

- A Directive is binding legislation on all 28 member states, however, the interpretation of the law is left to the member state as is the implementation structure.
- A Regulation is an EU wide mandated law that specifies, what will be implemented, how the member states will implement the law and the requirements for EU reporting.

The Network and Information Systems Directive (commonly known as NIS-D) came into effect in May 2018 throughout the EU. The NIS-D provides an EU-level harmonized approach to cybersecurity, encompassing every EU member state. Under the NIS Directive, each EU member state is required to pass its own law regulating cybersecurity measures for any organization that offers the member state with any form of Critical Infrastructure as defined as "essential services". While most member states already have national agencies set up to facilitate cybersecurity detection and response measures, almost all have had to amend or restructure their cybersecurity frameworks in order comply with the NIS-D.

The NIS-D gave each member state until May 9, 2018 to form and pass laws that mandate cybersecurity measures applicable to all operators of "essential services" within their borders. These laws require international companies operating in EU nations to ensure compliance on a nation-by-nation basis. This will make operations much more complex, as now international companies will be required to stay up-to-date on the many member state regulations and requirements.

NIS Directive	**NERC CIP**[1]
Regulates all "essential service" providers	Regulates the "Bulk Electric System" (BES)
Requirements vary by member state	Standardized compliance requirements
Wording is ambiguous and vague	Requirements are clear and direct
Fines will vary by member state (up to 4% of Turnover)	Fines can be as high as $1 million per day

Essential Services versus Critical Infrastructure

The NIS-D references "essential services and critical infrastructure." Each of the 28 states has adopted a slightly different definition. For example, the UK Government defines Operators of

[1] The **NERC CIP** (North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.

Essential Services[2] (OES) as opposed to Critical infrastructure, as a broader group (there are approximately 50 Critical Infrastructure providers, however there are over 300 Essential services). It is helpful to understand the context of how the EU are defining the operators as follows:

(1) If a person provides an essential service of a kind referred to in paragraphs 1 to 9 of Schedule 2 and that service—

(a) relies on network and information systems; and

(b) satisfies a threshold requirement described for that kind of essential service,

that person is deemed to be designated as an OES for the subsector that is specified with respect to that essential service in that Schedule.

In other words, you rely on IT and meet a defined threshold of providing service (as defined by the nation state) you are on the hook

Critical Infrastructure is defined in the UK, as 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defense, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard3.

Affected Entities:

The NIS-D applies to any entity that provides the EU, or any citizen of a member state, with any service in the following sectors, which are defined as essential services:

- Energy (Electricity, Oil, and Gas) provision and transmission
- Transport (Air, Rail, Water, infrastructure and Road Transport)
- Banking and Financial Market Infrastructures
- Health Sector—Health care settings (including both hospitals and private clinics)
- Drinking Water Supply and Distribution

[2] See: http://www.legislation.gov.uk/uksi/2018/506/regulation/8/made

[3] See: https://www.cpni.gov.uk/critical-national-infrastructure-0

- Digital Infrastructure

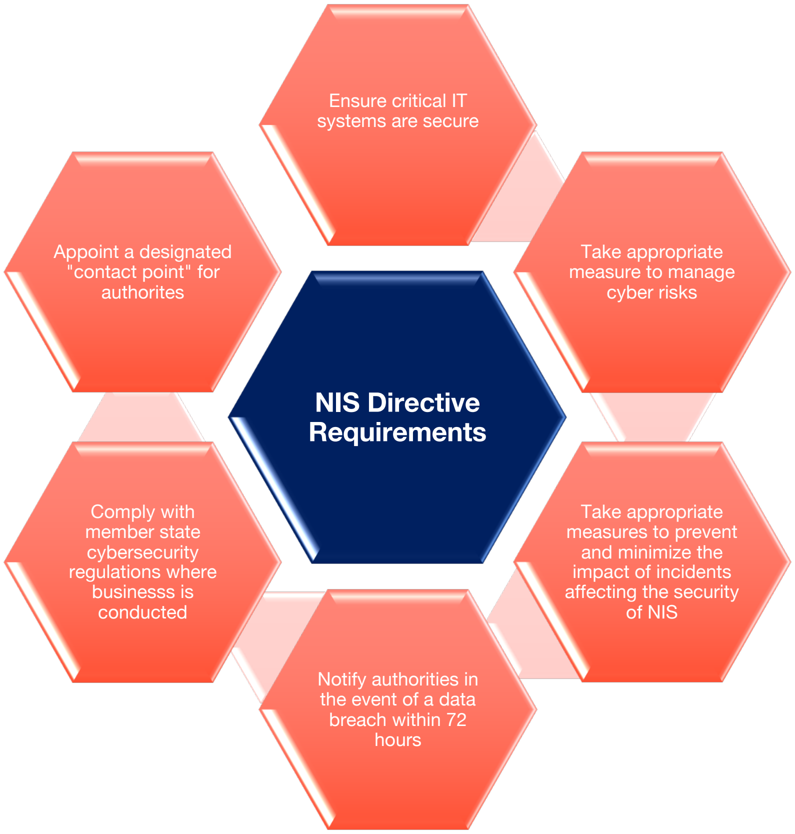
This definition of essential service providers, although fairly standardized throughout, is subject to change given a member state provides a subsequent definition within its own cybersecurity framework.

Key Components

Member states must legislatively mandate all providers of essential services to take, "appropriate and proportionate technical and organizational measures" to manage the risks posed to the security of network and information systems. Member states must also take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services[4].

Companies and other entities in the scope of the program within member states must also notify a central authority of incidents that could significantly impact the continuity of services, and public disclosure may occur at the discretion of the controlling authority when public awareness is necessary to prevent or handle an incident. Regarding a cyber-breach, notification of an incident must be made to authorities "without undue delay," normally expected to be within 24 to 72 hours after the breach is discovered. The requirement has been interpreted largely as the requirement to contact the Nation States Cyber Security reporting body, For example in the UK, this is the NCSC or National Cyber Security Centre, who will assess the incident and assist as appropriate. Whether this is then forwarded to the EU-CERT is a decision for the national entities, however, the enterprise can notify them as well, should they wish to do so. Incidents will be defined by the number of users affected, its duration, and the geographical spread of the affected area. Furthermore, the NIS-D also calls for the establishment of a cooperation network to coordinate cyber defense efforts, particularly where a cross-border issue is at stake, including sharing early warning threat intelligence between national authorities.

[4] The NIS Directive deliberately uses ambiguous language when describing measures of cybersecurity. It is intended to be a framework for members states to refer to when creating their own cybersecurity regulation. Consequently, member state legislation will likely be more specific when referring to its mandatory cybersecurity measures.


NIS Directive Requirements
Ensure critical IT systems are secure
Take appropriate measure to manage cyber risks
Take appropriate measures to prevent and minimize the impact of incidents affecting the security of NIS
Notify authorities in the event of a data breach within 72 hours
Comply with member state cybersecurity regulations where businesss is conducted
Appoint a designated "contact point" for authorites

Consequences for Noncompliance

The requirements in the NIS-D are intended to be minimal. Most countries understand the economic costs and hindrances of over-regulation. In this case, these laws are to serve as a minimum standard for organizational cybersecurity measures. However, the NIS-D does require member states to enforce penalties in the event of a data breach or any other violation of the cybersecurity regulations. These penalties are required to be "effective, proportionate, and dissuasive," meaning that, these fines have the potential to be as high as €20 million or 4% of a company's annual turnover, whichever number is greater. If a breach is serious enough, a security audit can be carried out by a competent authority; this implies that the organization is subject to the authority of the member state's designated cybersecurity agency.

The perceived success of NIS-D and its applicability in Europe has seen a number of carbon copy developments across the world from Australia (Cyber Security Strategy 2018-22) to Canada (National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure), which given the international nature of these relationships, is now providing a baseline to which in-scope entities (according to definitions of critical infrastructure and essential services) will need to adhere, requiring effective risk-based assessment of their critical infrastructure and the expectation of closer oversight by national bodies, when breaches occur.

One other point of note is that since their inception the national cyber security bodies have seen an increase in their role as responders, threat detectors and now more recently, have started to shift towards more offensive operations. This trend is demonstrating a willingness across the EU for these bodies to collaborate on cross boarder activities and operate with the larger goal of disrupting international threat actors and nation states.