To: Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 2089
Dear Diane, I am sending my comments (in the previous email I have copied only small part of it)

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

There are many aspects that can be categorized as a challenges:

a) lack of knowledge regarding the cyberthreats

b) legacy systems with little or no choice for updates

c) no standardized approach to identify and address cyber risks

d) lack of proper separation between business and production networks

e) inmature environment in terms of malicious code identification (no AntiVirus, IPS/IDS on the production network)

f) lack of clear an formal definition of roles and responsibilities of IT and production departments especially when it comes to “border” equipment

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Each sector may vary in terms of environment and system being in use (main systems as well as supporting systems). Differences between sectors can a major problem whe trying to establish one consistent framework. It should be considered to add a subsections for specifically for particular sector.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

Up to date risk related to critical infrastructure were usually related to “operational/ maintenance / performance ” problems. For this kind of risk there are specific standard and procedures in place. In terms of cybersecurity

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Where Enterprise Risk Management is implemented, usually companies are adding one high level threat related to cyberthreat (e.g. cyberattack on critical infrastructure).

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

Please find below the list of standards/guidelines that should be taken into consideration:

> Instruments, Systems and Automation Society

> ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

> ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems

> ANSI/ISA–99.02.01–2009, Security for Industrial Automation and Control Systems: Establishing
an Industrial Automation and Control Systems Security Program

> Draft - ISA-99.03.03 - Security for industrial automation and control systems- System security requirements and security assurance levels

> IEC/PAS 62443-3 – Security for industrial process measurement and control - Network and system security

> North American Electrical Reliability Corporation - Critical Infrastructure Protection

> NERC-CIP

> American Petroleum Institute

> API-1164 – pipeline SCADA security

> API-1165 - Recommended Practice for Pipeline SCADA Displays

> API-1167 - Alarm Management

> American Gas Association

> AGA-12 - SCADA encryption

> International Organization for Standardization / International Electrotechnical Commission

> ISO/IEC 27001 / 27002

The above mentioned list covers many if not all important aspects of security, however there are different in terms of level of details and usually focus on requirements not how to achieve the desired “to be state”.

In terms of developed framework I think it should be taken consideration that implementation of only basic and very simple security mechanisms may eliminate 80% of cyberthreats. Therefore it may a good idea use “levels of protection”:

a) basic - all critical infrastructure operators should be compliant with and it should be enough to protect them from “amateur / hobbyist” hackers.

b) Medium – security mechanisms that are more complex, expensive etc.and therefore suggested for more

c) High – with “nice to have”s recommended for the most mature CI operators

The framework should also include step by step approach hot to establish adequate Organization structure and program focused on improving cybersecurity.

In addition it has to be taken to consideration that every single CI operator will change their system/environment eventually and when they will create requirements for new systems, also cybersecurity should be included.

Kind regards,
Piotr Ciepiela

Piotr Ciepiela | Manager
Ernst & Young Business Advisory
Rondo ONZ 1, 00-124 Warszawa, Poland
Office: +48 22 557 8761 | Mobile: +48 519 511 603 | Piotr.Ciepiela@pl.ey.com
Fax: +48 22 557 70 01
Website: www.ey.com/pl
Assistant: Monika Uhma | Phone: +48 22 557 6263 | Monika.Uhma@pl.ey.com