# Study on Cybersecurity in the Energy Community

Blueprint Energy Solutions GmbH
Elena Boskov-Kovacs, Peter Grasselli, Szabolcs Hallai

Vienna, 17.09.2019.

# Agenda

1. Introduction
2. Preliminary findings from Intermediary Report: gap analysis, threat assessment, next steps
3. Roundtable discussion, comments and proposals from the representatives

# Welcome to the

# 2ND WORKSHOP – CYBERSECURITY RISKS AND ASSESSMENT

**Cybersecurity Study – Workshop #2 (10:00 – 12:00)**

**10:00 – 10:15** Welcoming of attendees ECS, Consultants
**10:15 – 11:30** Study on Cybersecurity in the Energy Community – Intermediary Report
- Presentation of the findings in the Report, gap analysis, threat assessment, next steps (ECS, Elena Boskov-Kovacs, Peter Grasselli)
- Roundtable discussion, comments and proposals from the representatives
- Q & A

**11:30 – 12:15** Presentation on the latest development in EU and new cybersecurity trends in energy (dr. Ferenc Suba)
- Q & A

**Coffee break (12:15 – 12:30)**

**12:30 – 14:00** Workshop "Criteria for identification of large-scale cybersecurity incidents"
- Q & A (Peter Grasselli, Szabolcs Hallai)

**Lunch break (14:00 – 14:30)**

**14:30 – 16:00** Workshop "Designing the action plans for EnC Contracting Parties" (Peter Grasselli, Szabolcs Hallai)
- Q & A

**16:00 – 16:30** Closing Remarks ECS

BLUEPRINT energy SOLUTIONS

# Study project of Energy Community

Study on Cybersecurity in energy

- Objectives:
  - Identify and assess key weaknesses, risks and exposure to cyber threats in the energy systems
  - Identify the existing regulatory framework and regulatory gaps for cybersecurity governance
  - Identify the relevant provisions of the NIS Directive and the Directive on European critical infrastructure and provide an impact assessment of their implementation in the Energy Community
  - Propose the necessary measures to improve cybersecurity in Contracting Parties (national level)
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents as well as a common cooperation platform, common certification framework and common framework for research, education and training programmes
  - Explore the possibility for the participation of Contracting Parties in the work of the European Union Agency for Network and Information Security (ENISA).

# Study project of Energy Community

On the basis of Procedural Act 2018/2/MC-EnC: on the Establishment of an Energy Community **Coordination Group for Cyber-Security and Critical Infrastructure**, created among other to promote a high level of security of network and information systems and of critical infrastructures within the Energy Community, a coordination group for cyber-security and critical infrastructure was set up.

1st Cybersecurity Day in the Energy Community - gathering representatives from Ministries, regulatory bodies and system operators from Albania, BiH, North Macedonia, Georgia, Kosovo*, Moldova, Montenegro, Serbia and Ukraine

# Engagement and ongoing activities

| Task | Activity | Activity | Month / Date | 1 January | 2 February | 3 March | 4 April | 5 May | 6 June | 7 July | 8 August | 9 September | 10 October |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Bi monthly reports | | | | | | | | | | | |
| T0 | | Inception report | | | | | | | | | | | |
| T1 | 1.1 | Overview of legal, regulatory and institutional cybersecurity frameworks | | | | | | | | | | | |
| T1 | 1.2 | Questionnaire development | | | | | | | | | | | |
| T1 | 1.3 | Workshop1: Identification of relevant stakeholders and questionnaire presentation | | | | | | | | | | | |
| T1 | 1.4 | Questionnaire delivery and collection | | | | | | | | | | | |
| T1 | 1.5 | Questionnaire | | | | | | | | | | | |
| T1 | 1.6 | Field activity (Contracting Parties) | | | | | | | | | | | |
| T1 | 1.7 | Threat identification and risk assessment | | | | | | | | | | | |
| T1 | 1.8 | Workshop2 – Cyber-risks workshop | | | | | | | | | | | |
| T1 | 1.9 | First interim report | | | | | | | | | | | |
| T2 | 2.1 | GAP assessment | | | | | | | | | | | |
| T2 | 2.2 | Second interim report | | | | | | | | | | | |
| T3 | 3.1 | Propose recommendations | | | | | | | | | | | |
| T3 | 3.2 | Workshop3 - Make an impact assessment of implementation of proposed measures and acts in the Energy Community Contracting Parties and in the Energy Community | | | | | | | | | | | |
| T3 | 3.3 | Relevant information for impact assesment collection (for W3 survey) | | | | | | | | | | | |
| T3 | 3.4 | Information for impact assesment analysis (for W3 survey) | | | | | | | | | | | |
| T3 | 3.5 | Final report | | | | | | | | | | | |
| T3 | 3.6 | Workshop4 - Final meeting | | | | | | | | | | | |

We are here

**September 2019:**
**Interim report finalized;**
**preparing recommendations**

Reports (Inception, Interim, Finl, Bi Mothly)
Project activity
Field activity

# Intermediary Report

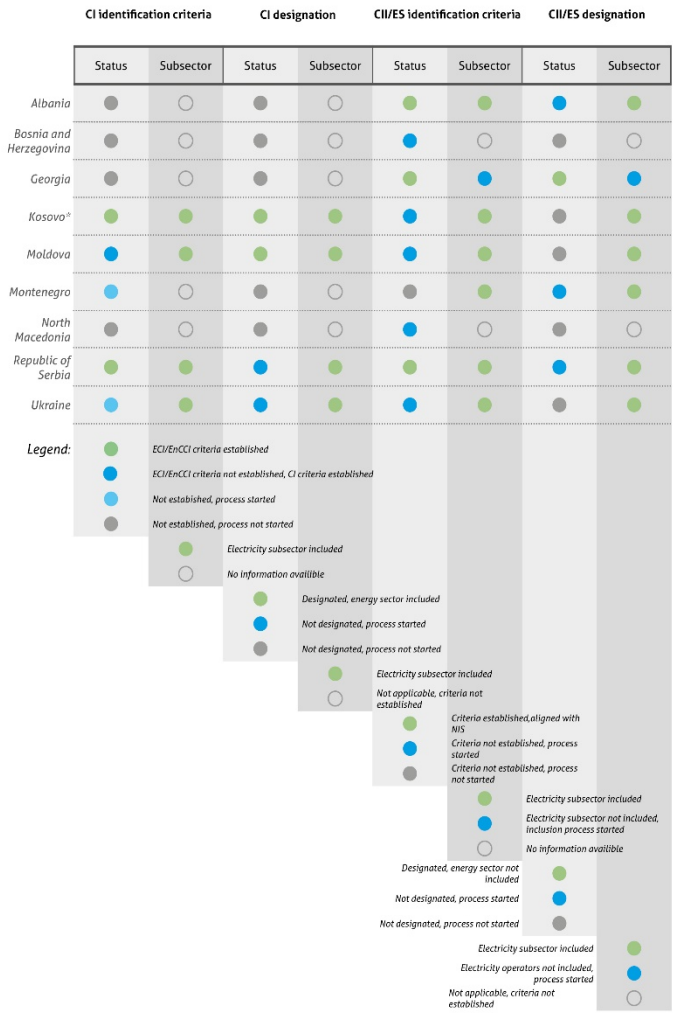
- Interim report is based on the information collection from CPs and risk assessment
- It provides overviews of EU rules and standards, legal, institutional and standards frameworks in CPs, cross-border cybersecurity initiatives and mechanisms and multilateral or bilateral cybersecurity governance projects/technical assistance, education and training programs related to the cybersecurity and cyber threats and risks to which the energy sector in the Energy Community can be exposed.
- Preliminary findings provide the current state of play in CPs regarding cybersecurity aspects of critical infrastructure analysing the current legislative framework in each CP and evaluate the degree to which national legislation is aligned with EU legislation.
- Report also includes overview of energy sector cyber security threats and risks from two angles: first through the perspective of energy sector stakeholders and second, as assessed by CPs in national security or cybersecurity strategies and assessments.

# Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties

While the criteria for identification of ECI/EnCCI are present in the national legislation only in two CPs, situation is much better with the criteria for identification of essential services which are already established or in preparation in more than half of CPs.

Situation related to the identification of CI is very similar in the electricity and gas subsectors of the energy sector, the only difference being that CII/ES designation criteria in Albania does not include gas subsector

Electricity ->




| Abbreviation | Meaning |
|---|---|
| CI | Critical Infrastructure |
| CII | Critical Information Infrastructure |
| ECI | European Critical Infrastructures |
| EnCCI | Energy Community Critical Infrastructure |

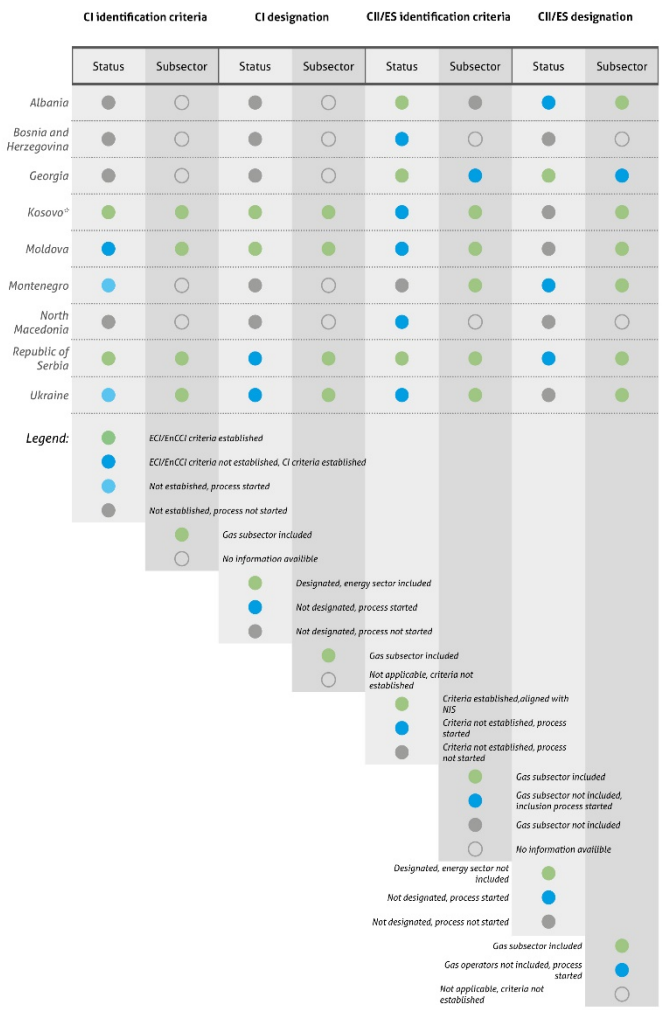
BLUEPRINT energy SOLUTIONS

# Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties

While the criteria for identification of ECI/EnCCI are present in the national legislation only in two CPs, situation is much better with the criteria for identification of essential services which are already established or in preparation in more than half of CPs.

Situation related to the identification of CI is very similar in the electricity and gas subsectors of the energy sector, the only difference being that CII/ES designation criteria in Albania does not include gas subsector

Gas ->



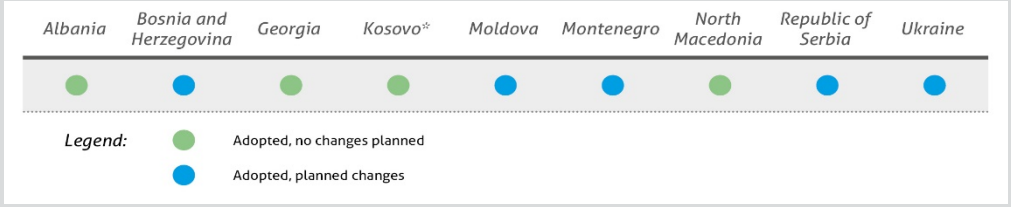

| Abbreviation | Meaning |
|---|---|
| CI | Critical Infrastructure |
| CII | Critical Information Infrastructure |
| ECI | European Critical Infrastructures |
| EnCCI | Energy Community Critical Infrastructure |

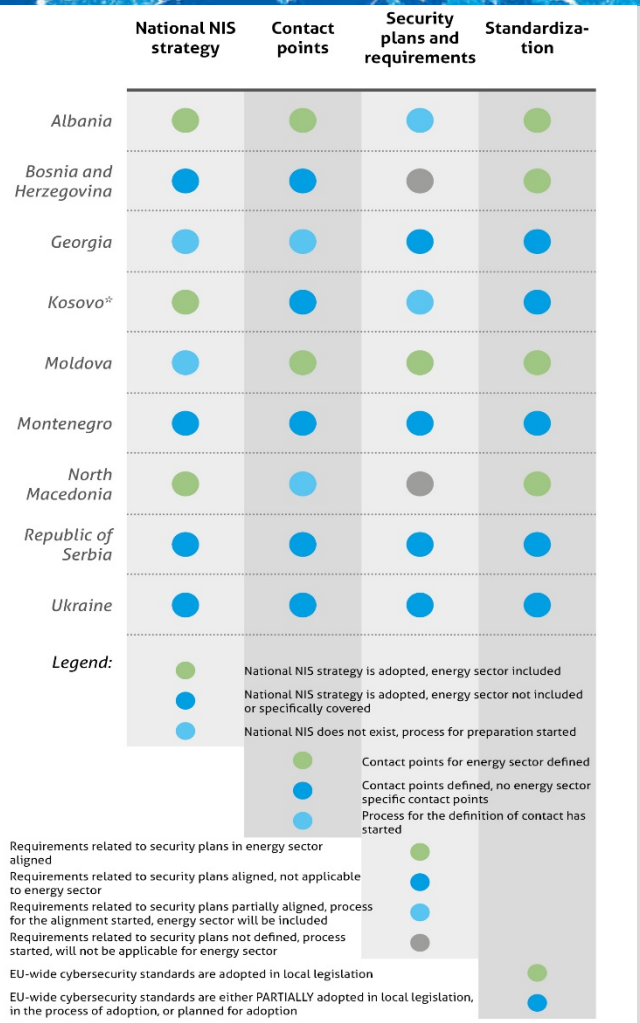
BLUEPRINT energy SOLUTIONS

# Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties

Legal and institutional cybersecurity framework presents an overview of the current situation in each of the CPs of the Energy Community, regarding the existing cybersecurity and strategy processes that are in place or expected to happen in the short term.

Planned amendments of cybercrime legislation give an overview and assessment of on-going or planned activities related to transposition of EU wide cybercrime legislation in the national legislative framework.




BLUEPRINT energy SOLUTIONS

# Overview of cyber threats and risks for EnC members


- The energy sector cybersecurity threat landscape changes in 2019 for EnC member states made significant shift in focus towards critical infrastructure protection.

- The possibilities of domino/cascading effect (cross-sectorial and cross-national as well) during cybersecurity incidents are in rise as legacy systems are overlapped with new technology (smart grid, virtual power plant etc.). The source of those developments was a shift in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors hence a significant rise of cyberwarfare in energy as a threat.

- Based on the detailed risk assessment two categories of high risks were identified, which are very important to be taken into consideration for the EnC member stakeholders:

  - **IT and OT systemic/inherent risks** which are causing the most danger as they are undermining the security of supplies. These risks are often coming as a results of poor decisions in the past and must be addressed daily to correct them by operational controls.
  - **Organisational risks** which are originating from lack of standardized and functional operational controls in the energy sectors of EnC members. The operational controls[3] are supposed to eliminate IT and OT systemic/inherent risks or at least lighten them to acceptable levels. From the standpoint of EU these risks in EnC member states are often seen as compliance risks.

# Overview of cyber threats and risks for EnC members


- Cyber Threats

| Cyber Threat | | | | | | | |
|---|---|---|---|---|---|---|---|
| Malware | Web Based Attacks/Web application attacks | Social engeneering/Phising/ Spam | Denial of Service (DoS) | Insider Threat | Cyber Espionage Cyberwarfare | Ransomware | Botnet |
| MEDIUM RISK for CA/NRA | NOT APPLICABLE for CA NRA | HIGH RISK for CA/NRA | HIGH RISK for CA/NRA | HIGH RISK for CA/NRA | CRITICAL RISK for CA/NRA | MEDIUM RISK for CA/NRA | MEDIUM RISK for CA/NRA |
| LOW RISK in cascading effect to other energy stakeholder | | MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder |
| HIGH RISK for TSO | MEDIUM RISK for TSO | HIGH RISK for TSO | LOW RISK for TSO | HIGH RISK for TSO | HIGH RISK for TSO | HIGH RISK for TSO | HIGH RISK for TSO |
| MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder |
| MEDIUM RISK for DSO | MEDIUM RISK for DSO | HIGH RISK for DSO | LOW RISK for DSO | MEDIUM RISK for DSO | HIGH RISK for DSO | HIGH RISK for DSO | HIGH RISK for DSO |
| MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder | HIGH RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder |
| LOW RISK for Generation | LOW RISK for Generation | MEDIUM RISK for Generation | LOW RISK for Generation | MEDIUM RISK for Generation | MEDIUM RISK for Generation | HIGH RISK for Generation | MEDIUM RISK for Generation |
| MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder | MEDIUM RISK in cascading effect to other energy stakeholder |
| LOW RISK for Exchange | LOW RISK for Exchange | LOW RISK for Exchange | LOW RISK for Exchange | LOW RISK for Exchange | LOW RISK for Exchange | MEDIUM RISK for Exchange | LOW RISK for Exchange |
| LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder | LOW RISK in cascading effect to other energy stakeholder |

# Overview of cyber threats and risks for EnC members


- Examples

## Stakeholder: Country cybersecurity authority (CA) and/or National Regulatory Agency (NRA)

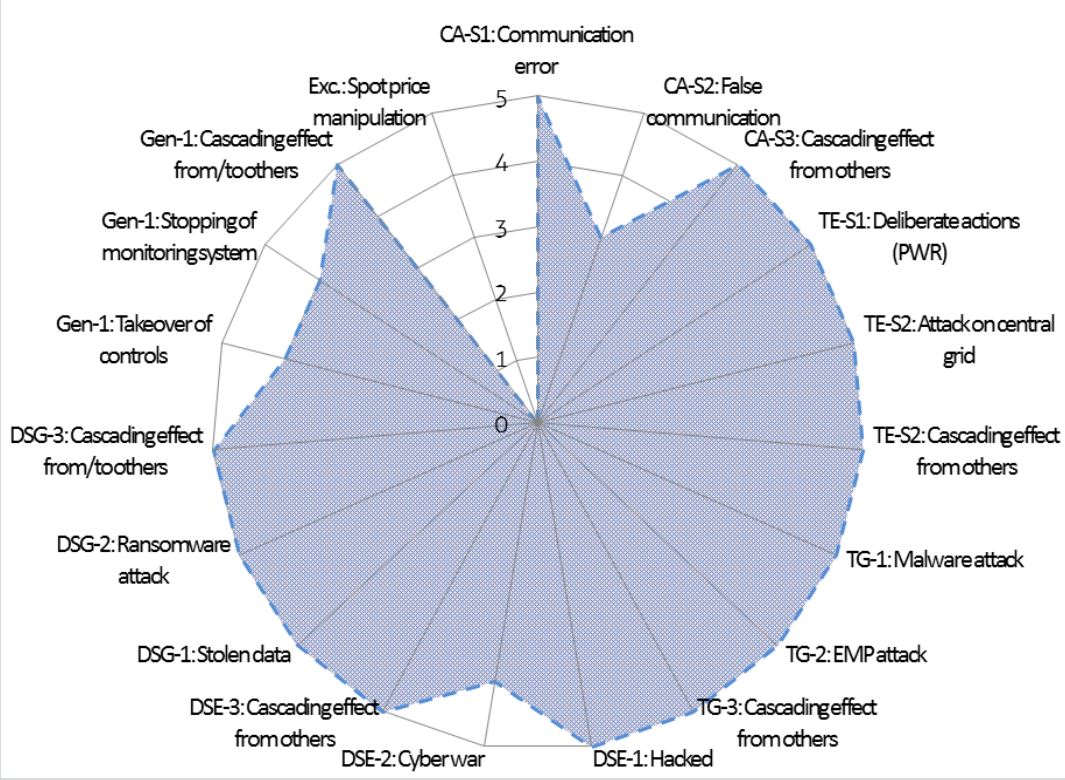
| **Scenario A – False communication** | | | | | **CA/NRA** |
|---|---|---|---|---|---|
| **Due to a spoofed false email to the CA it declared state of emergency which force the energy sector companies to work in critical conditions. A 24 hours a day shift was introduced at gas TSO critical supervisory operation control room unit. The reporting requirement was upgraded to once a minute. A government held a special meeting to discuss the cyberattack from which they release a special note to address the public. As the CA realises that there was a spoofed e-mail with false information, they try to stop the operation but it is too late as the information leak to public.** | | | | | |
| | | | Quantified Impact on Energy Sector | | |
| **Threat** | Vulnerability | Likelihood | Health / Safety | Economic | Social |
| **Phishing** | Lack of security awareness<br>Lack of proof of sending or receiving a message<br>Unprotected sensitive traffic<br>Lack of e-mail usage policy | Probably | 1 | 2 | 2 |

## Stakeholder: Country Transmission System Operators (TSO) Electricity

| **Scenario B - Cascading effect from others** | | | | | |
|---|---|---|---|---|---|
| **There is a lack of communication (an early warning monitoring system) with other countries TSOs. The TSO also do not inform ENTSO-E about the incident. An attack vector is not stopped by eliminating the attacker which was recognized by others (as they tried also to attack other countries TSOs). The TSO was an object of an attack type which was used before. This is also applicable for NRA-NRA and CA-CA interconnections as well as cross-sectorial.** | | | | | |
| | | | Quantified Impact on Energy Sector | | |
| **Threat** | Vulnerability | Likelihood | Health / Safety | Economic | Social |
| **Cyberwarfare** | Lack of procedures of risk identification and assessment<br>Lack of monitoring mechanisms | Possibly | 3 | 4 | 5 |

# Overview of cyber threats and risks for EnC members


- The risks were assessed based on the prioritisation of likelihood and impact quantified of scenarios
- If we broke down the risks with the type of cyber threat vectors to impact different stakeholders we can get a more precise picture of inherent risks



# The Next Steps

- Activities and organisational structures proposed to align the existing Contracting Parties energy cybersecurity framework with the EU legislation with proposed measures
- Recommendations per each CP
- Impact assessment of implementation of proposed measures and acts in the Energy Community Contracting Parties and in the Energy Community
- Proposed roadmap and timing for the implementation

# Questions?

BLUEPRINT energy SOLUTIONS