Ref: 13GIE149
October 2013

GIE position paper regarding the proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union from 7 February 2013

1. Who is GIE?

Gas Infrastructure Europe (GIE) is an association representing the sole interest of the infrastructure industry in the natural gas business such as Transmission System Operators, Storage System Operators and LNG Terminal Operators. GIE has currently 69 members in 25 European countries.

One of the objectives of GIE is to voice the views of its members vis-à-vis the European policy makers. Its mission is to actively contribute to the construction of a single, sustainable and competitive gas market in Europe.

2. GIE general comment

GIE welcomes that there is an initiative in place to define a common European Cyber security strategy.

GIE recognizes that nowadays major threats regarding security arise from cyber space and increased joined efforts for protection need to be taken.

Members of GIE have taken all relevant measures to improve security- assessing the risk, implementing management systems and technical solutions. Ensuring the gas supply at all times has been the main driver behind this.

3. GIE specific comments

3.1 Information sharing

Substantial improvements can only be achieved with increased information sharing that in the GIE point of view is the key factor.

- Critical Infrastructure Operators need an early warning system.
- Reporting of incidents should be vice versa. Operators need to get information on threats and incidents occurred from the authorities. The competent national authorities shall be obliged to inform critical infrastructures operators on relevant threats and incidents occurred.
- Information sharing (threats and incidents) between the named parties needs to stay confidential and shall not be shared with the public domain.

3.2 Private Public Partnership

GIE is supporting the concept of increased public- private partnership in this field but

- Currently the numbers of actors on the public side is too large- clear leadership, roles and responsibilities are needed on national and EU-level. The Critical Infrastructure Operators need in the EU region a formal one focal point for this subject.
- One coordinating national public organization for all cyber security topics would be desirable.

3.3 Standardization

GIE supports the idea of having minimum NIS (network and information) standards in all European countries instead of legally binding instruments (as stated in the GIE position paper regarding the revision and future of the European Programme for Critical Infrastructure Protection (EPCIP) from September 2012).

- Minimum security requirements should be defined by the sectors and supported by the national authorities. Security requirements should be based on the results of a sector specific risk assessment. The main driver to implement increased security measures is the business continuity.

3.4 Market Operators- Suppliers

GIE acknowledges the role of being market operator in this directive. For the gas sectors specifically protecting SCADA is vital for continuous operations. GIE proposes to come up proactively and provide authorities with minimum security requirements to protect SCADA.

- Critical infrastructure operators such as gas transmission companies are highly dependent on their IT suppliers such as network or SCADA suppliers – they are not covered in the current draft of the directive; they also need to be included in the directive.

3.5 Costs of implementation

Security requirements should be economically sustainable. In any case though cost that arises from implementing measures to increase the protection need to be included in the tariffs.