EDSO for smart grids view's on the proposed directive concerning measures to ensure a high common level of network and information security across the Union

Cyber-security is a major challenge for electricity distribution system operators (DSOs), the regulated companies in charge of a distributing electricity to every European citizen. Although electricity grids have expanded during the last century, they have not evolved dramatically from a technical point of view. However, the increasing amount of electricity from intermittent renewable energy sources has made grid innovation an absolute requirement. The further development of grid automation and the use of communication technologies are the most cost-efficient answer to the new requirements placed on the electricity networks.

The growing use of advanced information technologies combined with electricity grids open up new opportunities for DSOs but makes the need for cyber-security even more acute.

The draft directive on network and information security (NIS) presented in February 2013 is the first step towards raising awareness about information security and coordinating the exchange of knowledge and best practices between companies in charge of critical infrastructures: public authorities, utilities companies and other stakeholders.

We welcome a number of amendments presented by Mr. Andras Schwab in his draft report, but we would like to invite Members of the European Parliament to take into account some additional questions when preparing their amendments or opinions.

- **Standardisation should be based on international compromise (article 16.2)**

Standardisation is a key issue for distribution system operators, and for the electricity sector in general. To guarantee the security of critical infrastructure, internationally recognised communications standards should be agreed and deployed. However, the approach chosen by the European Commission – directly establishing a list of standards - goes against proven current practices where each sector has created its own standardisation bodies.

In the electricity sector, all stakeholders gather at the International Electrotechnical Commission (IEC), created in 1906, where the definition of standards follow a strict drafting and validation process to ensure that eventually approved standards are accepted by all. In the European Union, the standardisation bodies CEN-CENELEC-ETSI also collaborate actively to develop standards and follow a stringent validation process. Letting an external party chose the standards to be used by industry may lead to investments in costly solutions which do not match current and future technical need and might limit innovation.

If a standard is good and adapted to the needs of several companies, it has every chance of spreading without requiring any direct intervention from public authorities.

- **Incident reports should only be compulsory for critical events (articles 3, 8, 14)**

Large companies employing several thousands of people are subject to a number of regular small-scale incidents, which have no effect on their core activities. The reporting scheme sketched in this draft directive does not differentiate between major incidents related to key infrastructure and day-to-day mundane incidents. The directive should be more specific to avoid overburdening companies with an unnecessary reporting process. We recommend only making the incident report compulsory for incidents affecting critical infrastructure or the services provided through this critical infrastructure.

- **The use of delegated and implementing acts should be further defined to avoid legal uncertainty (article 14)**

In the proposed directive, the European Commission is entitled to adopt delegated acts related to: the criteria to be part of the cooperation network, the criteria to trigger early warnings and the content of the incident reports. If fixing technical issues through delegated acts appears as the appropriate way not to overburden the European Institutions with unnecessary new legislative processes, the original text is too vague and creates uncertainty for all the stakeholders working together in the cooperation network.

- **Incident report confidentiality should be guaranteed (article 9)**

Fixing security breaches requires the exchange of knowledge between companies and public authorities. However, the draft directive does not explain how the national competent authority will handle the information received on incidents, and how this information will be shared with other companies and authorities.
To build up trust between all the companies involved in the reporting process and avoid an excessive dissemination of sensitive information, the incident reports should remain confidential.

- **Companies should have the possibility to perform their own security audits (article 15)**

Regular security audits are essential to make sure that critical installations are able to cope with attacks. In the European Commission's proposal, if the competent authority orders a security audit, it can only be performed by either the authority itself or external auditors. Due to the extreme sensitivity of critical infrastructures, in terms of full running/operational networks and devices impacting the national security, and taking into account the high rate of data protection of member states, Internal audit should also be considered as a valid method for testing information network security, as it will reduce audit costs. To keep the article balanced, the competent authority may have the possibility to ask for an additional audit performed by a third-party, if deemed necessary, based on the outputs and results coming from internal audits, in a full collaborative framework and guaranteeing the confidentiality of the provided information.