Energy: cyber security is crucial for protection against threats for smart grids which are key for energy availability claims EU cyber security Agency in new report.

The EU's cyber security agency ENISA signals that assessing the threats for smart grids is crucial for their protection and is therefore a key element in ensuring energy availability.

Smart grids are complex "systems of systems," storing, transporting and managing energy from production to consumers. A smart grid is de facto Critical Infrastructure as energy is crucial for society and for the well-functioning of the economy. By combining energy and information infrastructures, smart grids are critical infrastructures and should operate securely by respecting end users' privacy.

The Executive Director of ENISA, Professor Udo Helmbrecht, commented, "*An understanding of the cyber-threat landscape is indispensable for identifying which protection measures are necessary for smart grids. This report is the response to the urgent question of energy providers and stakeholders: It provides the tools to assess risk exposure of smart grid assets. In cyber security, we need common efforts and coordination to reduce impact.*"

This report provides a threat landscape affecting smart grid components. It takes stock of available cyber security and protection approaches as well as good practices in the field. The study also lists internal threats affecting IT smart grid assets, including a variety of threats emanating from errors and insider attacks.

Key conclusions: Some key conclusions identified are:

- *Consider external and internal threats*: in cyber security, external cyber threats constitute the main source of external exposure. This cyber threat environment originates from threat agents, utilising cyber threats and launching cyber attacks.
- *Decompose and classify smart grid elements being exposed to threats*: from electrical assets like cables, switches, routers, sensors and information to software such as operating systems, services, hardware, infrastructure, and the persons operating the systems.
- *Use available knowledge*: reuse existing good practices after defining the level of desired protection.
- *List the **specific smart grids cyber threats**, for example:*

- *Eavesdropping/interception/hijacking: e.g. information leaking, electro-magnetic/radio frequency interception, sniffer attacks, failures of devices and systems, attacks, and physical attacks,*
  *and the **threat agents,** such as corporations, cybercriminals, employees, hacktivists, nation states, natural disasters, terrorists, the new element of cyber fighters*
- *Assess vulnerabilities and risks in smart grids.*
- *Assessments to be done by asset owners*: Finally, the Agency concludes that the threat exposure and risk assessment of a smart grid can only be done by the asset owner, who masters the complexity and interdependencies of the related smart grid infrastructure.

For full report

Background: ENISA reports on Smart grids (December 2012); 10 recommendations (July 2012)
The EU Cyber Security Strategy, the proposal for a EU Cyber Security Directive

For interviews: Ulf Bergström, Spokesman, ulf.bergstrom@enisa.europa.eu, mobile: + 30 6948 460 143, Dr. Louis Marinos, ENISA Expert, resilience@enisa.europa.eu