Understanding the Facts: Edison Electric Institute's Positions on Radio Frequency, Cyber Security and Data Privacy

The Edison Electric Institute (EEI) has developed industry guidelines for the communications on the topics of Data Privacy, Cyber Security and Radio Frequency. Pepco and Delmarva Power are members of EEI and support these positions.

Does the radio frequency (RF) signal produced from smart meters cause any health effects?

No.

Some smart meters use technologies that transmit RF to enable communication between electric companies and their customers. While concerns have been raised about the potential impact of the RF generated by these smart meters, numerous studies have shown that smart meters using RF technologies pose no health risk.

A smart meter with RF technology uses a low-power radio to communicate the electricity usage of a home or business to the electric company through remote communication technologies. RF exposure from a smart meter is far below—and more infrequent—than other common electric devices, including cell phones, baby monitors, and microwave ovens.

As with any electric device that utilizes RF, smart meters have been monitored, tested, and certified to ensure they meet certain safety standards. The RF exposure levels from smart meters are far below the levels permitted by the Federal Communications Commission (FCC), which sets health standards for RF exposure, based on extensive reviews of the biological and health literature. The U.S. standards for radio waves are similar to those of the European Union and Canada.

According to research by the Electric Power Research Institute, the "relatively weak" strength of the RF signals generated by smart meters means that any impact of RF exposure would be minimal—similar to the levels of the exposure from televisions and radios.[1]

What's more, RF exposure depends partly on the proximity of the RF source to a person. Smart meters usually are located on the outside of your house in a metal box, away from your daily routine activity. The electric panel and wall behind the meter actually block much of the radio signal. Due to the extremely brief exposure to the radio waves that smart meters produce, there have been no long-term health effects identified as a result of the installation of smart meters, according to a study conducted by the California Council on Science and Technology.[2]

For more information on this topic visit www.eei.org or click here.

[1] Electric Power Research Institute, "An Investigation of Radio Frequency Fields Associated with the Itron Smart Meter,"December 2010."

[2] California Council on Science and Technology, "Health Impacts of Radio Frequency Exposure from Smart Meters," March 31, 2011.

Understanding the Facts: Edison Electric Institute's Positions on Radio Frequency, Cyber Security and Data Privacy

Do smart meters emit radio frequency (RF) signals continuously throughout the day?

No.

The actual percent of time the smart meter is transmitting, especially in the initial years of operation, is very small, usually less than 1% which is equivalent to an average of less than 60 seconds cumulatively throughout the day. Smart meter communications are typically less than a second and under normal operations, take place every 4-6 hours. For more information visit EEI's website at www.eei.org or click here for more details.

How do electric companies protect the privacy of customers' data?

America's electric companies work hard to protect the privacy of their customers' data—and have always done so. In fact, protecting the security of the grid and the privacy of customer data is a key component to the grid modernization effort. Electric companies use advanced encryption technologies to protect the privacy of the data transmitted by smart meters. Electric companies also comply with the data privacy guidelines and regulations set by state public utility commissions.

Since protecting customer data is a top priority in modernizing the grid, electric companies are working with federal agencies, such as the Department of Homeland Security, the Department of Energy, and the National Institute of Standards and Technology (NIST) to adapt existing privacy and security standards to meet the new data requirements that accompany smart grid technology. NIST guidelines are being applied to remote access, authentication, encryption, and the privacy of metered data and customer information.

In addition, before an electric company can implement a smart meter program, it must submit to its state regulatory commission detailed plans that describe how the data security systems will protect customer data. State regulators closely monitor the privacy safeguards that are being developed for the new smart grid technology systems.

For more information on this topic visit www.eei.org or click here.

Protecting the grid from cyber attacks requires a coordinated effort among electric companies, the federal government, and the suppliers of critical electric grid systems and components. Electric companies work closely with the North American Electric Reliability Corporation (NERC) and federal agencies to enhance the cyber security of the bulk power system. This includes coordination with the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE), as well as receiving assistance from federal intelligence and law enforcement agencies. The following are EEI principles for cyber security and critical infrastructure protection:

Protecting the Grid is a Shared Responsibility

1. **Prioritize Assets to Ensure Effective Protection**
   Recognizing that there are a variety of interdependencies, and potential consequences associated with the loss of different facilities, the utility industry supports a risk-based, prioritized approach that identifies assets

truly critical to the reliable operation of the electric grid. This ensures the most important elements of our system receive the highest level of attention, as well as the resources necessary to secure them.

2. **Threats Require Emergency Action; Vulnerabilities Should Be Addressed More Deliberately**
   In this context, a threat is imminent and requires a rapid response. In these instances, the industry is willing to accommodate certain operational consequences in the interest of addressing the threat. Vulnerabilities, on the other hand, have a longer time horizon and can benefit from a more measured response. Government authority should reflect and respect these different levels of danger.

3. **Clear Regulatory Structure and Open Lines of Communication**
   The Federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a crisis. It is critical that the federal government and industry communicate with each other seamlessly; to avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action.

4. **Proactively Manage New Risks**
   As the new Smart Grid develops, it is essential that cyber security protections are incorporated into both the grid architecture and the new smart grid technologies. The electric power industry must continue to work closely with vendors, manufacturers, and government agencies and be aligned with emerging and evolving cyber security standards (such as those being driven by NIST) to ensure that the new technology running the grid is, most importantly, secure and reliable. We encourage the development of a security certification program that would independently test smart grid components and systems and certify that they pass security tests. This certification process would help utilities select only those systems that provide appropriate cyber security.

5. **Committed to Protecting Bulk Electric System and Distribution Assets**
   The utility industry understands that cyber attacks affecting distribution systems could have broader implications. Since jurisdiction is split between state regulators and the Federal Energy Regulatory Commission, the utility industry supports enhanced threat information coordination and communication between regulatory agencies and utilities to protect our systems (whether distribution or the bulk electric system) while also honoring the existing regulatory model.

6. **Cost Recovery and Liability Protection**
   Costs associated with emergency mitigation are, by definition, unexpected and thus not included in a utility's rate base. To ensure emergency actions do not put undue financial strain on electric utilities, the industry supports mechanisms for recovering costs. In addition, electric utilities support liability protections for actions taken under an emergency order.

For more information on this topic visit www.eei.org or click here.