

June 10, 2010

VIA Certified Mail

Alexander Morris
FOIA Officer
United States Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585
(202) 586-5955

Dear Mr. Morris:

This letter constitutes a request to the Department of Energy ("DOE") under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks agency records in possession of DOE concerning the cybersecurity plans submitted by applicants to the DOE's Smart Grid Investment Grant Program ("SGIG").

Background

Originally authorized by Section 1306 of the Energy Independence and Security Act of 2007¹ and then modified by the American Recovery and Reinvestment Act of 2009,² SGIG is a DOE program intended to accelerate the country's transition to a modern electric transmission and distribution system by promoting investment in smart grid technology.³ SGIG seeks to accomplish this goal through competitive grants whereby the DOE will provide up to 50% of the cost for new projects implementing the smart grid.⁴ These grants range in size from a minimum of \$300,000 to as much as \$200 million.⁵

In June 2009, the DOE issued its initial announcement opening up the SGIG application process. As part of this process, DOE required applicants to submit a Project Plan describing how the project would address cybersecurity concerns.⁶ The plans needed to include summaries of:

¹ Pub. L. No. 110-140, 121 Stat. 1492.

² Pub. L. No. 111-5, § 405(5)–(8), 123 Stat. 115.

³ Office of Elec. Delivery and Energy Reliability, Dep't of Energy, No. DE-FOA-0000058, *Smart Grid Investment Grant Program Funding Opportunity Announcement* 7 (2009), available at http://www.wired.com/images_blogs/threatlevel/2009/10/proposal-requirements-for-smart-grid-grants.pdf.

⁴ *Id.*

⁵ *Id.* at 12.

⁶ *Id.* at 19.

- The cybersecurity risks of the project and how such risks would be mitigated throughout the project lifecycle
- The cybersecurity criteria utilized for vendor and device selection
- The relevant cybersecurity standards and best practices that the applicant intended to follow
- How the project would adapt to new cybersecurity standards that may emerge⁷

A DOE spokesperson has asserted that the plans were subsequently reviewed by two cybersecurity experts, however neither the names of the experts nor details of the plans themselves have been released to the public.⁸ In October 2009, President Obama announced that 100 winning applicants would receive a total of \$3.4 billion in SGIG funding.⁹

EPIC has called attention to the privacy risks posed by the smart grid and smart meters on numerous occasions, including in formal comments filed with the National Institute of Standards and Technology and the California Public Utility Commission.¹⁰ EPIC also maintains a website dedicated to the privacy issues surrounding the smart grid.¹¹ Smart meters have the capability to monitor and report on customer electricity consumption in near real-time.¹² Such monitoring might reveal sensitive personal behavior patterns. For example, smart meter data could distinguish between when the consumer is engaged in housework or personal hygiene. Similarly, it might reveal that a consumer has a serious medical condition that requires use of medical equipment every night or that his house is vacant all day. Experts predict that, as research progresses, increasingly detailed information will be discoverable through an individual's electricity profile, down to the ability to track the use of individual appliances.¹³ "With the whole of a person's home activities laid to bare, [appliance-usage tracking] provides a better look into home activities than would peering through the blinds at that house."¹⁴ In the wrong hands, such information could even leave the customer exposed to physical danger, either from burglars or vandals able to determine the best time to strike an unguarded home or from

⁷ *Id.* at 25.

⁸ Posting of Kim Zetter to Threat Level, <http://www.wired.com/threatlevel/2009/10/smartgrid/> (Oct. 28, 2009 3:00 PM).

⁹ Press Release, The White House, *President Obama Announces \$3.4 Billion Investment to Spur Transition to Smart Energy Grid*, available at <http://www.whitehouse.gov/the-press-office/president-obama-announces-34-billion-investment-spur-transition-smart-energy-grid>.

¹⁰ See EPIC, *Comments to The National Institute of Standards and Technology on Docket No. 0909301329-91332-01* (Dec. 1, 2009), available at http://epic.org/privacy/smartgrid/EPIC_Smart_Grid-Cybersecurity_12-01-09.2.pdf; EPIC, *Comments on Proposed Policies and Findings Pertaining to the EISA Standard Regarding Smart Grid and Customer Privacy* (Dec. 18, 2009), available at http://epic.org/privacy/smartgrid/EPIC_CPUC_Smartgrid_3-09-10.pdf; EPIC, *Comments to The National Institute of Standards and Technology* (Nov. 9, 2009), available at <http://epic.org/privacy/smartgrid/EPIC%20Smart%20Grid%20Comments.pdf>.

¹¹ See EPIC, *The Smart Grid and Privacy*, <http://epic.org/privacy/smartgrid/smartgrid.html> (last visited June 6, 2010) (detailing EPIC work on smart grid privacy).

¹² National Institute for Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft) 21* (2009), available at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf.

¹³ Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), available at <http://ssrn.com/abstract=1370731>.

¹⁴ *Id.* at 25.

stalkers given another tool to track their victims. Of the \$3.4 billion awarded through SGIG, approximately \$2.8 billion will go to making and deploying smart meters.¹⁵

Given the privacy risks posed by information potentially leaked from smart meters, strong cybersecurity procedures are essential. Release of the cybersecurity plans submitted by applicants to the SGIG would benefit the public interest by allowing the public the opportunity to meaningfully study and comment on the procedures that will be used to protect its sensitive personal information.

Documents Requested

EPIC requests the following agency records (including but not limited to electronic records):

1. All cybersecurity plans submitted by SGIG grantees.
2. Any evaluation criteria used by the agency to assess the cybersecurity plans submitted by SGIG grantees.
3. Any final reports submitted by cybersecurity experts evaluating the cybersecurity plans of SGIG grantees.

Request for "News Media" Status

EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media.¹⁶

Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Thank you for your consideration of this request. As the FOIA provides, I will anticipate your determination on our request within twenty (20) working days.

¹⁵ Jeff St. John, DOE's \$3.4B Smart Grid Grant Program: The Winners, Green Tech Media, Oct. 27, 2009, <http://www.greentechmedia.com/articles/read/does-3.4b-smart-grid-grant-program-the-winners/>.

¹⁶ *Epic v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

Sincerely,

Reuben Andrew Rodriguez
EPIC Clerk

John Verdi
Director, EPIC Open Government Project