

12:10 p.m.–12:20 p.m.—Wrap-up and Adjourn March 2017 Meeting of the EAC

The meeting agenda may change to accommodate EAC business. For EAC agenda updates, see the EAC Web site at: <http://energy.gov/oe/services/electricity-advisory-committee-eac>.

**Public Participation:** The EAC welcomes the attendance of the public at its meetings. Individuals who wish to offer public comments at the EAC meeting may do so on Thursday, March 30, 2017, but must register at the registration table in advance. Approximately 5 minutes will be reserved for public comments. Time allotted per speaker will depend on the number who wish to speak but is not expected to exceed three minutes. Anyone who is not able to attend the meeting, or for whom the allotted public comments time is insufficient to address pertinent issues with the EAC, is invited to send a written statement to Mr. Matthew Rosenbaum.

You may submit comments, identified by “Electricity Advisory Committee Open Meeting,” by any of the following methods:

- **Mail/Hand Delivery/Courier:** Matthew Rosenbaum, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, Forrestal Building, Room 8G–017, 1000 Independence Avenue SW., Washington, DC 20585.

- **Email:** [matthew.rosenbaum@hq.doe.gov](mailto:matthew.rosenbaum@hq.doe.gov). Include “Electricity Advisory Committee Open Meeting” in the subject line of the message.

- **Federal eRulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.

**Instructions:** All submissions received must include the agency name and identifier. All comments received will be posted without change to <http://energy.gov/oe/services/electricity-advisory-committee-eac>, including any personal information provided.

- **Docket:** For access to the docket, to read background documents or comments received, go to <http://energy.gov/oe/services/electricity-advisory-committee-eac>.

The following electronic file formats are acceptable: Microsoft Word (.doc), Corel Word Perfect (.wpd), Adobe Acrobat (.pdf), Rich Text Format (.rtf), plain text (.txt), Microsoft Excel (.xls), and Microsoft PowerPoint (.ppt). If you submit information that you believe to be exempt by law from public disclosure, you must submit one complete copy, as well as one copy from which the information claimed to be exempt by law from public disclosure

has been deleted. You must also explain the reasons why you believe the deleted information is exempt from disclosure.

DOE is responsible for the final determination concerning disclosure or nondisclosure of the information and for treating it in accordance with the DOE’s Freedom of Information regulations (10 CFR 1004.11).

**Note:** Delivery of the U.S. Postal Service mail to DOE may be delayed by several weeks due to security screening. DOE, therefore, encourages those wishing to comment to submit comments electronically by email. If comments are submitted by regular mail, the Department requests that they be accompanied by a CD or diskette containing electronic files of the submission.

**Minutes:** The minutes of the EAC meeting will be posted on the EAC Web page at: <http://energy.gov/oe/services/electricity-advisory-committee-eac>. They can also be obtained by contacting Mr. Matthew Rosenbaum at the address above.

Issued in Washington, DC, on February 24, 2017.

**LaTanya R. Butler,**

*Deputy Committee Management Officer.*

[FR Doc. 2017–03976 Filed 2–28–17; 8:45 am]

**BILLING CODE 6450–01–P**

## DEPARTMENT OF ENERGY

### Energy Information Administration

#### CIPSEA Confidentiality Pledge Revision Notice

**AGENCY:** U.S. Energy Information Administration (EIA), Department of Energy.

**ACTION:** Notice and request for comments.

**SUMMARY:** The U.S. Energy Information Administration invites public comment on the recent revisions that have been made to the confidentiality pledge it provides to its respondents. These revisions became effective upon publication of an emergency **Federal Register** notice that announced EIA’s revised confidentiality pledge that it provides to its respondents under the Confidential Information Protection and Statistical Efficiency Act. These revisions are required by the passage and implementation of provisions of the Federal Cybersecurity Enhancement Act of 2015 which permit and require the Secretary of the Department of Homeland Security (DHS) to provide Federal civilian agencies’ information technology systems with cybersecurity protection for their Internet traffic.

More details on this announcement are presented in the **SUPPLEMENTARY INFORMATION** section below.

**DATES:** Comments regarding these confidentiality pledge revisions must be received on or before May 1, 2017. If you anticipate difficulty in submitting comments within that period, contact the person listed in **ADDRESSES** as soon as possible.

**ADDRESSES:** Written comments and/or questions about this notice should be addressed to Jacob Bournazian, U.S. Energy Information Administration, 1000 Independence Avenue SW., Washington, DC 20585 or by fax at 202–586–3045 or by email at [jacob.bournazian@eia.gov](mailto:jacob.bournazian@eia.gov).

**FOR FURTHER INFORMATION CONTACT:** Jacob Bournazian, U.S. Energy Information Administration, 1000 Independence Avenue SW., Washington, DC 20585, phone: 202–586–5562 (this is not a toll-free number), email: [jacob.bournazian@eia.gov](mailto:jacob.bournazian@eia.gov). Because of delays in the receipt of regular mail related to security screening, respondents are encouraged to use electronic communications.

**SUPPLEMENTARY INFORMATION:** Under 44 U.S.C. 3506(e), and 44 U.S.C. 3501 (note), EIA revised the confidentiality pledge(s) it provides to survey respondents under the Confidential Information Protection and Statistical Efficiency Act (44 U.S.C. 3501 (note)) (CIPSEA) in a **Federal Register** notice released on January 12, 2017 in 82 FR 3764. These revisions were required by provisions of the Federal Cybersecurity Enhancement Act of 2015 (Pub. L. 114–11, Division N, Title II, Subtitle B, Sec. 223), which permit and require the Secretary of the Department of Homeland Security (DHS) to provide Federal civilian agencies’ information technology systems with cybersecurity protection for their Internet traffic. Federal statistics provide key information that the Nation uses to measure its performance and make informed choices about budgets, employment, health, investments, taxes, and a host of other significant topics. The overwhelming majority of Federal surveys are conducted on a voluntary basis. Respondents, ranging from businesses to households to institutions, may choose whether or not to provide the requested information. Many of the most valuable Federal statistics come from surveys that ask for highly sensitive information such as proprietary business data from companies or particularly personal information or practices from individuals. Strong and trusted confidentiality and exclusively

statistical use pledges under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) and similar statistical confidentiality pledges are effective and necessary in honoring the trust that businesses, individuals, and institutions, by their responses, place in statistical agencies.

Under CIPSEA and similar statistical confidentiality protection statutes, many Federal statistical agencies make statutory pledges that the information respondents provide will be seen only by statistical agency personnel or their sworn agents, and will be used only for statistical purposes. CIPSEA and similar statutes protect the confidentiality of information that agencies collect solely for statistical purposes and under a pledge of confidentiality. These acts protect such statistical information from administrative, law enforcement, taxation, regulatory, or any other non-statistical use and immunize the information submitted to statistical agencies from legal process. Moreover, many of these statutes carry criminal penalties of a Class E felony (fines up to \$250,000, or up to five years in prison, or both) for conviction of a knowing and willful unauthorized disclosure of covered information.

As part of the Consolidated Appropriations Act for Fiscal Year 2016 signed on December 17, 2015, the Congress included the Federal Cybersecurity Enhancement Act of 2015 (Pub. L. 114–113, Division N, Title II, Subtitle B, Sec. 223). This Act, among other provisions, permits and requires DHS to provide Federal civilian agencies' information technology systems with cybersecurity protection for their Internet traffic. The technology currently used to provide this protection against cyber malware is known as Einstein 3A; it electronically searches Internet traffic in and out of Federal civilian agencies in real time for malware signatures.

When such a signature is found, the Internet packets that contain the malware signature are moved to a secured area for further inspection by DHS personnel. Because it is possible that such packets entering or leaving a statistical agency's information technology system may contain a small portion of confidential statistical data, statistical agencies can no longer promise their respondents that their responses will be seen only by statistical agency personnel or their sworn agents. However, they can promise, in accordance with provisions of the Federal Cybersecurity Enhancement Act of 2015, that such monitoring can be used only to protect information and information systems from cybersecurity

risks, thereby, in effect, providing stronger protection to the integrity of the respondents' submissions.

The DHS cybersecurity program's objective is to protect Federal civilian information systems from malicious malware attacks. The Federal statistical system's objective is to ensure that the DHS Secretary performs those essential duties in a manner that honors the Government's statutory promises to the public to protect their confidential data. Given that the Department of Homeland Security is not a Federal statistical agency, both DHS and the Federal statistical system worked to balance both objectives and achieve these mutually reinforcing objectives.

Accordingly, DHS and Federal statistical agencies, in cooperation with their parent departments, developed a Memorandum of Agreement for the installation of Einstein 3A cybersecurity protection technology to monitor their Internet traffic.

However, EIA's current CIPSEA statistical confidentiality pledge promises that respondents' data will be seen only by statistical agency personnel or their sworn agents. Since it is possible that DHS personnel could see some portion of those confidential data in the course of examining the suspicious Internet packets identified by Einstein 3A sensors, EIA needs to revise its confidentiality pledge to reflect this process change.

Therefore, EIA is providing this notice to alert the public of this revision to its confidentiality pledge in an efficient and coordinated fashion. Below is a listing of EIA's current Paperwork Reduction Act OMB numbers and information collection titles and their associated revised confidentiality pledge(s) for the Information Collections whose confidentiality pledges will change to reflect the statutory implementation of DHS' Einstein 3A monitoring for cybersecurity protection purposes.

The following EIA statistical confidentiality pledge will now apply to the Information Collections whose Paperwork Reduction Act Office of Management and Budget numbers and titles are listed below.

The information you provide on Form EIA-XXX will be used for statistical purposes only and is confidential by law. In accordance with the Confidential Information Protection and Statistical Efficiency Act of 2002 and other applicable Federal laws, your responses will not be disclosed in identifiable form without your consent. Per the Federal Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data.

Every EIA employee, as well as every agent, is subject to a jail term, a fine, or both if he or she makes public ANY identifiable information you reported.

A shorter version of the CIPSEA pledge is used for telephone surveys:

The information you provide on Form EIA-xxx will be used for statistical purposes only and is confidential by law. Per the Federal Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data. Every EIA employee, as well as every agent, is subject to a jail term, a fine, or both if he or she makes public ANY identifiable information you reported.

- OMB No: 1905–0174 Petroleum Marketing Program
  - Form EIA–863, “Petroleum Product Sales Identification Survey”
  - Form EIA–878, “Motor Gasoline Price Survey”
  - Form EIA–888, “On-Highway Diesel Fuel Price Survey”
- OMB No: 1905–0175 Natural Gas Data Collection Program
  - Form EIA–910, “Monthly Natural Gas Marketers Survey”
  - Form EIA–912, “Weekly Underground Natural Gas Storage Report”
- OMB No: 1905–0205 Monthly Natural Gas Production Report
  - Form EIA–914, “Monthly Crude Oil, Lease Condensate, and Natural Gas Production Report”
- OMB No: 1905–0160 Uranium Data Program
  - Form EIA–851Q, “Domestic Uranium Production Report—Quarterly”
  - Form EIA–851A, “Domestic Uranium Production Report—Annual”
  - Form EIA–858, “Uranium Marketing Annual Survey”
- OMB No: 1905–0145 Commercial Buildings Energy Consumption Survey
  - Form EIA–871, “Commercial Buildings Energy Consumption Survey”
- OMB No. 1905–0092 Residential Energy Consumption Survey
  - Form EIA–457, “Residential Energy Consumption Survey”

Issued in Washington, DC, on February 23, 2017.

**Nanda Srinivasan,**

*Director, Office of Survey Development and Statistical Integration, U.S. Energy Information Administration.*

[FR Doc. 2017–03971 Filed 2–28–17; 8:45 am]

**BILLING CODE 6450–01–P**

## DEPARTMENT OF ENERGY

### Federal Energy Regulatory Commission

#### Combined Notice of Filings #1

Take notice that the Commission received the following electric rate filings:

*Docket Numbers:* ER17–772–001.