Energy Information Administration
Annual Report on Implementation of CIPSEA – 4/30/11

This report is for activity during calendar year 2010.

1) **Use of the CIPSEA Confidentiality Pledge.** The Energy Information Administration (EIA) collected information under Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) from the following 12 surveys during 2010.

Office of Oil and Gas
Petroleum Marketing Surveys OMB No: 1905-0174
- Form EIA-863, "Petroleum Product Sales Identification Survey"
- Form EIA-878, "Motor Gasoline Price Survey"
- Form EIA-888, "On-Highway Diesel Fuel Price Survey"

Natural Gas Data Collection Program Package OMB No: 1905-0175
- Form EIA-910, "Monthly Natural Gas Marketers Survey"
- Form EIA-912, "Weekly Underground Natural Gas Storage Report"

Monthly Natural Gas Production Report OMB No: 1905-0205
- Form EIA-914, "Monthly Natural Gas Production Report"

Office of Coal, Nuclear, Electric and Alternative Fuels
Uranium Data Program OMB No: 1905-0160
- Form EIA-851Q, "Domestic Uranium Production Report – Quarterly"
- Form EIA-851A, "Domestic Uranium Production Report – Annual"
- Form EIA-858, "Uranium Marketing Annual Survey"

Office of Energy Markets and End Use
Commercial Buildings Energy Consumption Survey OMB No: 1905-0145
- Form EIA-871, "Commercial Buildings Energy Consumption Survey"

Residential Energy Consumption Survey OMB No. 1905-0092
- Form EIA-457, "Residential Energy Consumption Survey"

Financial Reporting System OMB No: 1905-0149
- Form EIA-28, "Financial Reporting System."

All respondents to the surveys listed above were provided the CIPSEA confidentiality pledge prior to collecting any information under CIPSEA. The CIPSEA confidentiality pledge used by the EIA on ten surveys is shown below:

> The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A of Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents without your consent. By law, every EIA employee, as well as every agent, is subject to

a jail term, a fine of up to $250,000, or both if he or she discloses ANY identifiable information about you.

The EIA uses a shorter version of the CIPSEA confidentiality pledge shown below for two weekly telephone surveys: Form EIA-878, "Motor Gasoline Price Survey;" and Form EIA-888, "On-Highway Diesel Fuel Price Survey"

> The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions in Public Law 107-347, your responses will be kept confidential and will not be disclosed in identifiable form. By law, everyone working on this EIA survey is subject to a jail term, a fine, or both if he or she discloses ANY information that could identify any confidential survey response.

2) **Compliance with the CIPSEA Implementation Guidance**. The EIA complied with the elements of OMB's CIPSEA Implementation Guidance concerning Minimum Standards for Safeguarding Confidential Information Acquired Under CIPSEA. The EIA applied appropriate administrative and technical safeguards to ensure that the confidentiality of the information reported on these surveys was protected from any unauthorized disclosures and that only authorized persons are permitted access to confidential information stored in the EIA information systems. CIPSEA information is encrypted prior to transmitting data between the EIA and its contractor agents on secure FTP sites.

The EIA maintains a written record of each person that receives CIPSEA training and who is authorized to access confidential information. Each person is required to certify their understanding of the confidentiality requirements under CIPSEA upon completion of the training. Only authorized persons who have completed CIPSEA training are permitted access to confidential information stored in the EIA information systems. All employees are certified annually. Disclosure limitation procedures are applied to the aggregated information prior to dissemination to ensure that confidential information is not disclosed.

3) **Use of Agents Provisions in CIPSEA**. The EIA designated 609 contractor employees as agents of the agency in 2010. The contractor employees performed various statistical activities categorized as follows: 513 persons provided data collection or management services; 56 persons provided data processing, analysis, or design/planning services; and 40 persons provided Information Technology support.

The EIA shared CIPSEA survey information with one (1) federal agency and one (1) organizational unit within the U.S. Department of Energy (DOE) and designated a total of five (5) federal employees as agents in 2010. The EIA shared CIPSEA survey information with one (1) DOE affiliated laboratory and designated six (6) researchers as agents for accessing CIPSEA information in 2010.

The EIA complied with Section IV of the CIPSEA Implementation Guidance concerning Requirements and Guidelines for Designating Agents to Acquire or Access confidential information protected under CIPSEA. All contracts and agreements included the appropriate provisions for protecting the confidentiality of the information. Attachment A shows the relevant provisions that the EIA used in its procurement contracts with contractors that access CIPSEA information. Attachment B shows a sample agreement that the EIA uses for designating an agent to access CIPSEA information. The EIA incorporated the appropriate provisions in the Appendix of the CIPSEA Implementation Guidance in its data access agreements.

All designated agents are certified annually. Affidavits of Nondisclosure were signed by each individual that was employed by the agency or organization that was a party to the written agreement prior to accessing the confidential information. Each individual was required to complete the CIPSEA training. A written record is maintained for each individual who signed the Affidavit of Nondisclosure, completed the training and accessed the confidential information.

ATTACHMENT A
EIA 2010 ANNUAL CIPSEA REPORT
(Contract provisions relating to data confidentiality and data safeguards)

H.18 CONFIDENTIALITY OF INFORMATION (APR 1984)

(a) To the extent that the work under this contract requires that the contractor be given access to confidential or proprietary business, technical, or financial information belonging to the Government or other companies, the contractor shall, after receipt thereof, treat such information as confidential and agree not to appropriate such information to its own use or to disclose such information to third parties unless specifically authorized by the Contracting Officer in writing. The foregoing obligations, however, shall not apply to:

(1) Information which, at the time of receipt by the contractor, is in the public domain;

(2) Information which is published after receipt thereof by the contractor or otherwise becomes part of the public domain through no fault of the contractor;

(3) Information which the contractor can demonstrate was in his possession at the time of receipt thereof and was not acquired directly or indirectly from the Government or other companies;

(4) Information which the contractor can demonstrate was received by it from a third party who did not require the contractor to hold it in confidence.

(b) The contractor shall obtain the written agreement, in a form satisfactory to the Contracting Officer, of each employee permitted access, whereby the employee agrees that he will not discuss, divulge or disclose any such information or data to any person or entity except those persons within the contractor's organization directly concerned with the performance of the contract.

(c) The contractor agrees, if requested by the Government, to sign an agreement identical, in all material respects, to the provisions of this clause, with each company supplying information to the contractor under this contract, and to supply a copy of such agreement to the Contracting Officer. From time to time upon request of the Contracting Officer, the contractor shall supply the Government with reports itemizing information received as confidential or proprietary and setting forth the company or companies from which the contractor received such information.

(d) The contractor agrees that upon request by DOE it will execute a DOE-approved agreement with any party whose facilities or proprietary data it is given access to or is furnished, restricting use and disclosure of the data or the information obtained from the facilities. Upon request by DOE, such an agreement shall also be signed by contractor personnel.

(e) This clause shall flow down to all subcontracts.

H.31 ENERGY INFORMATION ADMINISTRATION (EIA) DATA (JAN 1990) REVISED

(a) Government Furnished Computer Support. EIA will furnish necessary computer and communications resources at DOE facilities. For off-site contractor performance, EIA will make a determination for the need for remote, high-speed computer access/communications for each task order on a case-by-case basis. Government computer systems and communications services will only be provided to the contractor when there is sufficient technical and cost justification provided to and approved by the Contracting Officer.

(b) Contractor Furnished Computer Support. The contractor shall supply all necessary computer resources for off-site contract performance unless a unique circumstance exists that requires the Government to provide GFE. Any contractor terminal equipment utilized in support of approved access (on-site and/or off-site) to the EIA computer facility must be fully compatible with the EIA computer system, desktop standards, and computer security requirements.

(c) EIA Data Rights. The Government shall have ownership rights in all data produced in the performance of the contract which uses, incorporates or is based on EIA furnished data and in all programs and data produced in the performance of this contract. When specified by the Contracting Officer or in any event upon termination of the contract, all such programs and data shall be delivered to EIA in machine readable form and made operational for use at the EIA computer facility.

(d) Restrictions on Use of EIA Data. The contractor acknowledges that data furnished to it by EIA may contain information which must be held in confidence. Accordingly, the contractor agrees to retain such data in confidence and not to use any EIA furnished data except in the performance of this contract. Further, the contractor shall not duplicate or disclose any EIA furnished data or data in which the Government has ownership rights under this contract without the prior written authorization of the Contracting Officer. The contractor agrees to maintain such data in accordance with this clause and the clause "Confidentiality of Information" if included in this contract.

(e) Standards and Documentation. The contractor shall comply with all standards contained in the Energy Information Administration Standards Manual, and as imposed by the Contracting Officer's Representative (COR) regarding the design and implementation of data systems. All data systems developed by the contractor must be documented in conformance with guidelines set forth in Federal Information Processing Standard (FIPS) Publication 38, Guidelines for Documentation of Computer Programs and Automated Data Systems. The Director, Office of Information Technology (OIT) is the source of information on EIA ADP standards and related computer activities.

(f) Data Validation. Pursuant to Section 54 of the Federal Energy Administration Act of 1974, and Section 11(b) (2) of the Energy Supply and Environmental Coordination Act, of 1974, the Energy Information Administration is authorized to audit the validity of energy information. Therefore, the Government reserves the right to conduct follow-up inquiries, investigations, and/or audits as necessary to establish the meaningfulness, accuracy, reliability, and precision of any data or models used in and/or generated under this contract. Upon request by the Contracting Officer, the contractor shall assist with such inquiries, investigations, and/or audits by EIA both of the resulting products and of the methodology used to arrive at those products.

(g) Contractor Security Requirements. The contractor shall establish administrative, technical and physical security measures to protect EIA furnished data marked as "Official Use Only" data from unauthorized disclosure or use, and to prevent unauthorized access to the EIA computer system via the contractor's terminals. Failure to adequately protect "Official Use Only" data from unauthorized disclosure or misuse, or failure to prevent unauthorized access to, or misuse of,

the EIA computer system from a contractor owned or operated terminal may result in a termination of the contract for default. EIA reserves the right to inspect the contractor's physical security measures, storage methods, data handling procedures and other security safeguards to determine the security posture of the contractor's facility.

(h) Specific contractor Security Requirements for the Protection of "Official Use Only" (OUO) Data. The specific security requirements for the protection of data are:

(1) The contractor facility must be located in a building which has a 24-hour guard force or other adequate physical security measures to limit access to authorized personnel only.

(2) Physical access to contractor office areas containing OUO data must be restricted to authorized personnel only. Office areas must be equipped with appropriate locking devices, and must be secured during non-work hours.

(3) Storage of OUO data – "Official Use Only" data, when not in actual use, must be stored by one of the following methods:

(i) In a locked, bar security container;

(ii) In a locked room over which a security guard maintains periodic surveillance during non-work hours.

(4) Destruction of OUO data – "Official Use Only" Information must be disposed of in a secure manner so as to preclude its reconstruction. Approved destruction methods include:

(i) Burning;

(ii) Pulping;

(iii) Disintegrating;

(iv) Shredding; and

(v) Chemical disposition.

(5) Under no circumstances shall "Official Use Only" material be disposed of in an unapproved security disposal.

(6) Transmission of "Official Use Only" Information - OUO Information may be sent from the contractor facility by:

(i) Special messenger or courier authorized by EIA to handle OUO material;

(ii) Regular U.S. mail, or commercial services;

(iii) Teleprocessing lines; or

(iv) Authorized contractor personnel.

(7) OUO material sent by the contractor will be secured in such a way so as to preclude disclosure during transit. OUO material must be transmitted under cover of a protective cover sheet marked with the legend "Official Use Only".

(8) Marking Requirements for OUO data:

(i) Reports containing "Official Use Only" data shall be marked with the legend "Official Use Only" on the front cover, and on each internal page of the document, in bold, conspicuous letters. All OUO reports generated by the computer system will have the required markings automatically printed on the document.

(ii) Any machine readable medium (e.g. magnetic tape reels, card decks, etc.) which contains "Official Use Only" information will bear a clear external marking designating the contents "Official Use Only."

(9) Release of "Official Use Only" data - All requests received by the contractor for Official Use Only data will be referred to EIA for action.

H.42 RELEASE OF INFORMATION

Any proposed public release of information including publications, exhibits, or audiovisual productions pertaining to the effort/items called for in this contract shall be submitted at least ten (10) days prior to the planned issue date for approval. Proposed releases are to be submitted to Jonathan Cogan, 1000 Independence Ave, SW, Washington, DC, 20585 with a copy provided to the Contracting Officer.

I.6 FAR 52.227-14 RIGHTS IN DATA--GENERAL (DEC 2007)

(a) *Definitions.* As used in this clause—
"Computer database" or "database means" a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 403(8)).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright—

(1) Data first produced in the performance of this contract.

(i) Unless provided otherwise in paragraph (d) of this clause, the contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 253d, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the contractor affording the contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the contractor's expense. The Contracting Officer may agree to do so if the contractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the contractor's expense if the contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software.

(1) The contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the contractor shall—

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting.* The contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

I. 11 DEAR 952.204-2 SECURITY (MAY 2002)

(a) Responsibility. It is the contractor's duty to safeguard all classified information, special nuclear material, and other DOE property. The contractor shall, in accordance with DOE security regulations and requirements, be responsible for safeguarding all classified information and protecting against sabotage, espionage, loss or theft of the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to DOE any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract, the contractor shall identify the items and types or categories of matter proposed for retention, the reasons for the retention of the matter, and the proposed period of retention. If the retention is approved by the Contracting Officer, the security provisions of the contract shall continue to be applicable to the matter retained. Special nuclear material shall not be retained after the completion or termination of the contract.

(b) Regulations. The contractor agrees to comply with all security regulations and requirements of DOE in effect on the date of award.

(c) Definition of classified information. The term "classified information" means Restricted Data, Formerly Restricted Data, or National Security Information.

(d) Definition of restricted data. The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

(e) Definition of formerly restricted data. The term "Formerly Restricted Data" means all data removed from the Restricted Data category under section 142 d. of the Atomic Energy Act of 1954, as amended.

(f) Definition of National Security Information. The term "National Security Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced for or by, or is under the control of the United States Government, that has been determined pursuant to Executive Order 12356 or prior Orders to require protection against unauthorized disclosure, and which is so designated.

(g) Definition of Special Nuclear Material (SNM). SNM means: (1) plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which pursuant to the provisions of Section 51 of the Atomic Energy Act of 1954, as amended, has been determined to be

special nuclear material, but does not include source material; or (2) any material artificially enriched by any of the foregoing, but does not include source material.

(h) Security clearance of personnel. The contractor shall not permit any individual to have access to any classified information, except in accordance with the Atomic Energy Act of 1954, as amended, Executive Order 12356, and the DOE's regulations or requirements applicable to the particular level and category of classified information to which access is required.

(i) Criminal liability. It is understood that disclosure of any classified information relating to the work or services ordered hereunder to any person not entitled to receive it, or failure to safeguard any classified information that may come to the contractor or any person under the contractor's control in connection with work under this contract, may subject the contractor, its agents, employees, or subcontractors to criminal liability under the laws of the United States. (See the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794; and E.O. 12356.)

(j) Foreign Ownership, Control or Influence.

(1) The contractor shall immediately provide the cognizant security office written notice of any change in the extent and nature of foreign ownership, control or influence over the contractor which would affect any answer to the questions presented in the Certificate Pertaining to Foreign Interests, Standard Form 328 or the Foreign Ownership, Control or Influence questionnaire executed by the contractor prior to the award of this contract. In addition, any notice of changes in ownership or control which are required to be reported to the Securities and Exchange Commission, the Federal Trade Commission, or the Department of Justice shall also be furnished concurrently to the Contracting Officer.

(2) If a contractor has changes involving foreign ownership, control or influence, DOE must determine whether the changes will pose an undue risk to the common defense and security. In making this determination, DOE will consider proposals made by the contractor to avoid or mitigate foreign influences.

(3) If the cognizant security office at any time determines that the contractor is, or is potentially, subject to foreign ownership, control or influence, the contractor shall comply with such instructions as the Contracting Officer shall provide in writing to safeguard any classified information or special nuclear material.

(4) The contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph, in all subcontracts under this contract that will require subcontractor employees to possess access authorizations. Additionally, the contractor must require subcontractors to have an existing DOD or DOE Facility Clearance or submit a completed Certificate Pertaining to Foreign Interests, Standard Form 328, required in DEAR 952.204-73 prior to award of a subcontract. Information to be provided by a subcontractor pursuant to this clause may be submitted directly to the Contracting Officer. For purposes of this clause, subcontractor means any subcontractor at any tier and the term "Contracting Officer" means the DOE Contracting Officer. When

this clause is included in a subcontract, the term "contractor" shall mean Subcontractor and the term "contract" shall mean subcontract.

(5) The Contracting Officer may terminate this contract for default either if the contractor fails to meet obligations imposed by this clause or if the contractor creates a FOCI situation in order to avoid performance or a termination for default. The Contracting Officer may terminate this contract for convenience if the contractor becomes subject to FOCI and for reasons other than avoidance of performance of the contract, cannot, or chooses not to, avoid or mitigate the FOCI problem.

(10) Specific contractor Computer Security Requirements are:

(i) Terminals used to access the EIA computer system will be located in locked office areas, and physical access limited to authorized individuals only.

(ii) Telephone numbers of the EIA computer system, security identifiers, log-on keywords, and data set passwords will be safeguarded from unauthorized use or disclosure.

(iii) Only those contractor personnel who have been formally validated by the COR and the EIA OIT staff may access the EIA computer system.

(iv) Contractor personnel will access only those data sets which have been approved by the EIA Program Office.

(v) The COR will be notified immediately should any contractor personnel possessing current log-on keywords leave the project.

(vi) All contractor personnel accessing the EIA ADP system must be familiar with the EIA security directives, and with EIA computer system security policy and procedures published by the EIA's OIT.

(vii) The contractor agrees to appoint an individual as the contractor Computer Security Officer, who will be responsible for ensuring that EIA security policy and procedures are complied with.

I.14 952.204-72 DISCLOSURE OF INFORMATION (APR 1994)

(a) It is mutually expected that the activities under this contract will not involve classified information. It is understood, however, that if in the opinion of either party, this expectation changes prior to the expiration or terminating of all activities under this contract, said party shall notify the other party accordingly in writing without delay. In any event, the contractor shall classify, safeguard, and otherwise act with respect to all classified information in accordance with applicable law and the requirements of DOE, and shall promptly inform DOE in writing if and when classified information becomes involved, or in the mutual judgment of the parties it appears likely that classified information or material may become involved. The contractor shall have the right to terminate performance of the work under this contract and in such event the

provisions of this contract respecting termination for the convenience of the Government shall apply.

(b) The contractor shall not permit any individual to have access to classified information except in accordance with the Atomic Energy Act 1954, as amended, Executive Order 12356, and DOE's regulations or requirements.

(c) The term "Restricted Data" as used in this article means all data concerning the design, manufacture, or utilization of atomic weapons, the production of special nuclear material or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

I.16 DEAR 952.204-77 COMPUTER SECURITY (AUG 2006)

(a) Definitions.

(1) Computer means desktop computers, portable computers, computer networks (including the DOE Network and local area networks at or controlled by DOE organizations), network devices, automated information systems, and or other related computer equipment owned by, leased, or operated on behalf of the DOE.

(2) Individual means a DOE contractor or subcontractor employee, or any other person who has been granted access to a DOE computer or to information on a DOE computer, and does not include a member of the public who sends an e-mail message to a DOE computer or who obtains information available to the public on DOE Web sites.

(b) Access to DOE computers. A contractor shall not allow an individual to have access to information on a DOE computer unless:

(1) The individual has acknowledged in writing that the individual has no expectation of privacy in the use of a DOE computer; and,

(2) The individual has consented in writing to permit access by an authorized investigative agency to any DOE computer used during the period of that individual's access to information on a DOE computer, and for a period of three years thereafter.

(c) No expectation of privacy. Notwithstanding any other provision of law (including any provision of law enacted by the Electronic Communications Privacy Act of 1986), no individual using a DOE computer shall have any expectation of privacy in the use of that computer.

(d) Written records. The contractor is responsible for maintaining written records for itself and subcontractors demonstrating compliance with the provisions of paragraph (b) of this section. The contractor agrees to provide access to these records to the DOE, or its authorized agents, upon request.

(e) Subcontracts. The contractor shall insert this clause, including this paragraph (e), in subcontracts under this contract that may provide access to computers owned, leased or operated on behalf of the DOE.

ATTACHMENT B
EIA 2010 ANNUAL CIPSEA REPORT

CIPSEA INFORMATION ACCESS AGREEMENT BETWEEN U.S. ENERGY INFORMATION ADMINISTRATION and [NAME OF AGENT ORGANIZATION]

BACKGROUND

This agreement provides for the U.S. Energy Information Administration (EIA) to share confidential energy information with the [INSERT ORGANIZATION NAME]. EIA is the statistical and analytical agency within the U.S. Department of Energy (DOE). EIA collects, analyzes, and disseminates independent and impartial energy information to promote sound policy-making, efficient markets, and public understanding of energy and its interaction with the economy and the environment. To achieve this mission and to balance both public and private interests, the EIA appropriately handles and safeguards information reported by energy suppliers and consumers.

The survey information covered under this Agreement is collected by EIA under the authorities of the Federal Energy Administration Act of 1974 (Pub. L. No. 93-275, 15 U.S.C. 761 et seq.), the DOE Organization Act (Pub. L. No. 95-91, 42 U.S.C. 7101 et seq.). This information is protected under the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), Title V of the E-Government Act of 2002 (Public Law 107-347). Improper handling and/or use of EIA's statistical survey information could seriously compromise the Federal government's on-going capability to collect, analyze, and disseminate energy information. In addition, a violation of confidentiality promises made to survey respondents could result in penalties to the person causing or making the unauthorized disclosure and seriously undermine companies' willingness to participate in future EIA statistical surveys. EIA enters into this Agreement to share information in the possession of the EIA under 15 U.S.C. 771(f) which provides that EIA shall disclose to, inter alia, "other Federal Government departments, agencies, and officials for official use upon request."

[*Background paragraph about agent describing who they are, entity type, organizational purpose, and reference any experience or relationship working on energy issues*]

CONDITIONS FOR ACCESS

This Agreement provides for the disclosure by the EIA, of individually-identifiable survey information submitted to the EIA as confidential and for exclusively statistical purposes in accordance with CIPSEA to the [agent name]. Upon execution of this Agreement, the EIA shall transmit confidential respondent-level information originating to the [agent name]. This Agreement shall apply only to the information provided by EIA to [agent name] and shall not apply to information acquired by [agent name] from other sources.

The [AGENT NAME] shall abide by the following conditions while utilizing information provided under this Agreement:

1. Survey Information to be Accessed: [Describe the specific confidential information that will be provided by EIA to the agent.]

2. Legal Authority for Collection of Survey Information: EIA's survey information is collected under the authorities of the Federal Energy Administration Act of 1974 (Pub. L. No. 93-275, 15 U.S.C. 761 et seq.) and the DOE Organization Act (Pub. L. No. 95-91, 42 U.S.C. 7101 et seq.)

3. Legal Authority for EIA to Provide Access to this Survey Information: Section 512 of the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), Title V of the E-Government Act of 2002 (Public Law 107-347).

4. Purpose of Access: [Provide a clear and detailed description of the agent's purpose for accessing the information.]

5. Uses: [Describe how the information will be used by the agent and state explicitly that the information shall only be used for exclusively statistical purposes.]

6. Funding: [Discuss if there is any funding of the other party's work in conjunction with the Agreement (e.g., EIA may fund part of the agent's work because of interest in the purposes/uses and/or the agent may fund EIA activities necessary to the establishment, monitoring, and other EIA work associated with this Agreement.]

7. Dissemination Plans: [Describe the agent's plan for disseminating information based on the survey information, any products planned for public distribution, and how the agent will ensure confidentiality is protected.] The [agent name] shall apply appropriate disclosure imitation methods and rules to identify sensitive table cells that may be used to estimate a respondent's data too closely and apply either cell suppression or rounding to minimize the risk of disclosure of a specific respondent's data in the event any table cell is identified as sensitive. The [agent name] shall consult with and obtain the concurrence of EIA before publishing or disseminating any aggregations based on the information provided to help ensure that any published aggregation is in a form that precludes the identification of any respondent. The [agent name] agrees to provide EIA with copies of all reports, journal articles, book chapters or any other publicly released information products to maintain project documentation as well as a record of research covered by this Agreement.

8. Who Will Have Access: [Describe the types of persons working for the agent who will have access to the information.] The [agent name] shall do the following:
    a. Prior to providing access to an individual, provide EIA with the name and email address of each person who will have access to the information provided under this agreement. The [agent name] shall update the list as

persons no longer need access (e.g., no longer employed by the agent) or new persons (e.g., new hirers) require access.

b. Train each person who will have access, using EIA's online CIPSEA training available at http://tonto.eia.gov/smg/cipsea/cipsea_prelim.html on the appropriate handling and use of confidential information and provide confirmation to EIA that all persons who will be granted access have been trained.

c. Inform each person of the existence of this Agreement and of the penalties for violating the Agreement and CIPSEA as stated in Paragraph 11.

d. Require each person to sign a sworn Affidavit of Non-disclosure, and Non-disclosure Agreement, and provide EIA with a copy of each signed form.

9. Security: [Discuss the security plan (information systems and physical security) for protecting the information.]

a. The [agent name] shall allow EIA to carry out an unannounced physical and/or information technology security inspection of the agent's workplace, physical security measures, storage methods, data handling procedures and other security safeguards to determine the adequacy of the security system of the facility.

b. The [AGENT NAME] shall provide adequate physical and administrative safeguards to protect the information transmitted under this Agreement from inappropriate use or inadvertent disclosure during both working and non-working hours. Appropriate cyber security software and safeguards will be applied to any computer equipment where the data maybe accessed. The file server where data are stored will have limited physical access and only authorized persons covered under this Agreement may access the data from the secure server. In the event, any data covered by this agreement is stored on a laptop computer [AGENT NAME] will use encryption software that requires authentication through a password as a minimum level of data security. Failure to adequately protect the confidential data from misuse or unauthorized disclosure, or failure to prevent unauthorized access to [AGENT NAME]'s computer system may result in a termination of this Agreement. The [AGENT NAME] certifies that it is in compliance with the requirements of the Federal Information Security Management Act of 2002 and the Office of Management and Budget's Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" for securing the Federal government's information technology, safeguarding of the personally individually and breach notification requirements.

c. When the data covered by this Agreement are no longer needed by [AGENT NAME], [AGENT NAME] will delete all electronic copies of the data in its possession and destroy any hardcopy by shredding, burning or other approved disposal methods for disposing of the information in a safe and secure manner. [AGENT NAME] shall send written notice to EIA that all copies of the data have been deleted or destroyed and that it no longer is in possession of information covered under this Agreement.

10. Timeframe for Access: [Discuss when the survey information is needed as well as when the project will be completed and the survey information will be securely disposed of or returned to EIA.

11. Penalties for Violating CIPSEA: The [agent name] and any authorized person allowed to access the information shall be fully aware that willful disclosure of information provided under this Agreement in any manner to a person or agency not entitled to receive it, shall be subject to prosecution for a class E felony and imprisoned for not more than 5 years, or fined not more than $250,000, or both as set forth in CIPSEA Section 513. EIA reserves the right to terminate this agreement for any negligent act or omission by [agent name] that results in an unauthorized disclosure of confidential information to an unauthorized person.

12. Changes: The [agent name] shall notify EIA when it:
    a. No longer needs the information;
    b. Proposes a change in the site where the information will be accessed (EIA approval must be obtained before the information is moved to a new site); and/or
    c. Proposes a change in the purpose/use of the information (EIA approval must be obtained before the information is used for purposes not specified in this Agreement).

13. Requests for Information: In response to a request for the information from any party not subject to this Agreement, the [AGENT NAME] shall refer the requestor to the EIA and their request to the EIA for response. The [AGENT NAME] shall advise the requester that the information was obtained by the EIA from respondents as confidential and for exclusively statistical purposes under CIPSEA.

14. Freedom of Information Act (FOIA): The [agent name] shall not release any information in response to a request made under the Freedom of Information Act (FOIA) for this information.). A release under FOIA is defined as a "nonstatistical purpose" (CIPSEA Section 502(5)) and thus is prohibited by CIPSEA (Section 512) and subject to CIPSEA's fines and penalties (section 513).

15. EIA Right of Approval for Persons Granted Access: EIA has the right of approval on each individual working for [agent name} who shall be allowed access to the information covered under this Agreement.

16. EIA Right to Deny Individuals Access: EIA has the right to direct the [agent name] to deny access to certain individuals working for the [agent name] if EIA determines that such action is in the best interest of EIA. If the agent will not comply with such direction, the [agent name] shall immediately discontinue the use of any information provided under this Agreement and return the information to EIA.

17. Termination: This Agreement may be terminated by either party with written notification to the other party. Upon termination, all information provided under this Agreement shall be securely returned to EIA by the [agent name] and the [agent

name], all copies of the information shall be disposed of in a secure manner so as to preclude its reconstruction, and [agent name] shall make no further use of the information.

18. Contact Persons: The contact persons for this Agreement are:
    a. EIA – [name, phone number, and e-mail address]
    b. [Agent name] - [name, phone number, and e-mail address]

19. Effective and Expiration Dates: This Agreement shall become effective upon signatures of both parties and expire upon return of the information, but no later than [date].

_____ _____

Head of Agent Organization (Date)
[Title – person must be at a level equal to or higher than EIA's Administrator; e.g., Assistant Secretary of a Federal agency; head of a State or local government agency; president of a private company)
[Name of Agent Organization]

_____ _____

Richard G. Newell (Date)
Administrator
U.S. Energy Information Administration

Exhibit A - Affidavit of Nondisclosure

_____
(Name)

_____
(Job Title)

_____ _____
(Email address) (Telephone number)

_____
(Organization or government agency/Contractor)

_____
(Address of organization or government agency/Contractor)

I, _____, do solemnly swear (or affirm) that when given access to Energy Information Administration (EIA) survey information collected under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), I will not:

(1) Use or disclose any individually identifiable confidential information furnished, acquired, retrieved or assembled by me or others for any purpose other than the statistical purposes specified in the CIPSEA Information Agreement, project or contract;

(2) Remove any individually identifiable confidential information from the secure physical facility in which I am employed;

(3) Store or possess any individually identifiable confidential information at my residence;

(4) Make any disclosure or publication whereby a sample unit or survey respondent could be identified or the information furnished by or related to any particular survey respondent could be identified;

(5) Permit anyone other than the individuals authorized by EIA to examine the individual reports prior to the public release of the report; or

(6) Remove any confidential information from the approved physical facility where the confidential information are stored without prior written approval by EIA.

I certify that I am currently an employee or student of [AGENT'S NAME] , and I will notify the EIA if I am no longer affiliated with the Contractor or of any change of status with the [AGENT'S NAME].

_____
(Signature)

City/County of _____
Commonwealth/State of _____

Before me, the undersigned notary public, personally appeared _____ whose name is signed to the foregoing affidavit, and after being first duly sworn under oath by me, declared to me and in my presence that he/she willingly signed and executed it as their free and voluntary act for the purposes therein expressed.

Subscribed, sworn and acknowledged before me on this ___th day of_____, 20__.
Witness my hand and official Seal.

_____
Notary Public

My commission expires_____ (SEAL)