U.S. Energy Information Administration
Annual Report on Implementation of CIPSEA – 4/30/15

This report is for activity during calendar year 2014.

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 eleven (11) surveys during 2014.

Office of Petroleum and Biofuels Statistics
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"

Office of Oil, Gas, and Coal Supply Statistics
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 Electricity, Renewables, and Uranium Statistics
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 Consumption and Efficiency Statistics
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"

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 nine 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 in Section III of OMB's CIPSEA Implementation Guidance concerning Minimum Standards for Safeguarding Confidential Information Acquired Under CIPSEA. 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 were permitted access to confidential information stored in EIA's information systems. CIPSEA information is encrypted prior to transmitting data between EIA and its contractor agents from secure FTP sites.

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.** EIA designated 501 contractor employees as agents of the agency in 2014. The contractor employees performed various statistical activities categorized as follows: 394 persons provided data collection or management services; 84 persons provided data processing, analysis, or design/planning services; and 23 persons provided Information Technology support.

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. Nondisclosure statements 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 Nondisclosure statement, completed the training and accessed the confidential information.

ATTACHMENT A

EIA 2014 ANNUAL CIPSEA REPORT

(Contract provisions relating to data confidentiality and data safeguards)

H.12 SUBCONTRACTS (JULY 2002)

(a) Prior to the placement of subcontracts and in accordance with the clause, FAR 52.244-2 "Subcontracts" the contractor shall ensure that:

(1) they contain all of the clauses of this contract (altered when necessary for proper identification of the contracting parties) which contain a requirement for such inclusion in applicable subcontracts. Particular attention should be directed to the potential flowdown applicability of the clauses entitled "Utilization of Small Business Concerns and Small Disadvantaged Business Concerns" and "Small Business and Small Disadvantaged Business Subcontracting Plan" contained in Part II, Section I of the contract;

(2) any applicable subcontractor Certificate of Current Cost or Pricing Data (see FAR 15.404-3(b) and subcontractor Representations and Certifications (see Part IV, Section K and the document referenced in the Representations, Certifications and Other Statements of the Offeror clause are received); and

(3) any required prior notice and description of the subcontract is given to the Contracting Officer and any required consent is received. Except as may be expressly set forth therein, any consent by the Contracting Officer to the placement of subcontracts shall not be construed to constitute approval of the subcontractor or any subcontract terms or conditions, determination of the allow ability of any cost revision of this contract or any of the respective obligations of the parties there under, or creation of any subcontractor privity of contract with the Government.

(b) Prior to the award of any subcontracts for advisory and assistance services, the contractor shall obtain from the proposed subcontractor or consultant the disclosure required by 48 CFR (DEAR) 909.507-1, and shall determine in writing whether the interests disclosed present an actual or significant potential for an organizational conflict of interest, in accordance with the clause contained in Section I of this contract. No work shall be performed by the subcontractor until the contractor has cleared the subcontractor for Organizational Conflicts of Interest (OCI).

H.18 <u>CONFIDENTIALITY OF INFORMATION (APR 1984)</u>

(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.

(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 ADP Services Staff may access the EIA computer system.

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

(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 Directive, and with EIA computer system security policy and procedures published by the EIA's Information Technology Group.

(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.

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.

H.35. Access to DOE-Owned Or Leased Facilities (OCT 2005)

(a) The performance of this contract requires that employees of the Contractor have physical access to DOE-owned or leased facilities; however, this clause does not control requirements for an employee's obtaining a security clearance. The Contractor understands and agrees that DOE has a prescribed process with which the contractor and its employees must comply in order to receive a security badge that allows such physical access. The Contractor further understands that it must propose employees whose background offers the best prospect of obtaining a security badge approval for access, considering the following criteria, which are not all inclusive and may vary depending on access requirements:

(1) is, or is suspected of being a terrorist;

(2) is the subject of an outstanding warrant;

(3) has deliberately omitted, concealed, or falsified relevant and material facts from any Questionnaire for National Security Positions (SF-86), Questionnaire for Non-Sensitive Positions (SF-85), or similar form;

(4) has presented false or forged identity source documents;

(5) has been barred from Federal employment;

(6) is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or

(7) is awaiting or serving a form of pre-prosecution, probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of sic(6) months or longer.

(b) The Contractor shall assure:

(1) In initiating the process for gaining physical access, (i) compliance with procedures established by DOE in providing its employee(s) with any forms directed by DOE, (ii) that the employee properly completes any forms, and (iii) that the employee(s) submits the forms to the person designated by the Contracting Officer.

(2) In completing the process for gaining physical access, that its employee (i) cooperates with DOE officials responsible for granting access to DOE –owned or leased facilities and (ii) provides additional information, requested by those DOE officials.

(c) The Contractor understands and agrees that DOE may unilaterally deny a security badge to an employee and that the denial remains effective for that employee unless DOE subsequently determines that access may be granted. Upon notice from DOE that an employee's application for a security badge is or will be denied, the Contractor shall promptly identify and submit the forms referred to in subparagraph (b)(1) of his clause for the substitute employee. The denial of a security badge to individual employees by DOE shall not be cause for extension of the period of performance of this Contract or any contractor claim against DOE.

(d) The Contractor shall return to the Contracting Officer or designee the badge(s) or other credential(s) provided by DOE pursuant to this clause, granting physical access to DOE – owned or leased facilities by the Contractor's employee(s), upon (1) the termination of this Contract; (2) the expiration of this Contract; (3) the termination of employment of this Contract by an individual employee; or (4) demand by DOE for return of the badge.

(e) The Contractor shall include this clause, including this paragraph (e), in any subcontract, awarded in the performance of this Contract, in which an employee(s) of the subcontractor will require physical access to DOE-owned or leased facilities.

I. 11 <u>DEAR 952.204-2 SECURITY (MAY 2002)</u>

(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.

DOE-H-2063 Confidentiality Of Information (OCT 2014)

(a) Performance of work under this contract may result in the Contractor having access to confidential information via written or electronic documents, or by virtue of having access to

DOE's electronic or other systems. Such confidential information includes personally identifiable information (such as social security account numbers) or proprietary business, technical, or financial information belonging to the Government or other companies or organizations. The Contractor shall treat this information as confidential and agrees not to use this information for its own purposes, or to disclose the information to third parties, unless specifically authorized to do so in writing by the Contracting Officer.

(b) The restrictions set out in paragraph (a) above, however, do not apply to -

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

(2) Information which, subsequent to receipt by the Contractor, becomes part of the public domain through no fault or action of the Contractor;

(3) Information which the Contractor can demonstrate was previously in its possession and was not acquired directly or indirectly as a result of access obtained by performing work under this contract;

(4) Information which the Contractor can demonstrate was received from a third party who did not require the Contractor to hold it in confidence; or

(5) Information which is subject to release under applicable law.

(c) The Contractor shall obtain a written agreement from each of its employees who are granted access to, or furnished with, confidential information, whereby the employee agrees that he or she will not discuss, divulge, or disclose any such information to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract. The agreement shall be in a form satisfactory to the Contracting Officer.

(d) Upon request of the Contracting Officer, the Contractor agrees to execute an agreement with any party which provides confidential information to the Contractor pursuant to this contract, or whose facilities the Contractor is given access to that restrict use and disclosure of confidential information obtained by the Contractor. A copy of the agreement, which shall include all material aspects of this clause, shall be provided to the Contracting Officer for approval.

(e) Upon request of the Contracting Officer, the Contractor shall supply the Government with reports itemizing the confidential or proprietary information it receives under this contract and identify the source (company, companies or other organizations) of the information.

(f) The Contractor agrees to flow down this clause to all subcontracts issued under this contract.

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

BACKGROUND

The U.S. Energy Information Administration (EIA) is the statistical and analytical agency of 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 serve both public and private interests, the EIA appropriately protects 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.), and 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 making the unauthorized disclosure and seriously undermine companies' willingness to participate in future EIA statistical surveys.

[*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

Upon execution of this Agreement, the EIA shall transmit confidential respondent-level information 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 survey 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) [*if sharing with another federal agency*] and 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."

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

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., DOE 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] agrees to publicly report any results relating to Proprietary Data in such a way that the identity of a specific company, facility, or person may not be reasonably inferred by either direct or indirect means The [AGENT NAME] shall apply appropriate disclosure limitation 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, rounding, or, collapse table rows or columns to minimize the risk of disclosure of a specific respondent's data in the event any table cell is identified as sensitive. Statistical methods for protecting tabular data are discussed in Chapter 4 of Statistical Policy Working Paper No. 22 "Report on Statistical Disclosure Methodology" available at http://www.fcsm.gov/working-papers/spwp22.html. 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. [AGENT NAME] agrees to provide EIA with the hyperlinks, or copies of all reports, journal articles, book chapters or any other publicly released information products to maintain project documentation covered by this Agreement.

8. Who Will Have Access: The persons accessing the data covered under this Agreement include [Insert the names of the persons accessing the data. 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 of each person who will have access to the information provided under this agreement. The notice shall include a reference whether the person is an employee of the [AGENT NAME] or a contractor of [AGENT NAME]. If the person is employed as a contractor, the notice shall include the contractor's name, address, telephone number and project manager's name and complete contact information. The [AGENT NAME] shall update the list as persons that 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 modules, available at http://tonto.eia.doe.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 by mailing the original signed certificates to EIA at the address shown on the form.
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.
   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 or destruction of the information, but no later than [insert termination date].

_____ _____

Head of Agent Organization (Date)
[Title – person must be an Agency head 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]

_____ _____

Adam Sieminski (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 U.S. 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)