U.S. Energy Information Administration
Annual Report on Implementation of CIPSEA – 4/30/18

This report is for activity during calendar year 2017.

1) Use of the CIPSEA Confidentiality Pledge. The U.S. Energy Information Administration (EIA) protected information collected from the following 11 surveys under the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) during 2017.

- Office of Petroleum and Biofuels Statistics
  - Petroleum Marketing Surveys OMB No: 1905-0174
    1. Form EIA-863 *Petroleum Product Sales Identification Survey* (suspended)
    2. Form EIA-878 *Motor Gasoline Price Survey*
    3. 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
    4. Form EIA-910 *Monthly Natural Gas Marketers Survey*
    5. Form EIA-912 *Weekly Underground Natural Gas Storage Report*
  - Monthly Crude Oil and Lease Condensate, and Natural Gas Production Report OMB No: 1905-0205
    6. Form EIA-914 *Monthly Crude Oil and Lease Condensate, and Natural Gas Production Report*
- Office of Electricity, Renewables, and Uranium Statistics
  - Uranium Data Program OMB No: 1905-0160
    7. Form EIA-851Q *Domestic Uranium Production Report – Quarterly*
    8. Form EIA-851A *Domestic Uranium Production Report – Annual*
    9. Form EIA-858 *Uranium Marketing Annual Survey*
- Office of Energy Consumption and Efficiency Statistics
  - Commercial Buildings Energy Consumption Survey OMB No: 1905-0145
    10. Form EIA-871 *Commercial Buildings Energy Consumption Survey*
  - Residential Energy Consumption Survey OMB No. 1905-0092
    11. 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.

As required by the passage of the Federal Cybersecurity Enhancement Act of 2015, EIA implemented the U.S. Department of Homeland Security's Einstein Cybersecurity Protection Program and modified the CIPSEA pledge language to notify respondents of this monitoring. On January 11, 2017. OMB granted EIA's request under OMB Control Number 1905-0211for an emergency six month approval so that EIA may immediately

use the revised confidentiality pledge beginning January, 2017. EIA published 60-day and 30-day federal register notices to solicit public comment and subsequently submitted the normal clearance request to OMB to convert the emergency clearance to permanent status. OMB approved the conversion of the emergency clearance to permanent status for the information collections under OMB Control Number 1905-0211 for three years on June 29, 2017. EIA updated the revised confidentiality pledges in response to the Federal Cybersecurity Enhancement Act of 2015 for all 11 surveys. EIA subsequently filed non-substantive changes and uploaded revised survey instructions containing revised pledges during 2017.

The text below is the modified CIPSEA pledge that EIA used for nine surveys during 2017 for protecting information:

> "The information you provide on Form EIA-xxx will be used for statistical purposes only and is confidential by law. In accordance with the Confidential Information Protection and Statistical Efficiency Act of 2002 and other applicable Federal laws, your responses will not be disclosed in identifiable form without your consent. Per the Federal Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data. Every EIA employee, as well as every agent, is subject to a jail term, a fine, or both if he or she makes public ANY identifiable information you reported."

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

2) Compliance with the CIPSEA Implementation Guidance. EIA complied with the elements outlined in Section III of OMB's *CIPSEA Implementation Guidance for Title V of the E-government Act* dated June 15, 2007 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 were permitted access to confidential information stored in EIA information systems. CIPSEA information is encrypted prior to transmitting data between the EIA and its contractor agents from secure FTP (File Transfer Protocol) sites.

EIA maintains a written record of each person that receives CIPSEA training and who is authorized to access confidential information. Persons that need access to CIPSEA protected data are re-certified every year by completing EIA's online training program. 555 persons took the online training and recertified in 2017. Of the 555, 245 were federal employees and EIA designated 310 persons as agents. Only persons who have completed the online CIPSEA training are authorized to access confidential information stored in EIA information systems.

Each person that needs access to CIPSEA protection information is required to complete EIA's online CIPSEA training. All designated agents are certified annually. Nondisclosure statements are signed by each person that was employed by the agency or organization that was a party to the written data access agreement prior to accessing confidential information. A written record is maintained for each individual who signed the nondisclosure statement, completed the training, and accessed the confidential information.

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 310 contractor employees as agents of the agency in 2017. The contractor employees performed various statistical activities categorized as follows: 110 persons provided data collection or management services; 115 persons provided data processing, analysis, or design/planning services; and 85 persons provided Information Technology support.

EIA complied with Section IV of the *CIPSEA Implementation Guidance* concerning, "Requirements and Guidelines for Statistical Agencies or Organizational Units When 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 EIA used in its procurement contracts with contractors that access CIPSEA information. Attachment B shows a sample agreement that EIA uses for designating an agent to access CIPSEA information. EIA incorporated the appropriate provisions in the Appendix of the *CIPSEA Implementation Guidance* in its data access agreements.

ATTACHMENT A

EIA 2017 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 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.

H.20 DOE-H-2075 Prohibition on Funding for Certain Nondisclosure Agreements (OCT 2014)

The Contractor agrees that:

(a) No cost associated with implementation or enforcement of nondisclosure policies, forms or agreements shall be allowable under this contract if such policies, forms or agreements do not contain the following provisions: "These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."

(b) The limitation above shall not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(c) Notwithstanding the provisions of paragraph (a), a nondisclosure or confidentiality policy form or agreement that is to be executed by a person connected with the conduct of an intelligence or intelligence-related activity, other than an employee or officer of the United States Government, may contain provisions appropriate to the particular activity for which such document is to be used. Such form or agreement shall, at minimum, require that the person will not disclose any classified information received in the course of such activity unless specifically authorized to do so by the United States Government. Such nondisclosure or confidentiality forms shall also make it clear that they do not bar disclosures to Congress, or to an authorized official of an executive agency or the Department of Justice, that are essential to reporting a substantial violation of law.

H.23 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.24. Access to DOE-Owned Or Leased Facilities (OCT 2005) (EIA 2012 Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)

(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 six (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. (See Attachment E – Affidavid of Nondisclosure).

(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 this 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 on 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.

DEAR 952.204-2 Security (MAR 2011)

(a) Responsibility. It is the Contractor's duty to protect all classified information, special nuclear material, and other DOE property. The Contractor shall, in accordance with DOE security regulations and requirements, be responsible for protecting all classified information and all classified matter (including documents, material and special nuclear material) which are in the Contractor's possession in connection with the performance of work under this contract against sabotage, espionage, loss or theft. Except as otherwise expressly provided in this contract, the Contractor shall, upon completion or termination of this contract, transmit to DOE any classified matter or special nuclear material 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 classification levels and categories of matter proposed for retention, the reasons for the retention, 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 classified 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 contract requirements of DOE as incorporated into the contract.

(c) Definition of Classified Information. The term Classified Information means information that is classified as Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954, or information determined to require protection against unauthorized disclosure under Executive Order 12958, Classified National Security Information, as amended, or prior executive orders, which is identified as National Security Information.

(d) Definition of Restricted Data. The term Restricted Data means all data concerning design, manufacture, or utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy, but excluding data declassified or removed from the Restricted Data category pursuant to 42 U.S.C. 2162 [Section 142, as amended, of the Atomic Energy Act of 1954].

(e) Definition of Formerly Restricted Data. The term "Formerly Restricted Data" means information removed from the Restricted Data category based on a joint determination by DOE or its predecessor agencies and the Department of Defense that the information-- (1) relates primarily to the military utilization of atomic weapons; and (2) can be adequately protected as National Security Information. However, such information is subject to the same restrictions on transmission to other countries or regional defense organizations that apply to Restricted Data.

(f) Definition of National Security Information. The term "National Security Information" means information that has been determined, pursuant to Executive Order 12958, Classified National Security Information, as amended, or any predecessor order,

to require protection against unauthorized disclosure, and that is marked to indicate its classified status when in documentary form.

(g) Definition of Special Nuclear Material. The term “special nuclear material” means-- (1) plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which, pursuant to 42 U.S.C. 2071 [section 51 as amended, of the Atomic Energy Act of 1954] 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) Access authorizations of personnel. (1) The Contractor shall not permit any individual to have access to any classified information or special nuclear material, except in accordance with the Atomic Energy Act of 1954, and the DOE's regulations and contract requirements applicable to the particular level and category of classified information or particular category of special nuclear material to which access is required. (2) The Contractor must conduct a thorough review, as defined at 48 CFR 904.401, of an uncleared applicant or uncleared employee, and must test the individual for illegal drugs, prior to selecting the individual for a position requiring a DOE access authorization.

(i) A review must-- verify an uncleared applicant’s or uncleared employee’s educational background, including any high school diploma obtained within the past five years, and degrees or diplomas granted by an institution of higher learning; contact listed employers for the last three years and listed personal references; conduct local law enforcement checks when such checks are not prohibited by state or local law or regulation and when the uncleared applicant or uncleared employee resides in the jurisdiction where the Contractor is located; and conduct a credit check and other checks as appropriate.

(ii) Contractor reviews are not required for an applicant for DOE access authorization who possesses a current access authorization from DOE or another Federal agency, or whose access authorization may be reapproved without a federal background investigation pursuant to Executive Order 12968, Access to Classified Information (August 4, 1995), Sections 3.3(c) and (d).

(iii) In collecting and using this information to make a determination as to whether it is appropriate to select an uncleared applicant or uncleared employee to a position requiring an access authorization, the Contractor must comply with all applicable laws, regulations, and Executive Orders, including those-- (A) governing the processing and privacy of an individual’s information, such as the Fair Credit Reporting Act, Americans with Disabilities Act (ADA), and Health Insurance Portability and Accountability Act; and (B) prohibiting discrimination in employment, such as under the ADA, Title VII and the Age Discrimination in Employment Act, including with respect to pre- and post-offer of employment disability related questioning.

(iv) In addition to a review, each candidate for a DOE access authorization must be tested to demonstrate the absence of any illegal drug, as defined in 10 CFR 707.4. All positions requiring access authorizations are deemed testing designated positions in accordance

with 10 CFR part 707. All employees possessing access authorizations are subject to applicant, random or for cause testing for use of illegal drugs. DOE will not process candidates for a DOE access authorization unless their tests confirm the absence from their system of any illegal drug.

(v) When an uncleared applicant or uncleared employee receives an offer of employment for a position that requires a DOE access authorization, the Contractor shall not place that individual in such a position prior to the individual's receipt of a DOE access authorization, unless an approval has been obtained from the head of the cognizant local security office. If the individual is hired and placed in the position prior to receiving an access authorization, the uncleared employee may not be afforded access to classified information or matter or special nuclear material (in categories requiring access authorization) until an access authorization has been granted.

(vi) The Contractor must furnish to the head of the cognizant local DOE Security Office, in writing, the following information concerning each uncleared applicant or uncleared employee who is selected for a position requiring an access authorization-- A. The date(s) each Review was conducted; B. Each entity that provided information concerning the individual; C. A certification that the review was conducted in accordance with all applicable laws, regulations, and Executive Orders, including those governing the processing and privacy of an individual's information collected during the review; D. A certification that all information collected during the review was reviewed and evaluated in accordance with the Contractor's personnel policies; and E. The results of the test for illegal drugs.

(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 protect any classified information, special nuclear material, or other Government property 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, 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794).

(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 Standard Form (SF) 328, Certificate Pertaining to Foreign Interests, executed prior to 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. Contractors are encouraged to submit this information through the use of the online tool at https://foci.td.anl.gov. When completed the Contractor must print and sign one copy of the SF 328 and submit it 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 protect any classified information or special nuclear material. (4) 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 foreign ownership, control, or influence 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 foreign ownership, control, or influence and for reasons other than avoidance of performance of the contract, cannot, or chooses not to, avoid or mitigate the foreign ownership, control, or influence problem.

(k) Employment announcements. When placing announcements seeking applicants for positions requiring access authorizations, the Contractor shall include in the written vacancy announcement, a notification to prospective applicants that reviews, and tests for the absence of any illegal drug as defined in 10 CFR 707.4, will be conducted by the employer and a background investigation by the Federal government may be required to obtain an access authorization prior to employment, and that subsequent reinvestigations may be required. If the position is covered by the Counterintelligence Evaluation Program regulations at 10 CFR 709, the announcement should also alert applicants that successful completion of a counterintelligence evaluation may include a counterintelligence-scope polygraph examination.

(l) Flow down to subcontracts. The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph, in all subcontracts under its contract that will require subcontractor employees to possess access authorizations. Additionally, the Contractor must require such subcontractors to have an existing DOD or DOE facility clearance or submit a completed SF 328, Certificate Pertaining to Foreign Interests, as required in 48 CFR 952.204-73, Facility Clearance, and obtain a foreign ownership, control and influence determination and facility clearance 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.

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.

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

2017 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 data protection 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 Limitation Methodology" available at http://fcsm.sites.usa.gov/files/2014/04/spwp22.pdf. 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 a copy of the agency's contracting provisions that relate to protecting or safeguarding confidential data that are satisfactory to EIA, 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://www.eia.gov/cipsea/cipsea.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 an original 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. These safeguards include access restrictions and authentication requirements, through locked doors with key card ID swipe security access or similar technology to apply authentication and access restrictions, to ensure only authorized personnel may physically enter the server room. Appropriate cyber security software and safeguards will be applied to any computer equipment where the data may be accessed. Computer terminals used to access EIA information shall be located in locked office areas, and physical access limited to authorized individuals only. Security identifiers, log-on passwords, and data set passwords will be applied to any computer equipment where the Proprietary Data may be accessed. The file server where data are stored will have access restricted to authorized

persons referenced in this Agreement and an audit log will be maintained of persons accessing the protected data files from the restricted folder on the server. All log-in attempts are tracked by system logs. Passwords security shall include a minimum length of 8 characters, including one upper case letter, one lower case letter and one symbol and no dictionary words. 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. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute, or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

19. 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]

20. 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]

_____ _____

John J. Conti (Date)
Acting 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 I am a U.S. citizen and when given access to U.S. Energy Information Administration (EIA) survey information protected under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), I will use the confidential information furnished, acquired, retrieved or compiled by me or others only for statistical purposes specified in the CIPSEA Information Access Agreement, project or contract. I understand that I must complete the online CIPSEA training and return this signed Affidavit and the CIPSEA training certificate to EIA prior to accessing any confidential EIA survey information.

Pursuant to section 744 of Title VII, division E of the Consolidated Appropriations Act, 2016:

"These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling."

During the time period that I have access to confidential information I will not:

(1) Remove any individually identifiable confidential information from the secure physical facility in which I am employed;
(2) Store or possess any individually identifiable confidential information at my residence;
(3) Make any public disclosure or information release 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;
(4) Permit anyone other than the individuals authorized by EIA to examine the individual reports prior to the public release of the report; or
(5) 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 _____ ss:

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)