Energy Information Administration
Annual Report on Implementation of CIPSEA

This report is for activity during calendar year 2009.

1) **Use of the CIPSEA Confidentiality Pledge.** The Energy Information Administration (EIA) collected information under Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) from the following 12 surveys during 2009.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3) **Use of Agents Provisions in CIPSEA**. The EIA designated 282 contractor employees as agents of the agency in 2009. The contractor employees performed various statistical activities categorized as follows: 181 persons provided data collection or management services; 68 persons provided data processing, analysis, or design/planning services; and 33 persons provided Information Technology support.

The EIA shared CIPSEA survey information with three (3) federal agencies and designated a total of five (5) federal employees as agents in 2009. The EIA designated one (1) researcher as an agent for accessing CIPSEA information in 2009. The researcher completed his work during 2009 and accessed the information on-site at the EIA headquarter facility.

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.

EIA staff inspected two off-site federal agency facilities during 2009. All designated agents are certified annually. Affidavits of Nondisclosure were signed by each individual that was employed by the agency or organization that was a party to the written agreement prior to accessing the confidential information. Each individual was required to complete the CIPSEA training. A written record is maintained for each individual who signed the Affidavit of Nondisclosure, completed the training and accessed the confidential information.

Attachment A

H.12 Confidentiality Of Information (APR 1984)

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

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

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

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

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

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

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

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

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

H.13 Energy Information Administration (EIA) Data (JAN 1990) Revised

(a) Government Furnished Computer Support. EIA will furnish available computer resources required for performance of this contract for personnel assigned to perform work at a DOE facility such as the Forrestal building.

For off-site performance, EIA will furnish remote high speed computer access to the Contractor's LAN, if it complies with paragraphs (b) through (h) below.

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

(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, Information Technology Group (ITG) 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.14 **Subcontracts (July 2002)**

(a) Prior to the placement of subcontracts and in accordance with the clause, "Subcontracts Under Cost-Reimbursement and Letter Contracts," the Contractor shall ensure that:

ATTACHMENT B
EIA 2009 ANNUAL CIPSEA REPORT

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

BACKGROUND

The Energy Information Administration (EIA) was created by Congress in 1977 as the statistical 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 balance both public and private interests, the EIA appropriately handles and safeguards information reported by energy suppliers and consumers.

The survey information covered under this Agreement is collected by EIA under the authorities of the Federal Energy Administration Act of 1974 (Pub. L. No. 93-275, 15 U.S.C. 761 et seq.), the DOE Organization Act (Pub. L. No. 95-91, 42 U.S.C. 7101 et seq.) and 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 seriously undermine companies' willingness to participate in future EIA statistical surveys. Significant nonresponse could cause information quality problems that would result in discontinuing affected statistical time series.

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

CONDITIONS FOR ACCESS

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

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

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

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

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

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

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

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

7. Dissemination Plans: [Describe the agent's plan for disseminating information based on the survey information, any products planned for public distribution, and how the agent will ensure confidentiality is protected.] The [agent name] shall 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.

8. Who Will Have Access: [Describe the types of persons working for the agent who will have access to the information.] The [agent name] shall do the following:
    a. Prior to providing access to an individual, provide EIA with the name of each persons who will have access to the information provided under this agreement. The [agent name] shall update the list as persons no longer need access (e.g., no longer employed by the agent) or new persons (e.g., new hirers) require access.
    b. Train each person who will have access, using EIA's online CIPSEA training modules, on the appropriate handling and use of confidential information and provide confirmation to EIA that all persons who will be granted access have been trained.
    c. Inform each person of the existence of this Agreement and of the penalties for violating the Agreement and CIPSEA as stated in Paragraph 11.
    d. Require each person to sign a sworn Affidavit of Non-disclosure, and Non-disclosure Agreement, and provide EIA with a copy of each signed form.

9. Security: [Discuss the security plan (information systems and physical security) for protecting the information.]
    a. The [agent name] shall allow EIA to carry out an unannounced physical and/or information technology security inspection of the agent's workplace, physical security measures, storage methods, data handling procedures and other security safeguards to determine the adequacy of the security system of the facility.
    b. The [AGENT NAME] shall provide adequate physical and administrative safeguards to protect the information transmitted under this Agreement from inappropriate use or inadvertent disclosure during both working and non-working hours. Appropriate cyber security software and safeguards will be applied to any computer equipment where the data maybe accessed. The file server where data are stored will have limited physical access and only authorized persons covered under this Agreement may access the data from the secure server. In the event, any data covered by this agreement is stored on a laptop computer [AGENT NAME] will use encryption software that requires authentication through a password as a minimum level of data security. Failure to adequately protect the confidential data from misuse or unauthorized disclosure, or failure to prevent unauthorized access to [AGENT NAME]'s computer system may result in a termination of this Agreement. The [AGENT NAME] certifies that it is in compliance with the requirements of the Federal Information Security Management Act of 2002 and the Office of Management and Budget's Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" for securing the Federal government's information technology, safeguarding of the personally individually and breach notification requirements.
    c. When the data covered by this Agreement are no longer needed by [AGENT NAME], [AGENT NAME] will delete all electronic copies of the data in its possession and destroy any hardcopy by shredding, burning or other approved disposal methods for disposing of the information in a safe and secure manner. [AGENT NAME] shall send written notice to EIA that all copies of the data have been deleted or destroyed and that it no longer is in possession of information covered under this Agreement.

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

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

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

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

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

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

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

17. Termination: This Agreement may be terminated by either party with written notification to the other party. Upon termination, all information provided under this Agreement shall be securely returned to EIA by the [agent name] and the [agent name], all copies of the information shall be disposed of in a secure manner so as to preclude its reconstruction, and [agent name] shall make no further use of the information.

18. Contact Persons: The contact persons for this Agreement are:
    a. EIA – [name, phone number, and e-mail address]
    b. [Agent name] - [name, phone number, and e-mail address]
    c. 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 May 31, 2009.

20. Effective and Expiration Dates: This Agreement shall become effective upon

signatures of both parties and expire upon return of the information, but no later than [date].

_____ _____

Head of Agent Organization (Date)
[Title – person must be at a level equal to or higher than Mr. Caruso; 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]

_____ _____

Guy F. Caruso (Date)
Administrator
Energy Information Administration

Exhibit A - Affidavit of Nondisclosure

_____
(Name)

_____
(Job Title)

_____ _____
(Email address) (Telephone number)

_____
(Organization or government agency/Contractor)

_____
(Address of organization or government agency/Contractor)

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

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

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

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

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

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

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

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

_____
(Signature)

City/County of _____
Commonwealth/State of _____

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

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

_____
Notary Public

My commission expires_____ (SEAL)