# Energy Information Administration
# Annual Report on Implementation of CIPSEA – 4/30/08

This report is for activity during calendar year 2007.

1) 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 2007.

Office of Oil and Gas
Form EIA-863, "Petroleum Product Sales Identification Survey"
Form EIA-878, "Motor Gasoline Price Survey"
Form EIA-888, "On-Highway Diesel Fuel Price Survey"
Form EIA-910, "Monthly Natural Gas Marketers Survey"
Form EIA-912, "Weekly Underground Natural Gas Storage Report"
Form EIA-914, "Monthly Natural Gas Production Report"

Office of Coal, Nuclear, Electric and Alternative Fuels
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
Form EIA-871, "Commercial Buildings Energy Consumption Survey"
Form EIA-457, "Residential Energy Consumption Survey"
Form EIA-28, "Financial Reporting System."

All respondents to the surveys listed above were notified using the CIPSEA pledge prior to collecting any information under CIPSEA. In the notice to respondents EIA pledged to keep the information confidential and that the information would be used exclusively for statistical purposes.

2) EIA designated 12 contractors as agents of the agency in 2007. Six contractors performed a range of statistical activities including data collection, editing, and processing. Two contractors performed data base management, data systems development and support, and analysis. Two contractors performed data validation. One contractor handled the data archival, storage, and retrieval of the confidential information collected under CIPSEA. One contractor performed system maintenance for the servers where the data are hosted on-site.

The contractors' staffs that were designated as agents for EIA were required to complete on-line CIPSEA training at http://tonto.eia.doe.gov/smg/cipsea/cipsea_prelim.html prior to accessing any confidential information EIA maintains a written record of each person that receives CIPSEA training and 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.

The EIA followed the procedures in OMB's Implementation Guidance for CIPSEA dated June 15, 2007 in applying appropriate administrative and technical safeguards to ensure that the confidentiality of the information reported on these surveys was protected from any unauthorized disclosures. CIPSEA information are encrypted using Secured Socket Layer software prior to transmitting data between 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. All contractors accessing CIPSEA information off-site are required to use Virtual Private Network (VPN) software. In 2007, seven contractors accessed confidential information off-site from EIA headquarters using VPN software on nine of the CIPSEA surveys. Contractors were required to follow all requirements for data safeguards and procedures in their procurement contracts with EIA. The relevant provisions in EIA uses with its contractors that access CIPSEA information is shown in Attachment A.

During 2007 EIA did not designate any researchers as agents for accessing confidential information and did not enter into any licensing agreement to allow access at an off-site facility or agency controlled research data center.

3) EIA had no CIPSEA data sharing activities with other federal agencies under Subtitle B of CIPSEA during 2007.

Sincerely,

/signed on May 2, 2008/JHC

Jay Casselberry
Confidentiality Officer and
Executive Assistant to the Administrator
Energy Information Administration
U.S. Department of Energy

**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:

(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 15.404-3b) 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 allowability of any cost revision of this contract or any of the respective obligations of the parties thereunder, 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).