

NOTICE:

I. The following document entitled "United States Environmental Protection Agency Office of Air and Radiation Climate Change Division Greenhouse Gas Reporting Program & Greenhouse Gas Inventory CBI Policy" dated September 2, 2011 applies specifically to the following EPA contracts:

Active CCD Contracts as follows:

1. EP-W-07-067
2. EP-W-07-068
3. EP-W-07-069
4. EP-W-07-070
5. EP-W-07-071
6. EP-W-07-072

II. The policy shall also apply to any future CCD acquisitions that may involve work with the Greenhouse Gas Reporting Rule Program.

NOTE: Some document formatting may be lost by posting to the web.

United States
Environmental Protection Agency
Office of Air and Radiation
Office of Atmospheric Programs
Climate Change Division
Greenhouse Gas Reporting Program
Confidential Business Information Policy

September 28, 2011

Table of Contents

- Section 1 – Confidential Business Information (CBI) 6
- Policy Introduction, References, & Responsibilities 6
 - 1.1 Overview and Purpose 6
 - 1.2 Guidance Policies & Related Documents 6
 - 1.2.1 EPA 40 CFR Part 2..... 6
 - 1.2.2 EPA Information Security Manual (ISM) 7
 - 1.2.3 Greenhouse Gas Reporting Program (GHGRP) System Security Plan (SSP)..... 7
 - 1.3 Responsibilities 7
 - 1.3.1 EPA Employees..... 7
 - 1.3.2 GHGRP Contractors and Subcontractors 7
 - 1.3.3 CBI Administrator..... 8
 - 1.3.4 Alternate CBI Administrator..... 8
 - 1.3.5 EPA Management..... 8
 - 1.3.6 Contracting Officer (CO)..... 8
 - 1.3.7 Contracting Officer Representative (COR) 8
 - 1.3.8 EPA OEI National Computing Center (NCC) 8
 - 1.4 Application 9
 - 1.4.1 Electronic – Greenhouse Gas Reporting Tool (E-GGRT)..... 9
 - 1.5 Types of CBI Materials 9
 - 1.5.1 Hardcopy Materials..... 9
 - 1.5.2 Electronic Materials 9
- Section 2 – CBI Access Authority..... 9
 - 2.1 Eligibility for Access..... 9
 - 2.1.1 Need-to-Know 9
 - 2.1.2 Policy Acknowledgement..... 9
 - 2.2. Awareness Training..... 9
 - 2.2.1 EPA Employee Training Requirements..... 9
 - 2.2.2 Contractor Training Requirements 10
 - 2.2.3 Other Personnel Granted CBI Access 10
 - 2.3. CBI Access Procedures 10
 - 2.3.1 Rooms and Systems 10

2.3.2 Eligible Authorized Users	11
2.4 Relinquishment / Termination of Access Procedures	11
2.4.1 EPA Employees	12
2.4.2 Other Federal Agencies	12
2.4.3 NCC Contractors	12
2.4.4 Other Contractors	12
2.5 Requests from Congress for CBI Disclosure	12
Section 3 – Procedures for Secure Use of CBI Materials	12
3.1 Platforms for Accessing CBI (Authorized Systems)	12
3.1.1 Electronic Greenhouse Gas Reporting Tool (e-GGRT) Servers	12
3.1.2 CBI terminals Outside of the CBI Room	13
3.1.3 CBI terminals Inside the CBI Room – E-GGRT Workstations	13
3.1.4 CBI room – Verification Tool Workstation	14
3.1.5 CBI Room	15
3.2 Contractor CBI Procedures	15
3.3 Maintenance and Enforcement	15
3.4 Receipt of CBI	15
3.4.1 Hardcopy Materials	15
3.4.2 Electronic Materials	15
3.5 Storage of CBI	16
3.5.1 Hardcopy Materials	16
3.5.2 Electronic Materials	16
3.6 Removal of CBI from Safeguarded Areas	16
3.6.1 Hardcopy Materials	16
3.6.2 Electronic Materials	16
3.7 Labeling of CBI	16
3.7.1 Hardcopy Materials	16
3.7.2 Electronic Materials	16
3.8 Discussions of CBI	17
3.9 Accessing CBI from an Alternate Work Location	17
3.10 Reproducing CBI	17
3.10.1 Hardcopy Materials	17

3.10.2 Electronic Materials	17
3.11 Transferring CBI to an Authorized User	17
3.11.1 Between EPA employees	17
3.11.2 Between an EPA Employee and a Contractor	18
3.11.3 Between an EPA Employee and a Non-EPA Federal, State, or Local Agency.....	18
3.12 Destruction of CBI	18
3.12.1 Hardcopy Materials.....	18
3.12.2 Electronic Materials	18
3.13 Sanitizing CBI.....	18
3.14 Tracking CBI.....	19
3.14.1 Hardcopy Materials.....	19
3.14.2 Electronic Materials	19
Section 4 – Violations & Unauthorized Disclosures	19
4.1 Definition of Security Violations	19
4.1.1 For EPA Employees and Other Government Agency Employees.....	19
4.1.2 For contractors.....	19
4.2 Procedures for Reporting Violations of this Policy	19
4.2.1 Oral Report.....	19
4.2.2 Written Report	20
Section 5 – GHGRP CBI Covered by this Policy	20
5.1 Greenhouse Gas Report Program (GHGRP) Data	20
5.2 Electronic Greenhouse Gas Reporting Tool (e-GGRT) Data	21
5.3 E-GGRT Verification Tool Results & Data	21
5.4 Best Available Monitoring Method (BAMM) Data.....	21
Section 6 – Glossaries	21
6.1 Glossary of Acronyms	21
6.2 Glossary of Terms.....	22
Section 7 – Appendices	22
7.1 List of Relevant Rules	22

Section 1 – Confidential Business Information (CBI) Policy Introduction, References, & Responsibilities

1.1 Overview and Purpose

The purpose of this policy is to establish procedures to control and protect Confidential Business Information (CBI) received by EPA as part of the Greenhouse Gas Reporting Program (GHGRP) (40 CFR Part 98). For more information on GHGRP CBI covered by this policy, please see Section 5 of this document.

The provisions in this policy are designed to protect the confidential information entrusted to EPA and to ensure that employees and contractors are aware of the importance of adhering to the procedures for handling CBI, their personal responsibilities in doing so, and the consequences for failing to do so. When situations not specifically addressed in this policy arise, the obligation to protect CBI materials entrusted to EPA continues and must be guaranteed. For these unspecified instances, additional protections may be recommended or required at the appropriate time by the CBI Administrator or Office of Air & Radiation (OAR) management. If any such instances fall outside of the scope of this document, the document will be updated or amended to reflect these new protections.

In general, for access purposes, CBI related to the GHGRP is stored and handled at Environmental Protection Agency (EPA) Headquarters building located at 1310 L Street Northwest, Washington, District of Columbia (D.C.) 20005. Any electronic GHGRP CBI submitted to the Office of Transportation and Air Quality (OTAQ) will be covered by the OTAQ CBI Rules of Behavior (or other relevant OTAQ CBI policy). If this CBI is subsequently transferred into the CBI Administrator, it will then follow the requirements of this policy. EPA may approve, store, and handle CBI at other locations and facilities, such as EPA Regional Offices, other federal agencies, and contractor and subcontractor facilities. Customization of security and control procedures may be necessary depending on local circumstances; however, secure protection of the CBI must be in place. The need to safeguard CBI cannot be overstated. Valid and secure CBI procedures are essential to EPA's rulemaking mandate.

Any material or information categorized as CBI will be treated as such by EPA and its contractors and subcontractors in accordance with the provisions of 40 Code of Federal Regulations (CFR) Part 2. This policy does not address what is considered CBI under the GHGRP or how CBI is determined or claimed. Agency regulations governing the treatment of CBI information appear at 40 CFR Part 2. This policy conforms to all requirements set forth in those regulations, including the recently amended sections of 40 CFR 2.301. For updated information on EPA's GHGRP CBI determinations and other associated regulations, please visit the following website: <http://www.epa.gov/climatechange/emissions/CBI.html>.

1.2 Guidance Policies & Related Documents

1.2.1 EPA 40 CFR Part 2

40 CFR Part 2 contains the regulations that EPA follows in processing requests for records under the Freedom of Information Act (FOIA), 5 U.S.C. 552. Subpart B of Part 2 contains regulations that EPA follows in processing Freedom of Information (FOI) requests for records submitted to it as CBI, as well as other potential public disclosure of such records. 40 CFR 2.301(d) was amended on May 26, 2011 (Federal Register, Vol. 76, No. 102, Page 30782-30818)

1.2.2 EPA Information Security Manual (ISM)

EPA Office of Environmental Information (OEI) Information Security Manual (ISM) (Document # 2195A1, 1999 Edition) establishes EPA's information security policy. The primary objectives of the ISM are to:

- Set forth the requirements and provide guidance for securing EPA information resources in accordance with EPA and Federal security policies and mandates.
- Define the security responsibilities of all personnel who use Agency information or use, develop, operate, or maintain EPA information systems.

1.2.3 Greenhouse Gas Reporting Program (GHGRP) System Security Plan (SSP)

The GHGRP SSP was developed to describe the security controls in place as required by Title III of the E-Government Act of 2002 - Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, et seq. The system has successfully completed EPA's certification and accreditation process, required by FISMA.

1.3 Responsibilities

1.3.1 EPA Employees

Every EPA employee with access to GHGRP CBI (hereafter in this document "CBI") is personally responsible for adhering to the handling and security procedures applicable within this policy. Each employee who has access to CBI is required to complete the approvals, training, and certification processes defined in this policy and to report immediately, both verbally and in writing, any violation of this policy to the CBI Administrator, whose role is further defined in Section 1.3.3 of this policy.

EPA employees must safeguard all CBI they receive, including CBI from a business or other authorized employee, printed from systems containing CBI, or recorded on magnetic, optical, or other electronic storage medium. Employees must also ensure that memos, notes and reports that are generated by EPA staff and that contain CBI obtained from telephone conversations, visits, inspections, inquiries, or tests are properly safeguarded, as set out in Section 3 of this policy. Each individual employee must identify whether documents in his possession, either submitted by a facility, or newly created by the employee, contain CBI according to regulations in 40 CFR Part 2. If an employee is unable to determine whether a document is CBI, that employee should consult with the CBI Administrator.

1.3.2 GHGRP Contractors and Subcontractors

GHGRP contractors and subcontractors (generally, "contractors") that have access to CBI must establish CBI policies and procedures that adhere to the handling and security procedures defined in this policy in addition to those in 40 CFR 2.211(d) and 40 CFR 2.301(h)(2). Such policies must have at least the same level of security and risk mitigation as this policy and must be submitted to the CBI Administrator. Each contractor who has access to CBI is required to report, verbally and in writing, any potential violations of this policy to their EPA Contracting Officer (CO) and the CBI Administrator. These requirements are further outlined in Section 4.2. This policy will also be included in the contracts and/or task orders that require access to GHGRP CBI.

Contractors must safeguard all CBI received from EPA, printed from systems containing CBI, or recorded on magnetic, optical, or other electronic storage medium. Contractors must also ensure that memos, notes and reports containing CBI obtained from telephone conversations, visits, inspections, inquiries, or tests are protected as CBI.

A contractor should consult with their EPA CO, Contracting Officer Representative (COR), or the CBI Administrator with any questions regarding whether a document contains CBI.

Contractors must ensure that any subcontractors comply with the provisions contained within this policy and include this policy in any relevant subcontracts.

1.3.3 CBI Administrator

The CBI Administrator is responsible for approving and managing access to GHGRP CBI; maintaining records of any changes made to this policy or CBI access platforms, as well as records of contractor or other access to CBI; assisting with the identification of what is (and what is not) considered CBI; tracking EPA CBI training; providing a central point of contact for violation reporting; performing periodic compliance audits; and keeping this policy up-to-date. The CBI Administrator will be named by the Greenhouse Gas Reporting Branch Chief (OAP). The CBI Administrator's duties and authority may be delegated to the Alternate CBI Administrator, defined below, during any period of CBI Administrator absence or unavailability.

1.3.4 Alternate CBI Administrator

Any responsibility or authority assigned to the CBI Administrator in this policy is granted to the Alternate CBI Administrator when delegated or requested by, or in the absence or unavailability of, the CBI Administrator. The Alternate CBI Administrator will be named by the Greenhouse Gas Reporting Branch Chief.

1.3.5 EPA Management

EPA management, including the Greenhouse Gas Reporting Branch Chief and Climate Change Division Director (OAR), is responsible for (1) providing necessary resources to safeguard CBI, including training for all EPA personnel and (2) ensuring that this policy is properly implemented and that personnel are held accountable for their actions related to CBI.

EPA management must ensure the following:

- Adequate personnel are available to carry out the CBI Administrator's responsibilities;
- Proper physical control measures are implemented in areas where CBI is maintained;
- Employees under their supervision who require CBI access meet all necessary security requirements;
- Training relevant to safeguarding CBI is required for all EPA personnel who handle CBI

1.3.6 Contracting Officer (CO)

Contracting Officers are responsible for ensuring compliance with CBI clauses within the respective contracts.

1.3.7 Contracting Officer Representative (COR)

The COR, in cooperation with the CO, is responsible for maintaining oversight on contractors' adhering to this policy as practicable.

1.3.8 EPA OEI National Computing Center (NCC)

EPA's NCC provides large-scale computing services for EPA nationwide. NCC also supports regulatory program offices and administrative activities, as well as advanced supercomputing for scientific research in air quality protection and other environmental studies. NCC is responsible for providing technical support for computing resources that contain CBI and will host the server that will contain GHGRP CBI.

NCC personnel must protect CBI in accordance with 40 CFR part 2 and following required security procedures and safeguards.

1.4 Application

1.4.1 Electronic – Greenhouse Gas Reporting Tool (E-GGRT)

E-GGRT is the electronic application that supports facility and supplier reporting for the GHGRP covered in 40 CFR Part 98. E-GGRT is configured to allow only authorized staff, including both EPA employees and contractors, access to CBI. In addition, it is designed to allow authorized GHGRP reporters using e-GGRT to have access to only the information that they submit.

1.5 Types of CBI Materials

1.5.1 Hardcopy Materials

This includes: printed material, paper, microfiche, faxes, letters, printouts, and recorded material and is covered under 40 CFR 2.201(j).

1.5.2 Electronic Materials

This includes: electronic data on a variety of media such as USB drives, CDs, hard drives, DVDs, and recorded material and is covered under 40 CFR 2.201(j).

Section 2 – CBI Access Authority

2.1 Eligibility for Access

2.1.1 Need-to-Know

No person has a right of access to CBI by virtue of title or position alone. Only employees and contractors who need the record or information for the performance of their duties are permitted to access CBI. In order to have access to specific CBI, individuals must have received all the necessary approvals, including appropriate training, as defined in this policy. Access by individuals to CBI is ultimately determined by EPA supervisors, such as a Branch Chief or Division Director.

2.1.2 Policy Acknowledgement

All authorized employees and contractors are required to sign a policy acknowledgement before being granted access to CBI. If there are significant revisions to the policy or the required acknowledgement, employees and contractors must sign the updated policy acknowledgement within 90 days after its release. Annual recertification of this acknowledgment by all users is required.

2.2. Awareness Training

2.2.1 EPA Employee Training Requirements

All EPA employees with access to CBI data must be trained regarding the requirements in this policy prior to accessing CBI, and on an annual basis. The CBI Administrator must provide and track the annual training requirement. Failure to complete the necessary training in a timely manner will prevent access to CBI by that individual.

2.2.2 Contractor Training Requirements

Contractors who need to access CBI must provide training to all contract staff prior to accessing CBI and annually thereafter. Records of training must be provided to the CBI Administrator and the CO or COR.

2.2.3 Other Personnel Granted CBI Access

Any other personnel who need to access CBI in the course of their official duties must take training developed to meet the requirements of this policy before being granted access to CBI and annually thereafter. Records of training must be provided to the CBI Administrator. Failure to complete the necessary training in a timely manner will bar that individual from access to CBI.

2.3. CBI Access Procedures

2.3.1 Rooms and Systems

2.3.1.1 CBI Room

Access to the GHGTP CBI room (for information submitted under Part 98) located at EPA Headquarters (1310 L Street Northwest, Washington, D.C. 20005) is managed by the CBI Administrator. Employees and contractors must request access to the CBI room and each individual's initial application for access must be approved by both the employee's supervisor and the CBI Administrator. The CBI Administrator must verify that the employee or contractor has a need-to-know, has signed the required policy acknowledgement, and has completed the required training. Once all requirements have been met, access to the CBI room may be authorized by the CBI Administrator. Access includes knowledge of the CBI Room door code, access to the CBI room file cabinet key, and knowledge of other access safeguards, as required. Staff located at other EPA or contractor facilities may use other CBI rooms for the purpose of accessing GHGRP CBI and must have access authorization procedures in place in such a CBI room that meet or exceed those identified here, as well as a written policy that has been submitted to the CBI Administrator.

2.3.1.2 CBI Terminals Located Outside of the CBI Room

Employees at EPA facilities who have a need-to-know may have terminals in their offices to view CBI data. Access to the CBI terminals outside of the CBI room must be managed by the CBI Administrator. Each individual's initial application for EPA employee access must be approved by both the employee's supervisor and the CBI Administrator. The CBI Administrator must verify that the employee has a need-to-know, has signed the required policy acknowledgement, and has completed the required training. Once all requirements have been met, access to the CBI terminal may be authorized by the CBI Administrator. Access includes username and password establishment on a CBI Terminal computer to be located in the employee's workspace / office and knowledge of other access safeguards, as required. CBI terminals outside of the CBI room at other EPA facilities may be created and must have access authorization procedures in place that meet or exceed those identified here.

2.3.1.3 CBI Terminals Located Inside of the CBI Room

Access to the CBI terminals inside of the CBI room located at EPA Headquarters building, as specified above, are managed by the CBI Administrator. EPA employees and contractors must request access to the CBI terminals inside of the CBI room and each individual's initial application for access must be approved by both the employee's supervisor and the CBI Administrator. The CBI Administrator must verify that the employee or contractor has a need-to-know, had signed the required policy agreement, and has completed the required training. Once all requirements have been met, access to the CBI terminal may be authorized by the CBI Administrator. Access includes username and password

establishment on the appropriate CBI room computer(s) and knowledge of other access safeguards, as required. CBI terminals inside of a CBI room at other EPA or contractor facilities may be utilized and must have access authorization procedures in place that meet or exceed those identified here, as well as a written policy that has been provided to the CBI Administrator.

2.3.2 Eligible Authorized Users

2.3.2.1 EPA Employees

Any EPA employee with a need-to-know who participates in the implementation or enforcement of the GHGRP is eligible to have access to CBI.

2.3.2.2 State or Local Government Agency

CBI may be provided to state or local government agencies provided that the requirements at 40 CFR 2.301 (h)(3) are satisfied. The CBI Administrator shall maintain records of any CBI released to state or local governments as well as documentation that the appropriate requirements are met. The authorized personnel that release CBI to a state or local government agency must notify the CBI Administrator. The state or local government agency must sign an acknowledgement of CBI receipt stating that they agree to safeguard the CBI.

2.3.2.3 Other Federal Agencies

CBI may be provided to other Federal agencies in accordance with 40 CFR 2.209(c). The CBI Administrator shall maintain records of any CBI released to other federal agencies as well as documentation that the appropriate requirements are met. The authorized personnel that release CBI to another federal agency must notify the CBI Administrator. The other federal agencies may sign an acknowledgement of CBI receipt stating that they agree to safeguard the CBI before being granted access.

2.3.2.4 NCC Contractors

NCC contractors conduct maintenance on CBI resources as a part of their normal job responsibilities, which include maintaining the server that hosts e-GGRT's CBI data. Under the terms of their contracts, NCC contractors are responsible for safeguarding CBI on the systems they maintain.

2.3.2.5 Other Contractors

Contractors who perform work for EPA may be designated authorized representatives of EPA in accordance with 40 CFR 2.301(h). As authorized representatives, contractors may be granted access to CBI pursuant to the requirements established by the provisions in that regulation. When disclosure is necessary, contractors must abide by the contract clauses that address the treatment of confidential information from the Environmental Protection Agency Acquisition Regulations (EPAAR) 1552.235-71 - "Treatment of Confidential Business Information" - http://edocket.access.gpo.gov/cfr_2006/octqtr/pdf/48cfr1552.235-71.pdf).

2.4 Relinquishment / Termination of Access Procedures

Access to CBI must be terminated or relinquished when one of the following occurs:

- The authorized individual no longer needs access to CBI data to perform their job responsibilities
- The authorized individual has violated this policy

2.4.1 EPA Employees

To terminate or relinquish access, the employee and / or their supervisor should notify the CBI Administrator. Upon notification, access by that individual to CBI must be ended within one business day. All hardcopies of CBI must be given to the CBI Administrator and returned to the CBI room. In addition, the CBI Administrator must conduct annual reviews of the list of employees with access, document the review, and address any issues identified within two weeks of the review date.

2.4.2 Other Federal Agencies

To terminate or relinquish access, the agency employee and / or their supervisor should return all hardcopy CBI to the CBI Administrator or notify the CBI Administrator that the CBI has been destroyed. If applicable, the CBI Administrator shall ensure that all CBI provided to the agency is returned within two business days.

2.4.3 NCC Contractors

NCC contractors must follow EPA NCC's operating procedures for terminating access in a timely manner.

2.4.4 Other Contractors

To terminate or relinquish access, the CBI Administrator shall act to remove all access methods from contractor facilities and notify the CO. If applicable, the CBI Administrator shall ensure that access to CBI on EPA controlled resources has been removed within one business day. Any hardcopy CBI material must either be returned to the CBI Administrator within two business days or destroyed using an acceptable method, per Section 3.12 of this policy. The CO must be notified of the return or destruction by the appropriate party. In addition, annual reviews of contractors with access to CBI must be documented, and any issues identified must be remediated in a timely manner. The contractor should have procedures in place to remove access to any CBI located at contractor controlled facilities.

2.5 Requests from Congress for CBI Disclosure

Requests for CBI from Congress are processed in accordance with 40 CFR 2.209.

Section 3 – Procedures for Secure Use of CBI Materials

3.1 Platforms for Accessing CBI (Authorized Systems)

3.1.1 Electronic Greenhouse Gas Reporting Tool (e-GGRT) Servers

3.1.1.1 Description

E-GGRT is a web-based reporting system that supports implementation of the GHGRP under 40 CFR 98, by facilitating GHG reporting for sources making regulatory submissions under the GHGRP. E-GGRT servers also may be used to store other CBI related to the GHGRP. Examples are provided in Section 5 of this document.

3.1.1.2 Safeguards

The necessary safeguards for information in e-GGRT are documented in the e-GGRT System Security Plan (SSP), which is maintained and enforced by the e-GGRT system manager, the Office of Air & Radiation Information Security Officer (ISO) and the e-GGRT ISO.

3.1.1.3 Access

Access to the application must be strictly controlled and comply with the specifications outlined in the e-GGRT SSP and this policy.

3.1.2 CBI terminals Outside of the CBI Room

3.1.2.1 Description

The CBI terminals are computers that are located within access controlled EPA office buildings in the workspaces / offices of authorized users. These terminals provide read-only access to CBI data, allow users to temporary save files, but do not allow users to print hard copies of data.

3.1.2.2 Safeguards

The CBI terminals must be configured to provide access to CBI data. All methods to transfer data from the CBI terminal must be disabled, including USB drives, CD-R/DVD-R drives, printers, e-mail, and any other transfer methods. Access and file permissions must be implemented to prevent users from permanently saving any data to the individual terminal. The CBI Administrator is responsible for ensuring these safeguards are in place.

Network access for these terminals must be restricted to e-GGRT data only and prevent access to the general internet. Monitors must be configured to restrict unauthorized viewing of the data presented, such as using a monitor privacy screen / filter or positioning a monitor to limit viewing from doors, windows, or other office openings. The terminals must have full disk encryption with pre-boot authentication and comply with the Federal Information Process Standard (FIPS) 140-2. This is part of the standards that govern utilization and management of computer and related telecommunications systems in the Federal government. End users must only be permitted to use a web browser and all other applications must be disabled, removed, or otherwise restricted. The computer must automatically lock or logoff a user after a period of inactivity (less than 10 minutes) and must require the user to re-authenticate before being granted access to the original session.

CBI terminals outside of the CBI room at other EPA facilities may be created and must have safeguards in place that meet or exceed those identified here.

3.1.2.3 Access

Access to these terminals must be controlled with username and password. The password configuration must meet EPA password standards, as defined in EPA OEI's Information Security Manual (ISM). End users must lock or logoff the computer when not in use or when they are not using it for any period of time.

3.1.3 CBI terminals Inside the CBI Room – E-GGRT Workstations

3.1.3.1 Description

The CBI room contains multiple computers used to access CBI data. These computers provide additional functionality compared to the CBI terminals located outside of the CBI room described above. Users are permitted to store data locally only and print hard copies of data.

3.1.3.2 Safeguards

These terminals must be configured with the same safeguards as the CBI terminals outside of the CBI room except that end users are permitted to save data locally. The CBI Administrator is responsible for ensuring these safeguards are in place.

CBI terminals inside of the CBI room at other EPA or contractor facilities may be utilized and must have safeguards in place that meet or exceed those identified here.

3.1.3.3 Access

Access to these terminals must be controlled with username and password. The password configuration must meet EPA password standards, as defined in EPA OEI's Information Security Manual (ISM). End users must only access the applications and resources that are required to perform their job responsibilities. End users must lock or logoff the computer when not in use or when they are not using it for any period of time.

3.1.4 CBI room – Verification Tool Workstation

3.1.4.1 Description

The CBI room contains a single computer running a data verification application or "Verification Tool". The Verification Tool (VT) is an application that downloads data submitted to e-GGRT, performs verification checks and produces reports that display all failed checks (i.e., flags). The goal of this tool is to verify that data submitted through e-GGRT reporting is accurate. The types of checks that the VT will run include ranges, algorithms, statistical tests, and other tests as needed.

This computer will be used to upload electronic files from external media sources (i.e. USB drives, CD-R/DVD-R drives) to the e-GGRT system. Examples of when portable electronic files containing CBI may exist include CBI data storage that predates this policy and CBI submissions from outside parties that pertain to the GHGRP but are not part of the reporting data (i.e. supporting documents). If an authorized user needs to upload an electronic file to the e-GGRT system, they should contact the CBI Administrator.

3.1.4.2 Safeguards

For the VT system, USB drives, CD-R/DVD-R drives, and any other electronic transfer methods will be enabled. VT Administrators, the CBI Administrator, and a select group of VT personnel will be given access to this system and are subject to all training and certification requirements covered in this policy. The physical computer system for this system will be stored in a locked cabinet. Only approved VT administrators will have access to this cabinet. The CBI Administrator must approve access for individuals to the VT system separately from the other systems in the CBI room, and only those with job duties that relate to the VT workstation operation will be granted access.

The terminal must have full disk encryption with pre-boot authentication and comply with the Federal Information Process Standard (FIPS) 140-2. This is part of the standards that govern utilization and management of computer and related telecommunications systems in the Federal government. . The computer must automatically lock or logoff a user after a period of inactivity (less than 10 minutes) and must require the user to re-authenticate before being granted access to the original session.

The VT software has access to annual reports that are submitted to EPA. It will process all of the CBI data in the annual reports. Furthermore, the VT will generate output reports in PDF format that may contain data designated as CBI by EPA.

3.1.4.3 Access

Access to these terminals must be controlled with username and password. The password configuration must meet EPA password standards, as defined in EPA's Information Security Manual (ISM). End users must be granted access only to the applications and resources that are required to perform their job responsibilities. Users must lock or logoff the computer when not in use.

3.1.5 CBI Room

3.1.5.1 Description

The CBI room is designed to house terminals and hard copy materials that contain CBI.

3.1.5.2 Safeguards

The CBI room must be a physically separate office or area and all doors or access points must have a cipher lock or similar mechanism to prevent unauthorized access. The physical security measures must provide reasonable assurance that access to unauthorized personnel will be prevented.

CBI rooms at other EPA or contractor facilities may be created and must have access authorization procedures in place that meet or exceed those identified here.

3.1.5.3 Access

Access to the CBI room must be controlled by cipher lock or similar mechanism. The combination / passcode utilized must be strong and provided to only authorized users. The combination / passcode must be changed at least annually by the CBI Administrator.

3.2 Contractor CBI Procedures

Contractors with access to CBI are required to have safeguards and procedures that meet or exceed the requirements set forth in this policy. These safeguards and procedures must be documented and submitted to the CBI Administrator and contract CO. If appropriate safeguards and procedures cannot be implemented, then contract staff will be required to access CBI only at EPA authorized facilities and in accordance with the requirements in this policy.

3.3 Maintenance and Enforcement

This policy will be reviewed annually by the CBI Administrator and approved by the Greenhouse Gas Reporting Branch Chief and Climate Change Division Director. All major changes must be approved by these two EPA management personnel. All affected parties must be notified of any revisions in a timely manner.

3.4 Receipt of CBI

3.4.1 Hardcopy Materials

All hardcopy CBI received must be placed into the CBI room as soon as possible but no later than close of business on the day of receipt. Envelopes marked as "CONFIDENTIAL BUSINESS INFORMATION" should not be opened, and coversheets not removed, until the hardcopy material is located within the CBI room or other location where it can be securely reviewed.

3.4.2 Electronic Materials

All electronic CBI received must be stored on authorized systems, as defined above, immediately after receipt. These systems include only e-GGRT and the computers permanently located within the CBI room. CBI data not submitted through e-GGRT and received on electronic media (USB drive, CD-R, DVD-R, etc.) should be physically secured using continuous personal possession or a locked security mechanism until it can be placed into the CBI room. Upon receipt, all electronic media containing CBI must be checked-in to the CBI room by the authorized recipient. Viewing of electronic media that contains CBI outside of the authorized systems, as defined above, is prohibited.

3.5 Storage of CBI

3.5.1 Hardcopy Materials

Folders, documents, and other hardcopy material containing CBI must be secured within the CBI room. Temporary storage of CBI outside of the CBI room is permitted during business hours as long as the documents are in the physical custody of an authorized person or the documents are secured in a locked cabinet or storage area within a secure facility. Storage of CBI outside of the CBI room over one or more nights is permissible only in situations where hardcopy CBI is needed off-site for official purposes, such as discussions with GHGRP reporters or enforcement activities. In such cases, the reason for prolonged removal of hardcopy CBI must be stated in the CBI room log, along with the projected date of return.

3.5.2 Electronic Materials

All electronic CBI must be stored on authorized systems at all times. These systems include e-GGRT and the computers located within a CBI room. If CBI data is stored for any reason on electronic media (USB drive, CD-R, DVD-R, etc.), it must be housed in a CBI room using the requirements above for hardcopy materials.

3.6 Removal of CBI from Safeguarded Areas

3.6.1 Hardcopy Materials

Hardcopy CBI may be removed from the CBI room during working hours. Hardcopy CBI must be checked out by the authorized user using the CBI Room log. When removing hardcopy materials from the CBI room, individuals must use a cover page or similar device to protect the CBI material from unauthorized viewing when not in use. Hardcopy material must stay in the authorized user's possession at all times or appropriately secured and returned to the CBI room when it is no longer needed or at the end of each business day, whichever is earlier. When unauthorized persons are present, CBI documents must be covered, turned face down, removed from the area, or otherwise protected. Proper labeling procedures, detailed below, must also be followed. Hardcopy CBI must be returned to the CBI room at the end of the business day, checked-in on the log, and cannot be stored in locked office space or a similar environment overnight or on weekends.

3.6.2 Electronic Materials

Electronic CBI data must not be removed from authorized systems as defined above. Standard EPA workstations are not permitted to store CBI either permanently or temporarily.

3.7 Labeling of CBI

3.7.1 Hardcopy Materials

All hardcopy material that contains CBI must be stamped with "CONFIDENTIAL BUSINESS INFORMATION" on the cover page, at a minimum. Any hardcopy material with CBI must be protected in a folder or with a cover sheet also marked "CONFIDENTIAL BUSINESS INFORMATION" before being removed from the CBI room.

3.7.2 Electronic Materials

All systems that contain or can access CBI must be labeled "CONFIDENTIAL BUSINESS INFORMATION" in a conspicuous place on the computer case. This requirement does not extend to systems located within EPA NCC data centers.

3.8 Discussions of CBI

All discussions, both in person and on the phone, of CBI should be protected from unauthorized personnel. Authorized employees and contractors must take care to ensure their discussions are not overheard by unauthorized people. This includes limiting discussions to the CBI room, in an office or conference room, or similar method. When discussing CBI over the phone, the calling party must use reasonable measures to validate the identity of the recipient. This includes validating the identity of GHGRP reporters when discussing their own CBI submissions with them.

3.9 Accessing CBI from an Alternate Work Location

Accessing hardcopy or electronic CBI from an alternate work location is not permitted under any circumstances.

3.10 Reproducing CBI

3.10.1 Hardcopy Materials

Reproduction (i.e. copies) of hardcopy documents containing CBI must be kept to a minimum and copies may be made only when absolutely necessary. Copies or additional printouts of documents must be performed within the CBI room. Copies must not be made outside of the CBI room. All copies of CBI must be noted separately in the CBI room log.

3.10.2 Electronic Materials

Reproduction of electronic data containing CBI must be kept to a minimum and avoided whenever possible. The protection of the copied data must be at least as rigorous as that for the original.

3.11 Transferring CBI to an Authorized User

3.11.1 Between EPA employees

3.11.1.1 Hardcopy Materials

All hardcopy CBI must be transferred in person, through interoffice mail, or via private carrier. If using a private carrier, the package must be traceable and the recipient must sign for the package in-person. If utilized, envelopes or other packaging materials must be completely sealed using the double envelope/packing method, which is defined as follows: The outside envelope must have the recipient's address along with text stating that the package should only be opened by the addressee. The inside envelope must be labeled as "CONFIDENTIAL BUSINESS INFORMATION" and also have the recipient's name and address.

3.11.1.2 Electronic Materials

Authorized users of e-GGRT are permitted to transfer CBI within the authorized systems. Transfer of CBI data between authorized users on portable media (USB drive, CD-R, DVD-R, etc.) or via e-mail is prohibited at all times with one exception: Transferring electronic CBI that is not submitted using the e-GGRT system through the Verification Tool computer is allowed. This transfer exception should be used only when no other option is available for electronic viewing of CBI data. A transfer of this type will be completed by the CBI Administrator. The portable media device used must be scanned for viruses and other computer hazards prior to transferring the data to the e-GGRT CBI system.

3.11.2 Between an EPA Employee and a Contractor

3.11.2.1 Hardcopy Materials

All hardcopy CBI must be transferred in person or by private carrier. If using a private carrier, the package must be traceable and the recipient must sign for the package in-person. If utilized, envelopes or other packaging materials must be completely sealed using the double envelope/packing method. The outside envelope should have the recipient's address along with text stating that the package should only be opened by the addressee. The inside envelope must be labeled as "CONFIDENTIAL BUSINESS INFORMATION" and also have the recipient's name and address.

3.11.2.2 Electronic Materials

Authorized users of e-GGRT are permitted to transfer CBI within the system. Transfer of CBI data between authorized users on portable media (USB drive, CD-R, DVD-R, etc.) or through e-mail is prohibited at all times.

3.11.3 Between an EPA Employee and a Non-EPA Federal, State, or Local Agency

3.11.3.1 Hardcopy Materials

All hardcopy CBI must be transferred in person or by private carrier. If using a private carrier, the package must be traceable and the recipient must sign for the package in-person. If utilized, envelopes or other packaging materials must be completely sealed using the double envelope/packing method. The outside envelope should have the recipient's address along with text stating that the package should only be opened by the addressee. The inside envelope should be labeled as "CONFIDENTIAL BUSINESS INFORMATION" and also have the recipient's name and address.

3.11.3.2 Electronic Materials

Electronic transfer of CBI to another federal agency or a state or local agency is subject to the terms of existing EPA regulations, such as 40 CFR part 2, and this policy.

3.12 Destruction of CBI

3.12.1 Hardcopy Materials

All hardcopy data that is no longer used or required must be either stored in the CBI room or securely destroyed. Hardcopy data must be shredded, burned, or destroyed using a similar method that prevents the data from being read or recreated. On the day that the destruction occurs, the destruction must be noted in the CBI room log or the CBI Administrator must be notified by the person who destroyed the document.

3.12.2 Electronic Materials

All electronic CBI data that is no longer used or required must be securely erased or the media containing the data must be securely destroyed. Software used to erase the data must meet the Department of Defense (DoD) Standard 5220.22-M standard. Electronic media must be shredded, burned, degaussed, or destroyed using a similar method that prevents the data from being read or recreated. On the day that the destruction occurs, the destruction must be noted in the CBI room log or the CBI Administrator must be notified by the person who destroyed the media.

3.13 Sanitizing CBI

Either all CBI data elements must be removed or the data must be sufficiently aggregated that it protects the CBI in order to sanitize a document (electronic or hardcopy). The responsibility for

determining whether documents contain CBI rests with the document's owner, who must be an authorized user with CBI access as defined in this policy. All documents must be reviewed by both the originator and one other person with CBI access authority to ensure that they are appropriately sanitized. Authorized employees and contractors should consult with their supervisor or the CBI Administrator with any questions regarding whether a document contains CBI.

3.14 Tracking CBI

3.14.1 Hardcopy Materials

All hardcopy CBI must be tracked when one of the following actions occurs: (1) receipt and storage within the CBI room, (2) removal from the CBI room, (3) transfer to another authorized person, (4) destruction, or (5) reproduction. The following items must be tracked for each action: name, signature, date/time checked in, data/time checked out, document name, received from, transferred to, disposition, and notes. It is the responsibility of the authorized personnel in possession of the hardcopy document to provide this information.

3.14.2 Electronic Materials

All electronic CBI must be tracked when one of the following actions occurs: (1) receipt and storage within the CBI room, (2) destruction, or (3) reproduction. The following items must be tracked for each action: name, signature, date/time checked in, media type, media name, received from, disposition, and notes. It is the responsibility of the authorized personnel in possession of the electronic data to provide this information.

Section 4 – Violations & Unauthorized Disclosures

4.1 Definition of Security Violations

4.1.1 For EPA Employees and Other Government Agency Employees

Requirements related to security violations for unauthorized disclosure of CBI are set out in 40 CFR 2.211 and are governed by the Trade Secrets Act, 18 U.S.C. 1905. These requirements apply to EPA employees and other government agency employees.

After a finding of a likely violation of the rules in this policy, the appropriate party must follow the reporting procedures outlined in Section 4.2 of this policy.

4.1.2 For contractors

Contractors are responsible for ensuring compliance with this policy and the CBI clauses within their respective contracts. Failure to comply with the provisions in the CBI clauses may be considered a material breach of contract.

4.2 Procedures for Reporting Violations of this Policy

4.2.1 Oral Report

Any employee of EPA, another Federal agency, or a contractor with access to CBI shall report, at least verbally within one working day if he or she thinks it is possible that:

- A CBI protection procedure has been violated.
- CBI is unaccounted for.
- CBI may have been disclosed to a person not authorized to receive it.

EPA and other federal employees must provide oral notice to their Branch Chief (or equivalent supervisor in their organization) and the CBI Administrator. Contractors with access to CBI must provide oral notice to their EPA CO, their EPA COR, and the CBI Administrator within one business day, if any of the above situations occur. The EPA CO or COR must then report to their Branch Chief (or equivalent manager in their organization) within one business day.

4.2.2 Written Report

In addition, Federal and contractor employees shall file a written report within 2 business days in any of the same situations identified above (unless otherwise relieved of the requirement by the supervisor who received the oral report). EPA and other federal employees must provide this written report to their Branch Chief and Division Director (or equivalent supervisor in their organization) and the CBI Administrator. Contractor employees must provide the written report to their CO, COR and the CBI Administrator.

The written report shall include any relevant circumstances or facts known by the employee or contractor, and describe any of the following:

- Possible violation of procedures.
- Possible unauthorized disclosure of CBI.
- Materials possibly unaccounted for.

The employee's Division Director (or equivalent) must review the report and, within 2 business days of receiving the report, refer the report to the CBI Administrator with their findings. If the Division Director reviews the employee's report and determines there was no violation of procedures, loss of CBI, or unauthorized disclosure, the report need not be referred. The Division Director is encouraged to consult with the CBI Administrator and other relevant management during this process.

Section 5 – GHGRP CBI Covered by this Policy

This section provides examples of the types of material that may contain CBI and are covered by this policy. This section is not designed to include all areas of CBI covered, but is provided as an example to personnel who must comply with the policy. CBI data that was in the possession of an authorized user prior to the approval of this policy may be incorporated into this policy at the discretion of EPA management. Any application of this policy to existing CBI documents will be completed within 3 months of this policy's approval.

5.1 Greenhouse Gas Report Program (GHGRP) Data

In response to the FY2008 Consolidated Appropriations Act (H.R. 2764; Public Law 110–161), EPA issued the Mandatory Reporting of Greenhouse Gases Rule (74 FR 5620) which requires reporting of GHG data and other relevant information from large sources and suppliers in the United States. The purpose of the rule is to collect accurate and timely GHG data to inform future policy decisions. In general, the Rule is referred to as 40 CFR Part 98. Implementation of 40 CFR Part 98 is referred to as the Greenhouse Gas Reporting Program (GHGRP).

Suppliers of certain products that would result in GHG emissions if released, combusted or oxidized; direct emitting source categories, and facilities that inject carbon dioxide underground, are covered in Part 98. In general, facilities that emit 25,000 metric tons or more per year of GHGs are required to

submit annual reports to EPA. Part 98 was published in the Federal Register (www.regulations.gov) on October 30, 2009 under Docket ID No. EPA-HQ-OAR-2008-0508-2278 and was amended through several follow-up rulemakings that amended requirements for existing source categories or added additional categories for reporting.

5.2 Electronic Greenhouse Gas Reporting Tool (e-GGRT) Data

E-GGRT supports facility and supplier reporting for the GHGRP covered in 40 CFR Part 98. The rule requires electronic reporting of GHG emissions from covered sources and suppliers in the United States. Some of this data is designated as CBI by EPA. In cases where EPA has not yet designated whether or not data is to be considered CBI, the reporter may claim data as CBI. This claim must be substantiated in accordance with the provisions in 40 CFR Part 2.

5.3 E-GGRT Verification Tool Results & Data

The Verification Tool (VT) is an application that downloads data submitted to e-GGRT, performs verification checks, produces output reports that display all failed checks (i.e., flags), and prepares reports. The types of checks that the VT will run include ranges, algorithms, statistical tests, and other tests as needed.

The VT software has read-only access to annual reports that are submitted to EPA. Therefore, the VT will process all of the CBI data in the annual reports. In addition, the VT will generate reports in PDF format that may contain data designated as CBI by EPA, and be properly protected.

5.4 Best Available Monitoring Method (BAMM) Data

The 2009 final rule, in §98.3(d), contained provisions to allow facilities and suppliers to automatically use best available monitoring methods (BAMM) for a period of three months without requesting approval by EPA's Administrator. Facilities and suppliers could extend the use of BAMM through December 31, 2010, by submitting a request to the Administrator outlining the parameters for which extended BAMM was needed and the reason for such request. Subsequent amendments to the 2009 final rule to add additional source categories for reporting also contained similar provisions allowing facilities to request use of BAMM (see 75 FR 39736, 75 FR 74458, 75 FR 74774, 75 FR 75060, and 75 FR 79092). The process of facilities generating the BAMM requests, EPA review of the request, and EPA response to the applicant may involve the transfer of information determined to be CBI.

Section 6 – Glossaries

6.1 Glossary of Acronyms

BAMM	Best Available Monitoring Method
CBI	Confidential Business Information
CCD	Climate Change Division
CD	Compact Disk
CFR	Code of Federal Regulations
CO	Contracting Officer
COR	Contracting Officer Representative
DoD	Department of Defense
DVD	Digital Versatile Disk or Digital Video Disk
e-GGRT	Electronic- Greenhouse Gas Reporting Tool

EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOI	Freedom of Information
FOIA	Freedom of Information Act
GHGRP	Greenhouse Gas Report Program
IRM	Information Resource Management
ISM	Information Security Management
NACI	National Agency Check with Inquiries
NCC	National Computing Center
SOW	Statement of Work
SSP	System Security Plan
USB	Universal Serial Bus

6.2 Glossary of Terms

Confidential Business Information (CBI): Trade secrets and commercial or financial information obtained from a person and privileged or confidential as defined in 5 U.S.C. section 552 (b) (4).

Electronic-Greenhouse Gas Reporting Tool (e-GGRT): E-GGRT is a web-based tool that supports facility and supplier reporting for the Greenhouse Gas Reporting Program (GHGRP).

Greenhouse Gas Reporting Program (GHGRP): In response to the FY2008 Consolidated Appropriations Act (H.R. 2764; Public Law 110–161), EPA issued the GHGRP (40 CFR Part 98), which requires reporting of greenhouse gas (GHG) data and other relevant information from large sources and suppliers in the United States. The purpose of the rule is to collect accurate and timely GHG data to inform future policy decisions.

System Security Plan (SSP): Formal document developed by the system manager that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Terminal: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Section 7 – Appendices

7.1 List of Relevant Rules

- 40 CFR Part 98 – Greenhouse Gas Reporting Rule
- 40 CFR Part 98 Amendment – Change to the Reporting Date for Certain Data Elements Required Under the Mandatory Reporting of Greenhouse Gases Rule - Federal Register Vol. 76, No. 165, Pages 53057-53071
- 40 CFR Part 2 – Protection of Environment – Public Information

- 40 CFR Part 2 Amendment - Confidentiality Determinations for Data Required Under the Mandatory Greenhouse Gas Reporting Rule and Amendments to Special Rules Governing Certain Information Obtained Under the Clean Air Act - Federal Register Vol. 76, No. 102, Pages 30782-30818