Privacy Impact Assessment
for the

Coast Guard Business Intelligence (CGBI) System

DHS/USCG/PIA-018

April 17, 2012

Contact Point
Mr. David Bandel
CGBI Program Manager
United States Coast Guard, CG-0954
(202) 372-4570

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Coast Guard (USCG) owns and operates the Coast Guard Business Intelligence (CGBI) System. CGBI is a Business Intelligence (BI) and mission support tool which provides USCG users with a web-based reporting and analysis capability. CGBI utilizes standardized enterprise data and metrics, consisting of the Enterprise Data Warehouse (EDW), and a front-end BI application providing standardized reports and data cubes. This system was created to provide an integrated reporting and analysis environment for organizational Knowledge and Performance Management by providing "one version of the truth." This Privacy Impact Assessment (PIA) is required as the system contains personally identifiable information (PII) obtained from authoritative, transactional source systems; this data may be transferred or viewed by other personnel or systems upon data sponsor approval, with limited PII data available within the CGBI interface to authorized users.

Overview

By law, the Coast Guard has 11 missions: ports, waterways and coastal security; drug interdiction; aids to navigation; search and rescue; living marine resources; marine safety; defense readiness; migrant interdiction; marine environmental protection; ice operations; and law enforcement. The purpose of the CGBI system is to provide data analysis and reporting capability across all 11 USCG mission areas, including Mission Support and Business Support functions, using standardized data and performance metrics. CGBI's goal is to constantly improve USCG outcomes by providing BI and analysis of USCG activities, performance, capabilities and readiness. Currently, CGBI accesses information from approximately 50 transactional Information Technology (IT) systems within the Department of Homeland Security (DHS), the federal government, and industry to provide USCG a unified data view used for business support and knowledge management. CGBI is a USCG system sponsored by the Office of the Vice Commandant (CG-0954). This project is authorized under the Clinger-Cohen Act of 1996 (40 U.S.C. § 1401(3)), the Government Performance and Results Act of 1993, Executive Order 13011: *Federal Information Technology*; Circular No. A-130: *Management of Federal Information Resources*, and Title 14 U.S.C. § 93 *Commandant; general powers*.

CGBI is designed to provide operational and performance analysis for reporting across all 11 mission areas of the USCG, as well as Mission Support and Business Support functions. Most reports do not depend upon PII. CGBI supports the DHS Intelligence and Warning, Emergency Preparedness and Response, Border and Transportation Security, and Protecting Critical Infrastructure and Key Assets mission areas. CGBI does not share any PII from the general public with any system or agency. A typical user transaction within the CGBI system could be characterized using the "Merchant Mariner Licensing and Documentation (MMLD) Credential Current" cube as an example. Cubes are large, detailed dimensional data constructs similar to the more common pivot table found in spreadsheet software such as Microsoft Excel. The "MMLD Credential Current" cube contains dimensions such as application dates, transaction types, current states and others. Standardized measures such as Average (Avg.) Days Total for Credential, Avg. Days to Current State, Avg. Hours Total for Credential, Avg. Hours to

Current State, Credential Count, Personnel Casualties, Total Days for Credential, Total Days to Current State, Total Hours for Credential, Total Hours to Current States are then applied to the selected data set. This particular cube utilizes data from MMLD to display the status of each Mariner application and credential, their times to reach the current state and total life-cycle time, providing the user a completely customized end data product tailored to the user's specific needs at the time.

CGBI is a read-only system located on the USCG Data Network (One Net). CGBI provides users with a web-based reporting toolset that utilizes standardized USCG-wide enterprise data. This toolset includes the following business lines: views, reports, cubes, and repository analytics. CGBI provides a centralized repository of USCG enterprise information customized for reporting. CGBI receives data required for reporting from authoritative source systems; this data may include PII. Based on requirements, CGBI will use this data to build a product within one of its business lines. CGBI provides system and ad-hoc user access to approved data sets in the EDW. EDW function is to hold a "working" copy of data from different systems and rearrange the data for speed of access by subject, no matter what system it came from, regardless of what architecture the transactional data system used. The internal architectures are completely different. The EDW is the "normalized" source of data for the reporting using the BI tools, but it remains a copy, not the "authoritative" source.

In order to protect privacy, CGBI is limited to all authorized Active Directory (AD) users located on the One Net. Upon program office/customer request, product access can be limited as follows:

- Applications - Measures Repository and Personnel Allowance Amendment (PAA) based on Employee ID (EMPLID) and/or Active Directory (AD) User ID.
- Cubes/Reports - Department ID (DEPTID) or EMPLID.
- Database - Data field or table-level based on authorized user name.

CGBI products containing PII information are marked with a red "FOUO - Privacy Act Sensitive" banner. Back-end users of the EDW must complete a *CGBI Access Authorization Form* and abide by the *CGBI Policies and Procedures* document. The *Access Authorization Form* lists which data elements the user has requested access to and signature approvals from the requestor's supervisor, government supervisor (if contractor), CGBI Authorizing Official and the Source System Owner, Information System Security Officer (ISSO), or Data Steward. Access for that user is then limited to only the approved data elements.

The overall privacy risk associated with CGBI is improper handling or use of PII. Some systems transfer PII from the general public such as name, address and phone number to CGBI, but access to this information is limited to users with a need to know and for official use only. To mitigate improper handling of PII, appropriate access agreements (for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements) are completed for individuals requiring access to organizational information and information systems before authorizing access.

This PIA shall be updated as necessary, when revisions to CGBI occur.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CGBI is authorized under the following legal authorities:

- Title 40 U.S.C. § 1401(3), the Clinger-Cohen Act of 1996. A statute which directs the development and maintenance of IT architectures by federal agencies, to maximize the benefits of IT within the government.

- Government Performance and Results Act of 1993. A statute wherein its purpose is to:

  - improve the confidence of the American people in the capability of the federal government, by systematically holding federal agencies accountable for achieving program results;
  - initiate program performance reform with a series of pilot projects in setting program goals, measuring program performance against those goals, and reporting publicly on their progress;
  - improve federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction;
  - help federal managers improve service delivery, by requiring that they plan for meeting program objectives and by providing them with information about program results and service quality;
  - improve-congressional decision-making by providing more objective information on achieving statutory objectives, and on the relative effectiveness and efficiency of federal programs and spending; and
  - improve internal management of the federal government.

- Executive Order 13011 Federal Information Technology. A Presidential Order establishing policy of the United States government whereas executive agencies shall:

  - significantly improve the management of their information systems, including the acquisition of IT, by implementing the relevant provisions of the Paperwork Reduction Act of 1995 (Public Law 104-13), the Information Technology Management Reform Act of 1996 (Division E of Public Law 104-106) "(Information Technology Act)", and the Government Performance and Results Act of 1993 (Public Law 103-62);

- refocus information technology management to support directly their strategic missions, implement an investment review process that drives budget formulation and execution for information systems, and rethink and restructure the way they perform their functions before investing in information technology to support that work;
- establish clear accountability for information resources management activities by creating agency Chief Information Officers (CIOs) with the visibility and management responsibilities necessary to advise the agency head on the design, development, and implementation of those information systems. These responsibilities include: (1) participating in the investment review process for information systems; (2) monitoring and evaluating the performance of those information systems on the basis of applicable performance measures; and, (3) as necessary, advising the agency head to modify or terminate those systems;
- cooperate in the use of information technology to improve the productivity of federal programs and to promote a coordinated, interoperable, secure, and shared government-wide infrastructure that is provided and supported by a diversity of private sector suppliers and a well-trained corps of information technology professionals; and

- establish an interagency support structure that builds on existing successful interagency efforts and shall provide expertise and advice to agencies; expand the skill and career development opportunities of information technology professionals; improve the management and use of information technology within and among agencies by developing IT procedures and standards and by identifying and sharing experiences, ideas, and promising practices; and provide innovative, multi-disciplinary, project-specific support to agencies to enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.

- Circular No. A-130. An Office of Management and Budget Circular that establishes policy for the management of Federal Information Resources.

- Title 14 U.S.C. § 93. A statute which authorizes the Commandant of the U.S. Coast Guard to issue rules, orders, and instructions, not inconsistent, relating to the organization, internal administration, and personnel of the Coast Guard.

- Additionally, the Memorandum of Agreement (MOA) for CGBI (2006) defines the life cycle support agreement between the owner and the Operations System Center (OSC); and the Performance Work Statement defines the scope of work in which the data is reutilized to meet emerging and existing USCG requirements not available in other systems.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CGBI is a read-only system that does not collect data directly, but reutilizes previously-collected data from other systems and authoritative data sources. Notice is provided pursuant with 5 U.S.C. § 552a *Records Maintained on Individuals* and via the following SORNS:

- DHS/USCG-013 Marine Information for Safety and Law Enforcement SORN June 25, 2009, 74 FR 30305
- DHS/USCG-027 Recruiting Files SORN August 10, 2011 76 FR 49494
- DHS/USCG-029 Notice of Arrival and Departure SORN December 11, 2008, 73 FR 75442
- DHS/USCG-030 Merchant Seaman's Records SORN June 25, 2009, 74 FR 63949
- DHS/USCG-060 Homeport SORN November 9, 2009, 74 FR 57692
- DHS/ALL-002 DHS Mailing and Other Lists SORN November 25, 2008, 73 FR 71659
- DHS/ALL-019 Department of Homeland Security Payroll, Personnel, and Time and Attendance Records SORN October 23, 2008, 73 FR 63172

1.3 Has a system security plan been completed for the information system(s) supporting the project?

CGBI has completed a System Security Plan and received an Authority to Operate (ATO). ATO was granted June 4, 2010. CGBI is categorized with a Confidentiality rating of Moderate, Integrity rating of Moderate, and Availability rating of Low.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. CGBI is not a transactional system (it is not the originating data source), but a dynamic reporting system which re-uses data from other systems. Cubes are also not static, but can be altered with each use. For example, each time a cube is used to report information, the information will be different in scope and result. For this reason, we rely on the source data systems to archive the raw data sets as is deemed fit for each data type by NARA.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not applicable.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

CGBI is a read-only system that does not collect data directly, but reutilizes previously collected data from other systems and authoritative data sources. The CGBI receives data from the following systems:

- Merchant Mariner License and Documentation (MMLD) - Provides merchant mariner details such as credentials, names, application history, license statistics. PII collected from the general public includes: full name (including maiden name if applicable), MMLD identification number, SSN, date of birth, place of birth, mailing address, phone numbers (home and work), email address, next of kin information (name, mailing address, phone number, email address), country of citizenship, eye color, hair, height and weight), biometrics information (photographs, fingerprint records), and character references information (names, addresses and telephone numbers). (DHS/USCG-030 Merchant Seaman's Records SORN).

- Shipboard Arrival Notification System (SANS) - Provides ship arrival information such as port names, foreign voyages, and previous port visits. PII collected from the general public is not submitted to CGBI. (DHS/USCG-029 Notice of Arrival and Departure SORN).

- Integrated Aids to Navigation Information System (I-ATONIS) - Provides aid availability details. (DHS/ALL-002 DHS Mailing and Other List SORN).

- Shore Asset Management (SAM) - Provides shore asset details such as infrastructure mission dependency indexes. PII collected from DHS employees includes: name, address, date of birth, email address and work number. (DHS/ALL-019 DHS Security Payroll, Personnel and Time and Attendance Records SORN).

- Marine Information for Safety and Law Enforcement/Vessel Documentation System (MISLE/VDS) - Provides marine and law enforcement details such as activities, enforcement offenses, facility inspections, and vessel inspections. Also, provides vessel documentation processing details such as time in queue. PII collected from the general public includes: name, race, address, and telephone number. (DHS/USCG-013 Marine Information for Safety and Law Enforcement SORN).

- Homeport - Provides Homeport system statistics such as publisher counts, invalid login counts, and content access counts for use in monthly progress reports. (DHS/USCG-060 Homeport SORN).

- Recruiting Analysis and Tracking System (RATS) - Provides recruiting and diversity details such as nationality numbers. PII collected from DHS employees includes: full name, address, citizenship status, SSN, race, ethnicity, phone numbers, email addresses, date of birth, marital status, dependent information (full names, date of birth, addresses, phone numbers), and medical history. (DHS/USCG-027 Recruiting Files SORN).

- Boating Accident Report Database (BARD) - Provides recreational boating accident data regarding date/time/location of incident, and characteristics of the vessel (such as make, model), role of individuals (such as operator, occupant, and bystander), casualties' information and cause(s). PII collected from the general public includes: date of birth, gender and age of operators and victims. (DHS/USCG-013 Marine Information for Safety and Law Enforcement SORN).

2.2 What are the sources of the information and how is the information collected for the project?

CGBI is a read-only system and receives all of its information from authoritative source systems via secure connections. CGBI either pulls the information utilizing its Informatica Extract, Transform, and Load (ETL) tool or receives it via SFTP/Enterprise Service Bus (ESB)/E-mail/Spreadsheet. As described above in 2.1, information is provided from the following sources:

- MMLD system database
- SANS system database
- SAM system database
- I-ATONIS system database
- MISLE system databases

- Homeport system database
- RATS system database
- BARD - Spreadsheet from the BARD office at USCG HQ

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

CGBI does not utilize commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

During development, developers check details against the source systems to determine if the information appears the same. Before a product rolls to production, CGBI has product requesters verify the data they are viewing is accurate. Users can check the accuracy of the data against the authoritative source systems CGBI receives it data from. Any corrections are directed to the source system for implementation. Corrections are received during the nightly refresh and viewed in the CGBI system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that CGBI could have unauthorized use of data.

Mitigation: CGBI minimizes exposure risk by utilizing PII only when needed. Requirements are defined by the customer and validated with the source system owner for the indicated use on a case-by-case basis. The purpose must be specified via the USCG Business Reference Model (BRM). Requirements are validated by the CGBI Program Office to tie directly to one of the eleven mission areas, mission support, or business support functions of the USCG. There is no direct entry of data into the CGBI system; data is retrieved from other authoritative systems only. CGBI does not handle data quality and integrity directly since it is not the source system, however there are policies and procedures in place to guide individuals on how to correct data visible in CGBI with the source system from which it was obtained. Any such corrections will be documented in the source system, for accounting purposes.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CGBI reporting and analysis products containing PII are based on documented USCG requirements, USCG reporting policies, and DHS and Congressional inquiries. The CGBI

system allows data from multiple systems from each mission area and business support function to be combined and viewed (along with selected PII) in one system for mission and business support functions. There are currently over 600 such products within the CGBI system. The data is also available for other systems to pull from the enterprise data warehouse databases and use within their system if approved by the system owner/data steward, and is in compliance with documented acceptable uses contained in the appropriate SORN on file. BI systems are not specific as they are designed to allow ad-hoc queries on the data they contain. For example, if the SORN for MISLE states appropriate use of the data collected, CGBI allows reutilization of the data within those limits. Use of information is consistent with the published SORNS stated in Section 1.2, which, pursuant with 5 U.S.C. § 552a(b), permits disclosure "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties."

CGBI is a BI and Mission Support toolset that uses multi-data sources for organizational performance management and improvement across all lines of business. CGBI supplements reports from authoritative sources which may be used for a variety of reasons such as responses to congressional inquiries, program status, or analysis which may yield changes to a particular program:

- MMLD - Provides merchant mariner details such as credentials, names, application history, license statistics used to administer the Commercial Vessel Safety Program, and to perform in-depth analysis on MMLD issues.

- SANS - Provides ship arrival information such as port names, foreign voyages, and previous port visits, which may be used for analysis to improve the boarding and vessel inspection programs.

- SAM - Provides shore asset details such as infrastructure mission dependency indexes. PII collected from DHS employees includes: name, address, date of birth, email address and work number which may be used for workforce and statistical analysis of a given area or region.

- I-ATONIS - Provides aid availability details, which may be used for inspection staffing and regional statistical analysis.

- MISLE/VDS - Provides marine and law enforcement details such as activities, enforcement offenses, facility inspections, and vessel inspections. Also, provides vessel documentation processing details such as time in queue, which may be used to plan and staff appropriate boarding and vessel inspection teams. CGBI provides case management reporting and analysis for law enforcement.

- Homeport - Provides Homeport system statistics such as publisher counts, invalid login counts, content access counts for use in monthly progress reports, which may be used for workforce and statistical analysis of a given area or region.

- RATS - Provides recruiting and diversity details such as nationality numbers. PII collected from non-DHS employees includes: full name, address, citizenship status, SSN, race, ethnicity, phone numbers, email addresses, date of birth, marital status, dependent information (full names, date of birth, addresses, phone numbers), and medical history. RATS provide point-in-time projections, and reports on quality, quantity, and diversity statistics for the recruiting effort.

- BARD - Provides recreational boating accident data regarding the date/time/location of incident, characteristics of the vessel (such as make, model), role of individuals (such as operator, occupant, bystander), casualties information (gender, date of birth and age), and cause(s) which may be used for analysis in a given area or region and trending.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. This PIA will be updated accordingly, when changes to CGBI occur.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. CGBI currently has no other components sharing this capability.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of inappropriate use of information.

Mitigation: CGBI has the ability to limit individual product access based on mission requirements. A user must have an AD account and Common CAC card to obtain entry into CGBI. Database user accounts are audited and the logs are reviewed daily for suspicious or out of the ordinary activity. If suspicious activity is noted, the account is locked and an investigation conducted. Accounts are also terminated upon the following changes:

Users who are contractors have their accounts terminated on their contract termination date or when tasking/performance period ends. Government and military user accounts are automatically terminated upon the user being reassigned, transferred, separated from the service or employment is terminated.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CGBI data and records are a compilation of many sources. CGBI and its supporting personnel do not interact directly with individuals to collect PII data. However, through the publication of this PIA and SORNs applicable to the various source systems noted in Section 1.2, notice has been provided.

CGBI does not collect information on individuals directly, but utilizes data containing PII retrieved from other systems. As data is reutilized in accordance with the source system authority no notification is necessary, as any data corrections will occur in the source system, not CGBI. Individuals, upon request, are referred back to the source system sponsor or owner if there are questions as to the SORN's stated usages and implementation within CGBI.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

None. CGBI is not the authoritative source of information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual will not have notice of this collection.

Mitigation: CGBI is not a primary collector of information. Notice is provided through the SORNs covering the various system interacting with CGBI. Individuals, upon request, are referred back to the source system sponsor or owner.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The project retains specific data elements at an aggregated level for up to five years to establish specific trends. CGBI backup information is as follows: Full backups are run once a week, and are kept for a minimum of four weeks or longer if space allows. Quarterly full backups are run in April, July and October and are kept for one year. Yearly full backups are run in January and are kept for a minimum of seven years. Incremental backups are run six days a week, and are kept for a minimum of two weeks. This information is in compliance with the retention policies of the OSC and in order to recover CGBI to a prior period of time in the event of a disaster. CGBI does not retain information. Data is refreshed nightly in most products and if needed, in extreme cases data could be pulled and reloaded from source system archives or backups into CGBI to recreate data views for a particular time period.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: CGBI retains records in accordance with the authoritative source approved records schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBGI does not share information from the general public outside of DHS.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CGBI does not share information from the general public outside of DHS.

6.3 Does the project place limitations on re-dissemination?

Users with database access are only authorized by the source system owner to utilize the data as described in their *CGBI Access Authorization Form.* Systems with access are limited according to existing Interconnection Security Agreements and/or Memorandum of Understanding which stipulate limitations on specific data sets. As a matter of policy, the CGBI system program management office process is to ask the source system data steward for guidance if CGBI receives a request for dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The project maintains print records of disclosures outside of the department. If a user/system has a database account, the *CGBI Access Authorization Form* is kept on file and updated as needed. If the account is a system account and the servers are interconnected, an Interconnection Security Agreement is completed and maintained on file. Any one time transfers or items that require additional setup can be found within the ClearQuest BI database.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk associated with this system that includes unauthorized disclosure of the information in CGBI.

Mitigation: CGBI does not share information from the general public outside of DHS. The data and information systems are be protected in accordance with DHS Sensitive Systems Policy Directive MD4300A.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any record contained in CGBI, may submit a Freedom of Information Act request in writing to USCG, Commandant (CG-611), Attn: FOIA Coordinator, 2100 2nd St. SW, Stop 7101, Washington, DC 20593-0001.

No specific form is required and requestors may obtain additional information from the FOIA website (http://www.dhs.gov/xfoia/editorial_0579.shtm) or 1-866-431-0486.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Data issues or inquiries from the general public regarding the content or accuracy are referred back to the authoritative source system manager's office for resolution.

7.3 How does the project notify individuals about the procedures for correcting their information?

CGBI is not a primary collector of information. Notice to the general public is provided via the SORNs applicable to the various systems interacting with CGBI.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that inaccurate information/data may be displayed in CGBI.

Mitigation: CGBI is a read-only system. Individuals are referred to the authoritative source, which outlines procedures for redress in the applicable SORN. Once corrected in the

authoritative source system, the item is updated within CGBI during the next nightly data refresh.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The project interface and database access are read-only and certain PII is further access restricted as required. Upon program office/customer request, product access can be limited as follows:

- Applications within CGBI include the Measures Repository and PAA. Access is based on EMPLID and/or AD User ID.
- Cubes/Reports - Can be limited access by organizational office (Department ID or DEPTID) or at the individual level by EMPLID.
- Database - Data field or table-level access to the "back-end" databases are based on authorized user name and password authentication following the rules described earlier in this document under section 2.1.

The project self audits daily; the audits and any anomalies are captured within a weekly system request in the ClearQuest BI database. System administration logs are also emailed to the administrator and project control specialist. These logs are set to look for specific suspicious activity. Any indications of suspicious activity are reviewed and researched by the administrator and the project control specialist is notified of the findings. If significant, the information assurance POC is also notified.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

One Net users are required to complete an annual Information Systems Security (ISS) and Culture of Privacy Awareness training in order to maintain access to the One Net. CGBI provides a report that lists all users who have not completed this training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Users must complete a *CGBI Access Authorization Form* and abide by the *CGBI Policies and Procedures*. The Access Authorization Form lists which data elements the user has requested access to and signature approvals from the user's supervisor, government supervisor,

CGBI Authorizing Official, and the Source System Owner. Access for that user is then limited to only the approved data elements. Audit logs are reviewed to ensure that no other individuals are connecting that are not approved.

Users with database accounts are notified in the *CGBI Access Policies and Procedures* document that the CGBI Authorizing Official and/or the CGBI Program Manager reserve the right to suspend any user's access, without notice, and begin an investigation if they fail to comply with policy or have suspicious/unusual activity.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations with DHS and outside?, new access to the system by organizations within DHS and outside?

All users requesting a database account for receiving information from the project must complete a *CGBI Access Authorization Form*. The form must be reviewed and approved by the requester's supervisor/government supervisor, CGBI Authorizing Official (either the CGBI project officer or CGBI program manager), and the steward of the authoritative source system for the PII data requested. An MOA, MOU and/or ISA must be completed. The documents are completed by both project technical teams, reviewed by each projects program office, and then provided to the systems DAA to sign.

Responsible Officials

David Bandel
CGBI Program Manager
United States Coast Guard
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security