Privacy Impact Assessment
for the

Coast Guard Headquarters Security and Safety Computer Network

June 16, 2010

<u>Contact Point</u>
CWO3 Jan Walker
Headquarters Support Command
United States Coast Guard
(202) 372-4387

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

Abstract

The United States Coast Guard (USCG) operates the Coast Guard Headquarters (CGHQ) Support Command Security and Safety Computer Network (CSS LAN). The CSS LAN is a stand-alone system that encompasses multiple applications that support: physical access control to the CGHQ facility, identity verification, security camera monitoring, and key security and tracking for master keys that are used throughout CGHQ. USCG conducted this PIA because the applications that comprise the CSS LAN collect personally identifiable information (PII).

Overview

The CGHQ Command Security and Safety Computer Network encompasses four major applications that support: physical access control to the CGHQ facility, identity verification, security camera monitoring, and key security and tracking for master keys that are used throughout CGHQ.

Physical Access Controls and Identity Verification

There are two applications that address physical access control and identity verification within the CGHQ facility, MAXXESS and VISSAGE. MAXXESS is the primary application within the network that controls physical access to the CGHQ facility (including restricted spaces) for authorized personnel. Authorized personnel include CGHQ employees, active duty military, government civilians, and contractors with a clearance). The VISSAGE application controls visitor access to the CGHQ facility.

Authorized Personnel Access – MAXXESS Application

The MAXXESS application controls physical access to CGHQ for all authorized personnel through a badge swiping process. MAXXESS operates on a coded badge system that scanners recognize to allow authorized personnel access to the building and secure spaces based on their assignments and duties. MAXXESS information is gathered via multiple sources depending on the individual being cleared. For example, military and government civilian clearance data is extracted from the CG Security Center database called Checkmate or the CG Personnel Database called Direct Access that provides clearance and employment history information on the individual. Contractor information is obtained directly from the contractor via a visit authorization or is verified via a background check by RAPIDGate. RAPIDGate is a vendor credentialing and access management program.

Biometric data collected in the form of a fingerprint impression is obtained from the member during the badge issuing process. Badges used with MAXXESS are issued by the Command Security & Safety (CSS) Office to CGHQ employees, active duty military and civilian personnel, based on information located in the Checkmate or Direct Access databases. These systems provide clearance and employment history information on the individual. Contractor's information is obtained directly from the contractor and is verified via a RAPIDGate background check. Once the background check is complete and approved, a badge is then issued to the contractor. Until the contractor is cleared and issued a badge, they are required to access the building as a visitor through the VISSAGE application described below and obtain a temporary badge.

Visitor Access – VISSAGE Application

The second application that addresses physical access control and identity verification within the network is called VIISAGE, a database CGHQ uses to confirm the validity of a visitor's identification before access is granted to the facility. VIISAGE checks government issued identification (state, federal and international) such as driver's licenses, passports, military ID, CAC cards and immigration ID cards and determines their legitimacy by identifying security points within the ID that each card must have. VIISSAGE scans the ID for the following characteristics: infrared or ultraviolet characteristics, proper seal application, tamper activity, and the legitimacy of the photo.

When a visitor arrives, they must provide at least one form of identification. The ID is then scanned through the VIISAGE machine and is screened for validity. VIISAGE stores the following information: name, date/time of visit, ID type (drivers license, CAC, etc.), ID issuer (country where the ID was issued), jurisdiction (normally the state or country where the ID was issued) and expiration date. The information is kept on file for two years through the application database. In addition to providing identification, the visitor must have a sponsor that will escort them throughout the facility. A badge is issued for them to wear and their ID is retained by the front desk guards and returned upon their departure.

Video Camera Monitoring

The third application is called PELCO. This application controls all the video cameras (currently, 140) within CGHQ and allows the Security Staff to monitor activity throughout the facility. The activity is recorded and each recording is kept on one of 13 DVRs for up to 30 days (but not less than 3 days) depending on the amount of activity on each camera. PELCO collects photographic images of employees and visitors throughout the CGHQ facility.

Key Security and Tracking

A fourth, fairly minor, application within the network is called Morse-Watchmen Keywatcher which monitors a locking cabinet that tracks access to master keys that are used throughout CGHQ. Each key has a computer chip attached that records when the key is removed from the locked cabinet, by whom it is removed (CG employees or contractors), and when it is returned. Access to the cabinet is controlled through badge swiping and biometrics.

Given that the to the network is a stand-alone system, there is no sharing of data between the applications or outside of the network. However, in certain unique circumstances CGHQ may share this information with law enforcement agencies and emergency response workers if certain situations occur (fire, terrorist attack, hostage situation, etc). DHS/ALL-23 entitled "Personnel Security Management System of Records" and DHS/ALL-024 entitled "Department of Homeland Security Facility and Perimeter Access Control and Visitor Management" covers the collection of this information and a routine use is in place to cover sharing in such circumstances.

The authority to operate the CGHQ Security & Safety System is in 14 U.S.C. § 93(a)(10) and 41 CFR Part 102-74, Subpart C. The measures in place adhere to the CG Physical Security & Force Protection Program, COMDINST 5530.1C and Interagency Security Committee, Security Standards for Leased Space DTD 29 September 2004.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

Physical Access Controls and Identity Verification

There are two applications that address physical access control and identity verification within the CGHQ facility, MAXXESS and VISSAGE. MAXXESS is the primary application within the network that controls physical access to the CGHQ facility (including restricted spaces) for authorized personnel. Authorized personnel include CGHQ employees, active duty military, government civilians, and contractors). The VISSAGE application controls visitor access to the CGHQ facility.

The MAXXESS application extracts CGHQ employee, active duty military and government civilian clearance data from the CG Security Center database called Checkmate or the CG Personnel Center database called Direct Access.

CSS employees input personal information into the MAXXESS application on authorized personnel's clearance data derived from the CG Security Center database called Checkmate or the CG Personnel Center database named Direct Access.

CheckMate is a database system owned and operated by the CG Security Center. CheckMate is the repository for security related information and is used to create, edit, maintain, and archive security clearance investigation data for individuals undergoing a security background investigation.

Direct Access is a PeopleSoft and Oracle-based system operated by CG-12 (Personnel Management) that provides administrative support and payroll services to CG military personnel.

RAPIDGate is an external application used to collect un-cleared contractor's information that will be validated and verified through an accepted background check. The information is collected directly from the contractor via a kiosk system owned by RAPIDGate located at CGHQ. The company that is sponsoring the contractor pays for the background investigation through RAPIDGate. All un-cleared contractors must be processed through RAPIDGate to gain access to the facility.

The results from RAPIDGate are then mailed to CGHQ in the form of a security badge that is manually entered into MAXXESS. The RAPIDGate results do not provide any specific information on the contractor other than if they have a clean background check or not. MAXXESS collects/verifies the following information:

- Employee identification number (EMPLID)
- Social Security number (SSN)
- Date of birth (DOB)
- Address
- Phone numbers

- Clearance history
- Employment and criminal History
- Biometric information on identification credentials
- Current employment location within the building

The VIISAGE application applies to visitors the CGHQ facility. VIISAGE physically scans visitor ID cards and compares them against its database to identify their validity. Coast Guard employees are not screened by the VIISAGE application, only visitors are. VIISAGE stores the following information: name, date/time of visit, ID type, ID issuer (, jurisdiction, and expiration date. The information is kept on file for two years.

Video Camera Monitoring

PELCO monitors video activity throughout CGHQ. Each recording is kept on one of 13 DVR's for up to 30 days depending on the amount of activity recorded on each camera. A total of 140 cameras make up our local PELCO network. Only CSS administrative privileged employees have the ability to transfer recordings to DVD and only copies can be made with the approval of the Commanding Officer. PELCO monitors, records and stores physical movement of individuals at CGHQ. PELCO collects photographic images of authorized personnel and visitors throughout the CGHQ facility.

Key Security and Tracking

The data regarding all the keys for Coast Guard Headquarters is manually entered into the Morse-Watchman Keywatcher application by an employee of the CSS office. Once all the data is entered, the Keywatcher monitors all activity in and out of the cabinet and when each key is returned or removed. Access to the cabinet is monitored and logged by through a badge swipe and biometrics access. Besides access information of employees who have been authorized access to the cabinet, no other PII is stored by the Morse Watchman directly.

1.2 What are the sources of the information in the system?

Physical Access Controls and Identity Verification

CG active duty personnel and government civilian employee's information are validated via the CG Checkmate program and Direct Access. Contractor and non-government employees are validated thru an external program called RAPIDGate that validates an individual's background information. If a contractor requires a formal security clearance other than general building access, their contracting agency must then fund the investigation and report the information directly to the CGHQ Security and Safety Division.

VIISAGE is a database that the CGHQ uses to check government forms of identification (state, federal and international) such as driver's licenses, passports, military ID, CAC cards and immigration ID cards as being legitimate by identifying security points within the ID.

Video Camera Monitoring

PELCO monitors video activity throughout CGHQ. Each recording is kept on one of 13 DVR's for up to 30 days depending on the amount of activity recorded on each camera. A total of 140 cameras make up our local PELCO network. Only CSS administrative privileged employees have the ability to transfer recordings to DVD and only copies can be made with the approval of the Commanding Officer. PELCO monitors, records and stores physical movement of individuals at CGHQ. PELCO collects photographic images of authorized personnel and visitors throughout the CGHQ facility

Key Security and Tracking

The data regarding all the keys for Coast Guard Headquarters is manually entered into the Morse-Watchman Keywatcher application by an employee of the CSS office. Once all the data is entered, the

Keywatcher monitors all activity in and out of the cabinet and when each key is returned or removed. Access to the cabinet is monitored and logged by through a badge swipe and biometrics access. Besides access information of employees who have been authorized access to the cabinet, no other PII is stored by the Morse Watchman directly.

1.3 Why is the information being collected, used, disseminated, or maintained?

Physical Access Controls and Identity Verification

CGHQ Security & Safety System collects and verifies PII in order to regulate and control access to CGHQ and spaces within the building based on security clearance level and need-to-know.

Visitor Access – VISSAGE Application

VIISAGE is a database that the CGHQ uses to check government forms of identification (state, federal and international) such as driver's licenses, passports, military ID, CAC cards and immigration ID cards as being legitimate by identifying security points within the ID that each card has. When an ID is scanned, the ID is analyzed as whether it: is a legitimate photo, has infrared or ultra-violet characteristics, is sealed, and has any indications of possible tamper activity.

Video Camera Monitoring

PELCO monitors video activity throughout CGHQ. Each recording is kept on one of 13 DVRs for up to 30 days depending on the amount of activity recorded on each camera. A total of 140 cameras make up our local PELCO network. Only CSS administrative privileged employees have the ability to transfer recordings to DVD and only copies can be made with the approval of the Commanding Officer. PELCO monitors, records and stores physical movement of individuals at CGHQ. PELCO collects photographic images of authorized personnel and visitors throughout the CGHQ facility.

Key Security and Tracking

The data regarding all the keys for Coast Guard Headquarters is manually entered into the Morse-Watchman Keywatcher application by an employee of the CSS office. Once all the data is entered, the Keywatcher monitors all activity in and out of the cabinet and when each key is returned or removed. Access to the cabinet is monitored and logged by through a badge swipe and biometrics access. Besides access information of employees who have been authorized access to the cabinet, no other PII is stored by the Morse Watchman directly.

1.4 How is the information collected?

Physical Access Controls and Identity Verification

The MAXXESS application controls physical access to CGHQ for all authorized personnel through a badge swiping process. MAXXESS operates on a coded badge system that scanners recognize to allow authorized personnel access to the building and secure spaces based on their assignments and duties. MAXXESS information is gathered via multiple sources depending on the individual being cleared. For example, military and government civilian clearance data is extracted from the CG Security Center database called Checkmate or the CG Personnel Database called Direct Access that provides clearance and employment history information on the individual. Contractor information is obtained directly from the contractor via a visit authorization or is verified via a background check by RAPIDGate. RAPIDGate is a vendor credentialing and access management program.

Visitor Access – VISSAGE Application

VIISAGE physically scans visitor ID cards when the visitor presents themselves at CG HQ.

Video Camera Monitoring

The PELCO video camera system records activity throughout CGHQ. This application controls all the video cameras within CGHQ and allows the Security Staff to monitor activity throughout the facility. The activity is recorded and each recording is kept on one of 13 DVRs for up to 30 days depending on the amount of activity on each camera.

Key Security and Tracking

The data regarding all the keys for Coast Guard Headquarters is manually entered into the Morse-Watchman Keywatcher application by an employee of the CSS office. Once all the data is entered, the Keywatcher monitors all activity in and out of the cabinet and when each key is returned or removed. Access to the cabinet is monitored and logged by through a badge swipe and biometrics access.

1.5 How will the information be checked for accuracy?

Physical Access Controls and Identity Verification

Quality control of the information entered is regulated by the CGHQ Security & Safety Division. All information entered into the network is received from the CG Security application called Checkmate or Direct Access. The results of RAPIDGate security checks are mailed back in the form of a security badge that is cleared to be used with MAXXESS and reflects that the background check was not negative and the person can be cleared for access to the building.

Visitor Access – VISSAGE Application

Visitors are required to produce an ID that is scanned by the VIISAGE system. The ID is analyzed as whether it: is a legitimate photo, has infrared or ultra-violet characteristics, is sealed, and has any indications of possible tamper activity.

Video Camera Monitoring

The PELCO video camera system records activity throughout CGHQ. This application controls all the video cameras within CGHQ and allows the Security Staff to monitor activity throughout the facility. The security staff monitors the system for accuracy and proper operations.

Key Security and Tracking

The data regarding all the keys for Coast Guard Headquarters is manually entered into the Morse-Watchman Keywatcher application by an employee of the CSS office. Once all the data is entered, the Keywatcher monitors all activity in and out of the cabinet and when each key is returned or removed. Accuracy of the information is maintained by the CSS office.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Coast Guard is authorized to maintain and operate Coast Guard facilities in a secure manner under 14 U.S.C. § 93(a)(10) and Title 41 CFR Part 102-74, Subpart C authorize. The Privacy Act of 1974;

and DHS/ALL-024 Facility Perimeter Access Control and Visitor Management System of Records govern the disclosure of the information contained in the system.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

USCG mitigated privacy risks presented by the collection of PII by assessing its collection of PII and limiting it to that which is relevant and necessary to accomplish the various functions for the Security and Safety network: physical access controls and identify verification, video camera monitoring, and key security and tracking. Since the CGHQ Security & Safety network is considered a closed stand-alone network due to the lack of an external connection, the primary risk the system exhibits is physical access to the network by an unauthorized individual. This risk is mitigated through a variety of physical security measures to keep the network safe. This includes 14 character passwords for all user accounts, disabled USB ports on terminals in unsecure areas, limited basic user account access, a 5 minute lockout feature, and the limited granting of administrative account privileges. In addition, all servers are kept in a secure space that requires badge and biometrics access. The CSS IT Support Staff is in the process of adding biometrics access to servers and workstations in addition to complex passwords to increase the level of security the network currently has in place.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Physical Access Controls and Identity Verification

The CGHQ Security & Safety network collects the information from authorized sources such as Checkmate, Direct Access and from the employee themselves through the mandatory arrival brief that all employees must read and acknowledge. The information is then entered into the MAXXESS application to allow badges for access to the building to be created for the individual and determine access to spaces.

Visitor's identification is screened against the database VIISAGE, which has been authorized to use in the performance of safeguarding the CGHQ and its personnel. No information is collected from the database, just verification of information based on the applicants identification in comparison to what is reflected in the data base. VIISAGE stores the following information: name, date/time of visit, ID type, ID issuer, jurisdiction, and expiration date. Coast Guard Headquarters hosts hundreds of foreign visitors yearly due to the co-location of the Near East South Asia (NESA) Center for Strategic Studies and the National Defense University at CGHQ. To ensure the facility is protected, tracking all visitors via the log process ensures that each visitor is accountable in case an incident occurs.

Video Camera Monitoring

PELCO is the manufacture of the camera system that CSS uses to monitor physical activity in and around CGHQ. The system is made of 140 cameras that record activity back to 13 DVRs. Recording on each camera is based on activity that occurs in front of each camera. The video is kept up to 30 days depending on the amount of activity on each camera. Only system administrators on the CSS network have access to the PELCO DVR. Reproduction of the video is possible from the DVR to a DVD but is only provided through written approval through the Commanding Officer of CGHQ Support Command.

Key Security and Tracking

The other application within the network is the Morse-Watchmen Keywatcher for key control. The application itself controls access to the key cabinet and can provide a report of access but no information besides the name of the individual who has accessed the cabinet and removed keys is available. The log will be used if a key is missing in order to identify who accessed the key cabinet.

2.2 What types of tools are used to analyze data and what type of data may be produced?

No specific tools are used to analyze the data kept within the network since all information is manually added or scanned via a scanning device for database verification. Reports are run on the network to manually examine information and validate data, but no specific tools are used to analyze information based on trends or complex analytical tasks.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The following security controls are in place to prevent unauthorized and exposures of information stored on the CGHQ Security & Safety network – User & Administrator password length and routine changing of users passwords. Disabled USB ports on terminals that are not located in secure locations. The entire system is considered a closed stand-alone network due to the lack of an external connection, the primary risk the system exhibits is physical access to the network by an unauthorized individual. This risk is mitigated through a variety of physical security measures to keep the network safe. This includes 14 character passwords for all users, five minute lockout feature to eliminate access, disabled USB ports on specific terminals, limited basic user account access and limited granting of administrative account privileges. In addition, all servers are kept in a secure space that requires badge and biometrics access.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Physical Access Controls and Identity Verification

Information that is retained within the MAXXESS application includes DOB, SSN, name, office where the individual is employed, type of employee the individual is and any other security clearance information the employee may have been granted. All of this information forms the employee profile and allows a badge to be issued to them for access to CGHQ. Within VIISAGE the following information is retained: name, date/time of visit, ID type, ID issuer, jurisdiction and expiration date. The information is retained within the system for two years as it serves as the Visitor Control Log for CG Headquarters in accordance with 1.15.55 General Records Schedule 18, 17b – Security & Protective Services Records.

Video Camera Monitoring

PELCO is the name of the company and camera system that monitors physical activity in and around CGHQ. The system is made of 140 cameras that record activity back to 13 digital video recorders (DVR's). Recording on each camera is based on activity that occurs in front of each camera. The video is kept up to 30 days depending on the amount of activity on each camera. Only system administrators on the CSS network have access to the PELCO DVR.

Key Security and Tracking

The log history associated with the Morse-Watchmen Keywatcher application is retained for six months. The application itself controls access to the key cabinet and can provide a report of access but no information besides the name of the individual who has accessed the cabinet and removed keys is available.

3.2 How long is information retained?

Physical Access Controls and Identity Verification

Once the visitor/employee no longer requires access, their badge is removed from the MAXXESS system. Within VIISAGE, the following information is retained: name, date/time of visit, ID type, ID issuer, jurisdiction, and expiration date. This information is retained within the system for two years in accordance with the 1.15.55 General Records Schedule 18 – Security & Protective Services Records through the VIISAGE system. VIISAGE serves as the visitor control log for CGHQ.

Video Camera Monitoring

The video is kept up to 30 days.

Key Security and Tracking

The Morse-Watchmen Keywatcher application that manages key control retains access history and key transactions for up to six months.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The CGHQ Command Safety and Security Network records are covered by the GRS 18, section 17: Visitor Control Files. This requires agencies to retain visitor control files for two years. This requirement is applicable to our MAXXESS, VIISAGE and Morse-Watchman Keywatcher applications. Video is not covered under this guidance but if an incident occurs that is on tape, a copy may be kept for as long as is deemed necessary at the command's discretion.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Within the two primary applications that run on the CGHQ Command Security & Safety network, VIISAGE is updated regularly by the proprietor of the application. All information is kept in a secure and closed network for a maximum of a two year period.

By following the NARA and CG policies on record retention, all visitor logs are retained for two years. VIISAGE stores the following information: name, date/time of visit, ID type, ID issuer (, jurisdiction, and expiration date. The information is kept on file for two years through the application database. This ensures visitors PII is kept for the shortest period retention period possible.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

No information stored on the CGHQ Command Security & Safety network is shared with any other CG commands or internal agencies.

4.2 How is the information transmitted or disclosed?

Information from the CGHQ Command Security & Safety network is not shared with any other CG commands or internal agencies.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information from the CGHQ Command Security & Safety network is not shared with any internal or external entities. All information is kept on a secure stand-alone network that is only accessible by authorized users designated by the CGHQ Command Security & Safety Division, thus risks of inappropriate internal sharing are mitigated.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Generally, information from CGHQ CSS is not shared with any internal or external entities. However, in certain unique circumstances CGHQ may have to share this information with law enforcement agencies and emergency response workers if certain emergencies occur (fire, terrorist attack, hostage situation, etc).

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

As noted in 5.1, in certain unique circumstances, CGHQ may have to share this information with law enforcement agencies and emergency response workers if certain emergencies occur(fire, terrorist attack, hostage situation, etc.). The DHS/ALL-23 SORN entitled "Personnel Security Management System of Records" covers the collection of this information and a routine use is in place to cover sharing in such circumstances.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information within the CGHQ CSS LAN is not normally shared with any internal or external entities. In the event of one of the circumstances mentioned above, personal information would be provided to law enforcement personnel in person (upon presentation of personal credentials) or encrypted email.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There is a risk of improper external sharing of this information. The risk is largely mitigated by the fact that CSS is only sharing the information externally in a set of limited circumstances identified previously in this section, thus the risk is low.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The System of Records Notices covering the collection of PII related to this system include DHS/ALL-023 entitled "Personnel Security Management System of Records" and DHS/ALL-024 entitled "Department of Homeland Security Facility and Perimeter Access Control and Visitor Management," and DHS/ALL-010 entitled "Department of Homeland Security Asset Management Records." Additionally, notice to individuals is provided through this PIA and the policies and procedures noted below.

When an Active Duty, Reservist, Government Civilian or Contractor submits a request for a badge to be allowed access to CGHQ, they are required to complete an "Arrival Brief." At the end of the brief, the employee completes the CGHQ Security Identification Badge and Security Clearance Request, acknowledging the brief and requesting a badge to be issued for access. Before submitting their information, the employee is provided a Privacy Act notice that addresses authority, principal purpose and disclosure.

Non-military visitors may be granted temporary access to the building if they are sponsored by an individual currently employed within CGHQ, and their photo identification is screened through the VIISAGE database without any negative responses. A Privacy Act notice is posted at the CGHQ Security Front Desk for all visitors to see, that addresses authority, principal purpose and disclosure to request identification to confirm the visitor's identity (see Appendix A).

In regards to the PELCO surveillance system, signs are posted in around the CGHQ facility to notify all members that they are under surveillance per 40 USC 1315 to protect the buildings, grounds and property owned, occupied or secured by the Federal Government, and the persons on the property. The signs state the following "This Area Under Video Surveillance."

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Government employees and contractors, as well as non-military visitors may decline to provide the requested information; however failure to provide the information will prevent them from accessing CGHQ.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes. By providing the requested information, individuals consent to the use of the information in order to verify their identity and grant access to CGHQ. Their information is not used in any other way.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Employees requesting access to CGHQ are provided a Privacy Act notice that informs them that their information is being collected for the purpose of granting access to CGHQ. Visitors are made aware of the collection of their information through the posting of a Privacy Act notice at the front security desk at CGHQ. Notice is also provided to all government employees while completing their arrival brief. A copy of the arrival brief which includes the Privacy Act notice is generated at the conclusion of the briefing for CG employees for their personal records. As a result, the risks of on individual being unaware about the collection are mitigated.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Physical Access Controls and Identity Verification

MAXXESS -

For all CG employees, including contractors and non-government employees, the CGHQ Command Security & Safety office only collects information for the MAXXESS system that has been obtained from Checkmate, Direct Access and the employees themselves through the arrival brief process. Employees are not provided access to information stored within MAXXESS, but are directed to the databases that the information came if validity of information is in question. If the employee believes the information may have been entered incorrectly into based on the information provided via the arrival brief, the Security & Safety Office will review the information within MAXXESS to ensure the information was entered correctly. Any employee may obtain a copy of their information by submitting a Privacy Act/Freedom of Information Act (FOIA) request to: Commandant (CG-611), 2100 2nd Street, SW. Washington, DC. 20593-0001, Attn: FOIA.

VISSAGE –

All visitors are processed by the VIISAGE system and the following information is retained: name, date/time of visit, ID type, ID issuer, jurisdiction, and expiration date. The information is retained within the system for two years in accordance with the 1.15.55 General Records Schedule 18 – Security & Protective Services Records through the VIISAGE system. VIISAGE serves as the visitor control log for CGHQ. Any visitor may obtain a copy of their information by submitting a Privacy Act/FOIA request to: Commandant (CG-611), 2100 2nd Street, SW. Washington, DC. 20593-0001, Attn: FOIA.

Video Camera Monitoring

PELCO is the name of the company and camera system that monitors physical activity in and around CGHQ. The system is made of 140 cameras that record activity back to 13 digital video recorders (DVR's). Recording on each camera is based on activity that occurs in front of each camera. The video is kept up to 30 days depending on the amount of activity on each camera. Only system administrators on the CSS network have access to the PELCO DVR.

Key Security and Tracking

The log history associated with the Morse-Watchmen Key watcher application is retained for six months. The application itself controls access to the key cabinet and can provide a report of access but no information besides the name of the individual who has accessed the cabinet and removed keys is available. Access to this application information is maintained by the MAXXESS system. If the employee believes the information may have been entered incorrectly into based on the information provided via the arrival brief, the Security & Safety Office will review the information within MAXXESS to ensure the information was entered correctly. Any employee may obtain a copy of their information by submitting a Privacy Act/FOIA request to: Commandant (CG-611), 2100 2nd Street, SW. Washington, DC. 20593-0001, Attn: FOIA.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If an individual believes that the information contained within MAXXESS is inaccurate or erroneous, CG employees are directed to engage the security representative for Checkmate or the personnel representative for Direct Access. Contractors and non-government employees may direct their concerns to their Contracting Officer's Technical Representative who will then advise RADIDGate of the discrepancy. Additionally, a review of the employee's record can be conducted by the CGHQ Security & Safety office if it is believed that information was manually entered incorrectly, it can be corrected immediately. Since a visitor's information is not kept within MAXXESS and the information retained in VIISAGE comes off of the ID, correcting inaccurate or erroneous information is not applicable. If a visitor wanted to address an issue of this nature, the CGHQ Command Security and Safety Office would be contacted.

7.3 How are individuals notified of the procedures for correcting their information?

Since all information that is stored within the MAXXESS system at CGHQ originates from other databases (Checkmate, Direct Access, and RAPIDGate) and the employees own provided information from their arrival brief, allowing the individual to review our MAXXESS system is not an option. If the employee disagrees with information that he or she believes that the MAXXESS application reflects, they are directed to address the database where the information originated or request that the CGHQ Command Security & Safety review their information to ensure it was entered correctly into the application. Since a visitor's information is not kept within MAXXESS and the information retained in VIISAGE comes off of the ID, correcting inaccurate or erroneous information is not applicable. If a visitor wanted to address an issue of this nature, the CGHQ Command Security and Safety Office would be contacted.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Since all information that is stored within the MAXXESS system at CGHQ comes from other databases (Checkmate & Direct Access), allowing the individual to review our MAXXESS system is not an option. If the employee disagrees with information that he or she believes that the MAXXESS application reflects, they are directed to address the database where the information was originally obtained from or can request that the CGHQ Command Security & Safety Office review their information to ensure it was entered correctly into the application.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Since all information that is stored within the MAXXESS system at CGHQ comes from other databases (Checkmate & Direct Access) and the employee themselves, allowing the individual to review our MAXXESS system is not an option. If the employee disagrees with information that MAXXESS reflects, he or she is directed to address the database where the information was originally obtained from or can request that the CGHQ Command Security & Safety Office review their information to ensure it was entered correctly into the application. There are no privacy risks associated with the redress process currently in place and if satisfaction is not obtained through the CGHQ Security & Safety Office, the matter can be addressed through the Privacy Act and Freedom of Information Act (FOIA) office/CG-611.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

All user accounts are created by the CGHQ Command Security & Safety Local Area Network (LAN) Administrator. Only authorized government employees and contractors who work within the CGHQ Command Security & Safety Division may have accounts created in the performance of their official duties. Roles within the network are granted based on the employee's position and duties. The average user maintains the ability to "Read Only" within the networks configuration, where as a system administrator maintains full access in the performance of his or her duties.

8.2 Will Department contractors have access to the system?

Yes. Only authorized CGHQ Security and Safety Division contractors who have been cleared for access to the network will be authorized to maintain accounts within the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All CGHQ Security & Safety Division personnel are provided Privacy Training as part of the CG yearly general yearly mandated training. Additional local training on privacy and handling of data within this specific network is provided by the CGHQ Command Security & Safety office for all users with accounts on a yearly basis.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

A Certification and Accreditation (C&A) of the CGHQ Command Security & Safety network has been started and is currently in progress. Since this network is a stand-alone system, precedence within the CG has been given to systems that are a part of the CG Data Network (CGDN) and recognized as operational networks due to the scrutiny set forth through the FISMA evaluation process. Presently the C&A on this particular system is being developed as a separate but supported subsystem of the Sensitive But Unclassified (SBU) General Support System (GSS) for Headquarters Support Command (HSC). The network will be documented and submitted this fall as part of the new C&A for the SBU GSS HSC network.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

To prevent misuse of data within the CGHQ Command Security & Safety network, the following auditing and technical safe guards are currently in place; access to all terminals within the network is limited to authorized personnel only. All terminals are kept in secure locations that require badge and/or biometric access. Length of all user passwords are 14 characters in length and users are forced to change their passwords every 90 days. If a user incorrectly enters his or her password 3 or more times, their computer account is locked out for 30 minutes. If the system detects in-activity for longer than 5 minutes, the terminal will time out and require the employee's password to be re-entered. The CGHQ Command Security & Safety Local Area Network (LAN) administrator monitors all system activities record log auditing and ensures that each user is only allowed privileges associated with their position and need to know. As part of the ongoing C&A process, additional security controls are expected to be added to increase security of the network.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The privacy risks that the CGHQ Command Security & Safety network experiences are primarily physical in nature. Since the network is a stand-alone system and does not connect to any other networks, outside infiltration and sharing issues are non-existent. To help mitigate exposure of the physical nature, access to all terminals within the network is limited to authorized personnel only. All terminals are kept in secure locations that require badge access. Length of all user passwords are 14 characters in length and users are forced to change their passwords every 90 days. If a user incorrectly enters his or her password 3 or more times, their computer account is locked out for 30 minutes. If the system detects in-activity for longer than 5 minutes, the terminal will time out and require the employee's password to be re-entered. The CGHQ Command Security & Safety Local Area Network (LAN) administrator monitors all system activities and ensures that each user is only allowed privileges associated with their position and need to know.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The CGHQ Command Security & Safety network was not conceived through a System Developmental Life Cycle (SDLC) approval process, but was evaluated and constructed through a step process of configuring the best security features available at the time with the approval of the Chief of Staff for CGHQ. This approval was based on the security needs set forth by the location of CGHQ following the attacks of September 11th 2001 and the increase in the force protection level throughout Washington, DC in accordance with the CG Physical Security and Force Protection Program (COMDTISNT M5530.1C).

9.2 What stage of development is the system in and what project development lifecycle was used?

The CGHQ Command Security & Safety network was not conceived through a System Developmental Life Cycle (SDLC) approval process, but was evaluated and constructed through a process of configuring the best security features available at the time with the approval of the Chief of Staff for CGHQ. This approval was based on the security needs set forth by the location of CGHQ following the attacks of September 11th 2001 and the increase in the force protection level throughout Washington DC in accordance with the CG Physical Security and Force Protection Program (COMDTISNT M5530.1C).

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The CGHQ Command Security & Safety network does utilize biometrics and unique security software, but with the system being a stand-alone network, many of the privacy concerns are mitigated based on this configuration. With the system being stand-alone, the primary obstacle becomes physical access which can be limited by physical security measures and system access.

Responsible Officials

Wayne Truax

Director

SILC Detachment, Washington DC

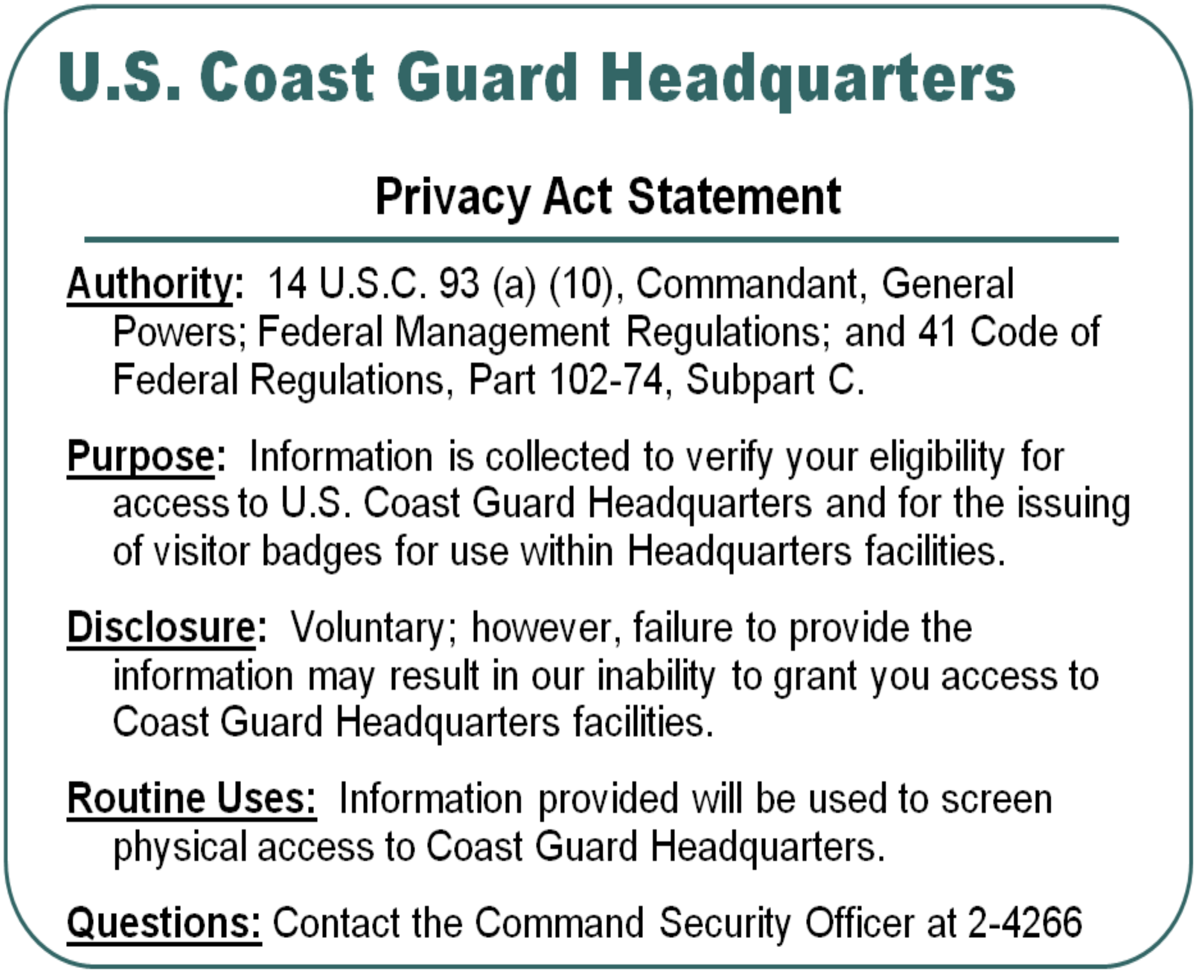
United States Coast Guard

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX A – Copy of U.S. Coast Guard Headquarters Privacy Act Statement.



U.S. Coast Guard Headquarters

Privacy Act Statement

Authority: 14 U.S.C. 93 (a) (10), Commandant, General Powers; Federal Management Regulations; and 41 Code of Federal Regulations, Part 102-74, Subpart C.

Purpose: Information is collected to verify your eligibility for access to U.S. Coast Guard Headquarters and for the issuing of visitor badges for use within Headquarters facilities.

Disclosure: Voluntary; however, failure to provide the information may result in our inability to grant you access to Coast Guard Headquarters facilities.

Routine Uses: Information provided will be used to screen physical access to Coast Guard Headquarters.

Questions: Contact the Command Security Officer at 2-4266