Privacy Impact Assessment
for the

United States Coast Guard Academy Information System (ACADIS)

January 26, 2010

Contact Point
ITCS Guy O. Cranfill
ISSO
CGA Information Services Division
860-444-8273

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

Abstract

The United States Coast Guard Academy (CGA or Academy) has developed the Academy information system (ACADIS) transactional database system. ACADIS provides an information resource for the management of the CGA educational environment including the training and development of all future Coast Guard officers. To support this function, ACADIS processes transactional data for cadet military program records and various facility applications, manages applicant data to facilitate the admissions process, and warehouses data on cadets, prior cadets, faculty, and staff. USCG conducted this privacy impact assessment (PIA) because ACADIS collects and maintains personally identifiable information (PII).

Introduction

Coast Guard Academy Background

As part of basic operations, CGA trains and educates future Coast Guard Officers. This is accomplished in one of two ways: the Leadership Development Center and a four year university. As background, the USCG requires all commissioned officers to have a bachelor's degree prior to obtaining a regular commission. Officer candidates who already meet this requirement are enrolled in Officer Candidate School where they are provided a basic military education. High School graduates and college students who have not achieved a bachelor's degree and are under the age of 23 may apply for enrollment into the CGA. Unlike other military academies, CGA uses competitive appointments instead of congressional nominations to select its pool of cadets. If the applicant meets all requirements and is accepted, they are enrolled to complete a four year Bachelor of Science degree in addition to receiving military instruction; once enrolled CGA students are called cadets. By law CGA and other military cadets are provided a fixed stipend that is paid each month to cover normal living expenses while enrolled at the CGA. The amount of this stipend is fixed by Congress. In exchange for this educational benefit, cadets are required to serve as commissioned officers in the United States Armed Forces for a period of at least five years.

Coast Guard Academy Information System (ACADIS)

ACADIS is the Academy's transactional database system owned and managed by the CGA Information Services Division. The main function and objective of this system is to provide an information resource for the management of the CGA educational environment; including the training and development of all future Coast Guard officers. ACADIS serves a number of purposes including:

- Processing of transactional data, such as attendance, grade information, excusals, and demerits for cadet military program records and various faculty applications, such as their grade books and time sheets;
- Management of applicant data to facilitate admissions process;
- Warehousing of data on applicants, cadets, prior students, and faculty.

Transactional Data

Transactional data entry is accomplished either through manual import from an outside source or by web forms. Web forms are created for each type of transaction; access to these forms is governed by the user roles. For example the admissions office can only access forms associated with evaluating potential students for admissions, while a faculty member may only be able to access the cadets' grade books.

Management of Applicant Data

Unlike other military academies, such as the Military Academy at West Point, and the Naval Academy in Annapolis that rely on congressional appointments to determine their pool of applicants, CGA relies on a competitive application process. Potential CGA Cadets apply to the CGA, and are screened based on factors such as grade point average, academic standing, community service, and athletic achievement.

Applicant data is stored in a separate module within the database. Potential cadets begin the formal application process by completing a profile on the CGA web page and creating an account. They provide contact information, desired degree program and interest information, as well as academic information such a current grade point average and standardized test scores if available. As additional records become available from the student, through the College Board, Paskill, Stapleton & Lord Consulting (PS&L), and Department of Defense Medical Examination Review Board (DoDMERB) they are imported into the applicant portion of the database.[1] Once an applicant is accepted by the CGA, their application records are manually imported into the cadet section of the database and made available to the Registrar's office.

Warehousing of Data

The CGA data warehouse is a 7 Terabyte (TB) enterprise network area storage system with a 5 TB backup storage unit that provides daily backups which are maintained for two weeks along with two months of full backups. CGA has recently implemented a policy to maintain three years of offline backup of the ACADIS database. This stores all cadet academic and military records such as grades, evaluations, demerits, and excusals for the duration of cadet enrollment. After disenrollment or graduation, cadet records are moved into an archival status to be used for future research, and to answer CG and congressional inquiries. Recent inquiries have included requests for information on historical cadet body demographics and minority success rates.

Typical Transactions

Once a potential cadet has submitted his or her application package, a team comprised of CGA faculty and staff as well as members of the admissions staff reviews each application package. This team ensures potential cadets meet current academic and physical requirements, and that their packages are complete. Packages are also screened to determine potential cadet suitability, and likelihood of program completion. The package is thereafter assigned a score. Application packages are then rank-ordered and offer letters are sent to the top scoring applicants. The number of applicants offered enrollment to the CGA varies from year to year based on the CG's anticipated need for new officers but the freshman class is usually about 400 cadets. Although CGA does actively recruit minorities and women, these effort are to increase the number of applicants from these groups in the pool, these factors are NOT a factor in the ranking or selection process.

[1] See Section 1.2 for details on these sources.

In addition to supporting the CGA admissions process, ACADIS also provides applications that support CGA faculty in performing their duties. Specifically, ACADIS allows authorized faculty members to enter grades for cadets in their classes. In addition, upper class cadets act as supervisors for lower class cadets and are responsible insuring the cadets are attending scheduled classes, meetings, and events as directed by members of the CGA faculty; upper class cadets are in turn supervised by CGA faculty. Both faculty and upper class cadets use ACADIS to enter cadet evaluations for a specific evaluation period. A typical transaction for faculty use of ACADIS, such as grade entry, requires a faculty member to log into ACADIS then choose the cadet record to be modified and enter the appropriate grade. Another type of transaction will require the cadet's supervisor to again log into the system, choose the cadet record, and enter evaluations for that evaluation period. In both cases the faculty member or supervisor making modifications can only access cadets assigned to their account and only fields associated with their role. For instance a non-supervisory faculty member can not access evaluations and a supervisor can not access cadet grades.

Section 1.0 Information collected and maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

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

Applicants: Applicants can apply either directly or indirectly, through external sources. In the case of a direct application the applicant must provide name, date of birth, address, phone number, and Social Security number (SSN). The applicant may also provide unofficial test scores and basic medical information if it is available, though final "official" information is collected from external sources. Applicants that are selected are scheduled for an entrance physical with a DOD medical examination facility (MEPS) through DoDMERB. The applicants name, address, SSN, and date of birth are manually exported and sent by HTTPS to the DoDMERB system; the applicant is then able to schedule an appointment at an MEPS facility near them.

Information collected from external sources, at the potential cadet's request (see at 1.2) include: name, date of birth, address, and SSN, as well as standard test grades and medical information. In each case the candidate must specifically request that the data be provided to the CGA, or provide the data directly to the CGA on its web site.

Cadets**:** Information collected internally on cadets includes: name, date of birth, mailing address, telephone number, SSN, e-mail address, zip code address, medical information, bank account numbers, education record, internet protocol addresses, names of limited relatives/guardians, automobile registration and insurance information, and photographic facial images. The ACADIS system generates grade reports for current cadets.

Faculty**:** Information collected internally on faculty includes: name, rank (or pay grade), SSN, employee ID, telephone number, and home address.

Staff**:** Information collected internally on staff includes: Name, rank (or pay grade), SSN, Employee ID, telephone number, and home address.

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

Applicant: ACADIS collects information directly from individuals seeking admission to the GCA. In addition, ACADIS uses external sources for the admissions process including the College Board; PS&L; and the DoDMERB. The College Board administers standard college admissions tests, such as the Scholastic Aptitude Test (SAT) taken by many high school students. PS&L provides an information request service for many universities to allow high school students to send their contact information to schools they hope to attend. DoDMERB is the Department of Defense Agency responsible for the determination of medical qualification of applicants for appointment to a United States Service Academy, and provides this information to the school selected by the examinee.

Cadet: The ACADIS system collects information directly from those currently enrolled as cadets as well as through the information provided on the cadet's application for admission to the CGA as noted above.

Faculty and Staff: The ACADIS system collects information directly from faculty and staff.

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

Applicant: External sources are used to identify and qualify prospective students who may be offered admission to the Coast Guard Academy. Students may use these sources (such as PS&L's service hosted on higher education information web sites) to request that the CGA recruiter contact them. Additionally they have this option when selecting the CGA as a school to which SAT results will be provided

Cadet: The ACADIS system collects cadet information to manage academic and military performance. Financial information is used to facilitate cadet pay. Photographs are used to identify cadets. The ACADIS system creates grade and conduct reports used by the institution to evaluate cadet progress.

Cadet automobile and insurance information is required to access military facilities, such as the CGA and other CG and DOD facilities, as required by military policy. The preferred method for accomplishing this is the issuance of a service specific sticker indicating that the vehicle has been previously screened and is eligible to enter the facility; ACADIS only maintains this information for cadets.

Faculty and Staff: Faculty and staff information is collected for identification and management of the workforce.

1.4 How is the information collected?

Applicant: Information is collected directly from the individual seeking admission to the CGA as well as from external sources, at the potential cadet's request from the College Board via mailed compact disks. Information is transmitted from PS&L via file transport protocol (FTP) and loaded into ACADIS. Information from DoDMERB is sent via HTTPS and loaded into ACADIS.

Cadet: Information is obtained directly from the individual via their applicant data which is uploaded electronically into ACADIS once they have been sworn in as a cadet on his or her first day at the CGA (reporting-in day). Cadets, on reporting-in day, validate the information that is in the system and make necessary changes. This information remains in the system and if changes arise during their tenure at CGA, they update the information via an online system and again, the database is updated with the current data.

Faculty and Staff: Faculty and staff information is collected directly from the affected individuals.

1.5 How will information be checked for accuracy?

Applicant and Cadet: ACADIS contains information collected directly from the individual when they applied for admission to the Academy. All information corrections, changes, etc. are available via the CGA Help Desk. Once erroneous data is discovered, either by the applicant, cadet, admissions officer, or registrar; corrected data is submitted to a database administrator by a CGA Help Desk work request. The administrator can then manually remove or correct the erroneous data.

Internally collected information (e.g., grade reports) is reviewed by chain of command, advisors, and is subject to formal audits to verify information. Externally collected information is verified via the external source, confirmed by direct correspondence restating information on file and requesting verification, and through personal requests with the applicant.

Faculty and Staff: Faculty and staff information is collected directly from affected individuals and is assumed to be accurate. If a faculty or staff member believes any of their information is inaccurate or requires an update (e.g., change to home address), they may contact the CGA Help Desk for assistance.

1.6 What specific legal authorities/arrangements/agreements define the collection of information?

USCG has the authority to collect this information in order to administer the CGA under 14 U.S.C § § 181-195. USCG has a contract with PS&L for their data collection service. Data is collected and transmitted to the CG and is not used by the PS&L for any internal purpose.

USCG has a contract with College Board for the hosting of the Recruitment Plus database. Candidate status updates are transmitted to the database from ACADIS for use by CG Academy staff, and is not used by the College Board for any internal purpose.

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

The privacy risk is the unauthorized disclosure of particularly sensitive information such as SSN and financial information. The mitigation strategy includes restricting access to the data as much as practical. This is accomplished through the designation of specific user roles that only allow access to sensitive data

elements required by the user on a need-to-know basis.

The information is collected consistent with the provisions of the Privacy Act. It is used to screen potential Academy cadets, track grades and performance, facilitate pay of current cadets, and manage current faculty and staff's personal information. Information is also retained on past cadets for research and statistical tracking purposes.

Externally collected information is confirmed by direct correspondence restating information on file and requesting verification. Existing cadets and staff may access personal information to verify accuracy.

Section 2.0 Uses of the system and 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.

Applicant: Applicant information is used to filter and select appropriate candidates for admission to the CGA. The personally sensitive data such as applicant name and SSN are necessary to uniquely identify candidates and match them with data reports such as transcripts, standardized test scores, etc. Dates of birth are necessary to validate eligibility. Medical information is needed to evaluate their ability to meet the strict standards for admission. Addresses and phone numbers are needed to maintain communications. Educational records/grades are needed to evaluate prior performance.

Cadet: Current cadet information is used to guide decisions and recommendations for cadet discipline, awards, privileges, probationary statuses and all officer leadership development called for under the Coast Guard Academy's curriculum.

Past cadet identifying information is recorded for Registrar purposes and institutional reporting and analysis of academic performance of the institution at large.

Faculty and Staff: Faculty and staff identifying information are used to enable access to ACADIS applications including timesheet entry. In addition, Academy faculty also use ACADIS applications for recording attendance, and grade entry. Faculty and staff contact information from ACADIS are also used as the source to create the Academy telephone directory.

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

The system itself does not inherently perform any data mining, however users in the Institutional Research and Admissions branches of the CGA conduct analysis on the data, which is provided from ACADIS in de-identified form, to help measure academic performance and improve recruiting respectively. It is the responsibility of Institutional Research to compile descriptive statistics and statistical models of cadet and Academy activities. The data that form the source of these statistics and statistical models is often or usually contained in ACADIS. We regularly pull data from ACADIS in de-identified form to construct and

update statistical tables and statistical models that are made available to Academy leadership and address HQ requests to aid them in their decision-making and responding to congressional inquiries.

2.3 If the system used commercially or publicly available data, explain how and why it is used.

Commercially available data from the College Board is provided to the ACADIS system, for applicants through mailed compact disks. This data, in the form of SAT or ACT standardized test scores, is used to evaluate potential cadet qualifications to attend the Coast Guard Academy.

Though not commercially or publicly available, ACADIS uses an external data source, DoDMERB, to evaluate potential cadet ability to meet military physical qualifications. As a government agency, DoDMERB will only provide data to the federal service academies and authorized accession sources for ROTC scholarship programs.

Commercially available data from PS&L, as indicated in section 1.1, is used to identify potential candidates for admission to the Coast Guard Academy. Data from ACADIS is transmitted to the College Board Recruitment Plus database in order to identify, and recruit potential candidates for admission to the CGA.

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.

Privacy risks associated with the potential misuse of ACADIS information are mitigated through a variety of factors. All users are required to complete acceptable use training and an acknowledgment form prior to being granted access to the system. Users must have a valid username and password to access ACADIS.

Audit logs are maintained and reviews of these logs are performed as necessary. Disciplinary programs are in place for violations of appropriate use policy. Privacy Act information penalties are posted on the system login page to remind users of the implications of negligent data safeguarding.

To mitigate the risk inaccurate information provided by commercial entities, ACADIS only uses commercially acquired data from sources used throughout the higher education industry that is considered very reliable.

Section 3.0 Retention

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

3.1 How long is information retained?

Applicant: Records for applicants who are not accepted, or who decline their appointment, are retained for one year to facilitate a future application(s). After one year, non-accepted applications are

removed from the system.

Cadet: All cadet data (except for banking and vehicle information which are removed from ACADIS in the December following the cadet's departure from the Academy) is retained indefinitely in order to comply with accreditation requirements. It also serves as a data warehouse for long term institutional research and analysis. Daily backups are accomplished and retained for two weeks while full backups are retained for two months. Monthly full backups of the ACADIS database are retained for three years, in the CGA tape storage safe, with the oldest tape being overwritten after 36 months. After graduation, cadet records are moved from active to archive status and maintained for ten years; after ten years cadet grade records are moved to fiche and retained indefinitely.

Faculty and Staff: Faculty and staff information, other than name, rank and gender, is removed in the December following their departure from the CGA.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

NARA is currently reviewing ACADIS to determine the proper records retention schedule.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

There is a significant privacy risk in retaining information for a long period of time. Cadet data, except for their banking and vehicle information, is retained indefinitely in order to comply with accreditation requirements. Frequent research requests and various ad hoc analyses are conducted to evaluate cadets and prospective cadets. Further, Institutional Research and Admissions branches of the Academy conduct analysis on the data in de-identified form to help measure academic performance and improve recruiting respectively.

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 organizations is the information shared, what information is shared and for what purpose?

The CGA shares international student academic and military performance information with Coast Guard International Cadet Program which is part of the CG International Affairs Office (CG-OOI). This information is shared with the international cadet's home country and serves to help improve the quality of international exchange cadets at the Academy. Traditional cadet, faculty and staff information is not shared outside the organization, other than through the institutional research branch to answer CG and congressional inquiries.

4.2 How is the information transmitted or disclosed?

Information can be provided to external offices, such as Coast Guard Headquarters or country of origin (in the case of a foreign student). If approved by the CGA Superintendent and Commandant of Cadets, the information is provided via unencrypted email, although such requests are approved only in extraordinary circumstances.

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.

Privacy is mitigated by limiting the disclosure of individually identifiable information such as name, SSN/cadet number, and academic record, outside the CGA or within the CG and DHS. If disclosure is deemed necessary then it will only occur on a case-by-case basis after careful review to ensure it is consistent with the Privacy Act. This review includes review by the Superintendent and Commandant of Cadets. Foreign students are the exception as they are usually required to provide access to their academic and military records to their sponsoring country.

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?

Applicant: College Board Recruitment Plus database is provided candidate status updates via secure FTP to aid and focus CGA recruiting efforts. Once an applicant is selected, his or her name, address, date of birth, phone number, and SSN are extracted and provided to DoDMERB, by HTTPS so that they may schedule an appointment to have a commissioning physical, passing this physical is a requirement to attend the CGA.

Cadet: As with any college or university, cadets may request their academic transcript be shared with other institutions such as colleges and graduate schools or with employers (after they have completed their obligation to the CG). This is done by submitting a signed transcript request form to the registrar's office, certified copies are then provided by US Mail as requested by the former cadet.

Name and account number of active cadets for processing payroll and credit accounts are provided to the applicable financial institution such as the Navy Federal Credit Union.

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

Yes. All information shared by ACADIS is in accordance with SORN DHS/USCG-014 entitled Military Pay and Personnel System.

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

As there is no unauthenticated external sharing of data, privacy risks are mitigated. All external sharing is directly in support of a specific business transactions or processes. The main risks are careless handling of the data by external partners. DoDMERB system is Certified and Accredited by the DOD. College Board is the national clearinghouse for college testing and has stringent privacy and security policies (http://www.collegeboard.com/html/privacy001.html). The financial institutions that active cadets designate for their payroll and credit account deposits such as the Navy Federal Credit Union each have stringent privacy and security policies to control the data in their systems. PS&L subcontracts the hosting of its database application with www.hostmysite.com, who is an established online hosting company. Their policies and terms of service for hosting are provided at http://www.hostmysite.com/termsofservice/

.

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?

Yes. Notice of how information is used is provided on the applicant web page when initiating an application. Standard FOIA and Privacy Act information links are provided at the web interface where data is collected. Collection of this information is covered under SORN DHS/USCG-014s entitled Military Pay and Personnel System.

Active cadets, staff, and faculty annually review a standard Coast Guard User Acknowledgement Form and Automated Information System brief describing their liabilities and restrictions in accessing a government information system.

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

PII is required to accurately analyze applications for admission to the Academy. Academic portion of records are fundamental to CGA business. Individuals have the right to not participate in any programs in the CGA, but certain information is required in order to enroll.

PII is required throughout the application process and in the procession of transactional data after enrollment, to insure that the proper records are being accessed. With a cadet population of approximately 1000 students, duplicate name are not uncommon, thus it is important is insure records, such as grades and academic schedules are processed against the proper applicant / student account.

Faculty and staff are briefed on Privacy Act information disclosures, but must provide the required information to be given access to government systems, a requirement for employment at the CGA.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right.

Individuals may choose to not participate in any CGA programs, and CGA use of the information provided will conform to the requirements of the SORN under which the information was collected. Once collected, though, individuals are not given specific choices as to how the information is used within the aforementioned parameters.

After graduation, training records and transcripts are only provided externally at the signed request of the former cadet, though such records may be used internally as allowed under the Military Pay and Personnel System SORN.

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.

Cadets are made aware of the collection of their information when they apply for admission to the CGA. Faculty and staff are also made aware of the collection of their information to facilitate their access to the ACADIS system and annually review a standard Coast Guard User Acknowledgement Form and Automated Information System brief describing their liabilities and restrictions in accessing a government information system. In addition, this PIA provides additional transparency and notice to individuals about the collection of their information, thus there is little risk that individuals are unaware of the collection of their information.

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 which allow individuals to gain access to their own information?

Applicant: Applicants can engage the Admissions office to validate their data at any time.

Cadet: Active cadets have access to their personal profile, from any CGA educational computer which allows them to verify their own data. While their personal profile is readily available, some fields, such as disciplinary and academic standings are not, however they can engage advisors or company officers to view this additional information as necessary.

Faculty and Staff: Faculty and staff are able to view their own personal data via the system entrance screen. They may request changes to this information at any time by contacting the CGA Help Desk.

Additionally, applicants, cadets, faculty and staff may request copies of their records from ACADIS via the Freedom of Information Act/Privacy Act at the following address:

Superintendent
U.S. Coast Guard Academy
15 Mohegan Ave
New London, CT 06320-8100

7.2 What are the procedures for correcting erroneous information?

As a precaution, applicant information is researched, verified, and corrected by the Admissions office as necessary. Actual data entry for corrections is accomplished through the CGA Help Desk. Corrections are submitted to the Help Desk via the CG Help trouble ticket system,[2] a technician then assigned the ticket to the appropriate database administrator who verifies the correction and updates the appropriate record(s). The person submitting the request is then notified by email, through the helpdesk system that the correction has been made.

Erroneous information on active cadets, faculty and staff is corrected through the same process, but research, verification and correction is conducted by the information services staff in conjunction with the data owner (i.e. Registrar for academic information, Commandant of Cadets for military information, etc).

Erroneous information for past cadets is corrected via a formal review process by the Registrar.

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

As part of their familiarization training, cadets are instructed when their account is established, that required corrections need to be reported to cadet admininstrators or an advisor who will assist them with getting the information corrected. There is no "self service" correction currently available.

7.4 If no redress is provided, are alternatives are available?

[2] Help desk trouble ticket systems are covered by the General Information Technology Access Account Records SORN, DHS/ALL-004, September 29, 2009, 74 FR 49882.

Redress is provided as described in sections 7.1 and 7.2.

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

Risks associated with the potential inaccuracies in the ACADIS system are mitigated in that opportunities are provided to cadets, faculty, and staff to review and correct their data as desired. There is no established review process by CGA to validate the data on a regular basis. Stringent review is conducted on entry of Academic and military data, but once entered, the data is accepted to be correct unless reviewed by a cadet or advisor or if a request is made to check accuracy or any data. Any changes or corrections to information require the cadet to physically visit the CGA Help Desk or Cadet Administration office with appropriate documentation, such as military ID card, records will then be manually corrected through the CGA Help Desk system by opening a trouble ticket with the appropriate database administrator to correct the impacted fields.

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.

There are procedures in place to ensure proper access to the system. The general public has no access to the system. Access for internal users is based on a role assignment determined by application owners. Prior to accessing ACADIS all users must complete a background check (per DHS regulation), complete AIS awareness training, sign an AIS Security brief and be granted access to the educational or military network at CGA. Once such access is granted, the user requests ACADIS access through their supervisor who establishes the roles they are required to perform and access they should have.

Users from other agencies do not have access to the system.

Most user roles have "read-only" access. Only a few roles allow entry or updating of any information. Much of the information entered into the system goes through the information services staff.

8.2 Will Department contractors have access to the system?

Yes. The CGA Information Services staff is made up of contract employees. The Information Services contract is reviewed and updated on a continuing basis by the Information Division. All contract staff are required by their contract to possess and maintain a secret security clearance.

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

All users must sign an Acceptable Use Policy annually. Military, civil service, and contract personnel also participate in mandatory USCG/DHS security and privacy training.

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

Yes. Certification and Accreditation was completed and granted a three year authority to operate dated 3 May 2007.

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

All application accesses are logged in the system. The database itself is only accessed via username and password authentication, and only from internal CGA computer systems. All servers are located in the CGA Data Center, a restricted area designated by the command, this data center is equipped with and Intrusion Detection System which notifies security in the event of an unauthorized entry, the facility is also equipped with video surveillance.

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?

Risks against unauthorized access to data are mitigated by access controls in place that limit access to specific users. New requests for data access go through a formal process of review by information services and data owners/managers. Additionally, formal review is conducted by management staff to continuously validate the need to provide private/personal information to those users. Access limitations and reductions in data availability are made as appropriate.

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 ACADIS system was built from the ground up as an infrastructure tool to support admissions, academic, and support activities at the Coast Guard Academy.

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

The ACADIS system is a production system in a maintenance cycle. An incremental development lifecycle was used.

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

ACADIS does not employ technology that raises privacy concerns. Data entry capabilities are strictly limited to controlled groups. This enhances data integrity. Data views are also closely controlled by user roles to maintain privacy of the data. System security is a top priority that is given first consideration in all steps of the system life cycle. Auditing logs were created to track usage of data. Usernames and passwords were implemented to control access privacy concerns.

Only the Admissions application is accessible through the Internet, and that is only for data entry and secured with SSL.

Appendix I:

Academy Information System (ACADIS) Privacy Act Statement

AUTHORITY: 14 USC §§ 181-195, US Coast Guard Academy Recruiting Plan

PURPOSE: Applicants: To obtain necessary information to solicit and process applications for admission to the US Coast Guard Academy. Cadets: Information is primarily used for academic purposes such as tracking grades, classes, and payroll. All Others: Information is primarily used for identity verification and granting access to the system.

ROUTINE USE: No disclosure of this information will be made outside of the Department of Homeland Security or Department of Defense.

DISCLOSURE: Applicants: Voluntary however, if you do not provide the information, we will be unable to process your application. All others: Disclosure is a condition of attendance or employment.

Responsible Officials

ITCS Guy O. Cranfill, ISSO

United States Coast Guard

Department of Homeland Security

Approval Signature Page

Original copy signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security