OFFICE OF INSPECTOR GENERAL

The Security Posture of the United States Coast Guard's Biometrics At Sea System Needs Improvements

Homeland Security

March 3, 2015

OIG-15-41

HIGHLIGHTS

The Security Posture of the United States Coast Guard's Biometrics At Sea System Needs Improvements

March 3, 2015

Why We Did This

The United States Coast Guard (USCG) operates the Biometrics at Sea System (BASS) to collect biometric data from interdicted aliens. The biometrics are sent to the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) to identify potential persons of interest, including suspected terrorists. We audited BASS interface with IDENT, security roles and responsibilities, and change control management.

What We Recommend

We made seven recommendations to USCG to perform reconciliation with IDENT, update security documents, eliminate use of common passwords, and ensure adherence to change management policies.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

We determined that USCG did not have a routine reconciliation process to ensure that all biometrics that it captured on the 23 cutters are maintained in IDENT. Not ensuring reconciliation between the total biometrics USCG submitted and the number stored in IDENT may impede future identification of suspected terrorists, aggravated felons, or other individuals of interest. USCG also allowed application programmers with unrestricted system access to share passwords. The control weakness may result in individuals making unauthorized changes to the system without detection. Further, we determined that the authorization for the transition from the 2-fingerprint to 10-fingerprint application system was not properly documented and security documentation had not been updated. Without a proper authorization process, USCG could not provide assurance that senior executives approved the change prior to implementation.

USCG Response

USCG concurred with all seven recommendations. USCG proposed to establish a BASS aggregate control log to verify the total number of biometrics entries sent to and received by IDENT. USCG had defined security roles and responsibilities in its *Information Security Assurance Manual,* but will further clarify roles and responsibilities as part of the new Security Authorization process starting in March 2015. As part of this process, USCG will prepare requisite security documentation. Further, USCG will ensure that the configuration change management policies are redistributed and followed.

Table of Contents

Appendices

Abbreviations

AMIO	Alien and Migrant Interdiction Operations
BASS	Biometrics at Sea System
CCB	Configuration Control Board
C3CEN	Command, Control, and Communications Engineering Center
DHS	Department of Homeland Security
FISMA	*Federal Information Security Management Act of 2002*
IACS	Information Assurance Compliance System
IDENT	Automated Biometric Identification System
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
OBIM	Office of Biometric Identity Management
OIG	Office of Inspector General
SDLC	System Development Life Cycle
USCG	United States Coast Guard

Results of Audit

The United States Coast Guard (USCG) conducts a program to identify individuals, including suspected terrorists, in the maritime environment.[1] Specifically, the USCG operates the Biometrics At Sea System on 23 of its ships (cutters) to collect biometric data from thousands of individuals the USCG interdicted attempting to enter the U.S. illegally. The USCG sends the biometrics to the Department of Homeland Security's (DHS) Office of Biometric Identity Management, which compares the biometrics against records in the Automated Biometric Identification System. In March 2013, USCG started upgrading the Biometrics at Sea System from a 2-fingerprint to a 10-fingerprint system to comply with standards for biometric identification.[2]

We designed our audit to determine whether the USCG has implemented 1) proper controls to monitor the quality of the Biometrics At Sea System's interface with the Automated Biometric Identification System; 2) effective security management controls to protect the integrity of the Biometrics At Sea System, and 3) an effective change management process to implement the 10-fingerprint standard.

We found that USCG did not have a routine reconciliation process to compare the aggregate total number of biometrics USCG captured and sent to the Automated Biometric Identification System for all cutters. Not ensuring that the USCG-submitted biometrics are reasonably complete in the Automated Biometric Identification System may impede future identification of suspected terrorists, aggravated felons, or other individuals of interest. In addition, USCG did not have sufficient security management controls, such as an updated system security plan. USCG allowed application programmers with unrestricted system access to share passwords and did not clearly define system roles and responsibilities in the security plan. These control weaknesses may result in individuals making unauthorized changes to the system without detection. We also found that USCG did not properly document

[1] Public Law 111-281; 46 U.S.C. § 70123.
[2] *Homeland Security Presidential Directive-24* calls for Federal agencies to use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals.

its authorization for the Biometrics At Sea System to transition from 2-fingerprint to 10-fingerprint capture. Without a proper authorization process, USCG could not provide assurance that senior executives approved the change prior to implementation.

We made seven recommendations that should enhance USCG's security over the Biometrics At Sea System information technology.

Background

USCG safeguards our Nation's maritime interests and environments in ports, at sea, and around the globe. In the course of operations, USCG encounters thousands of aliens of unknown identity through various interdiction and verification programs. Some may be known or suspected terrorists, aggravated felons, individuals previously ordered to be deported, or individuals already deported from the United States.

Federal law requires that USCG conduct a program for the mobile identification of individuals, including terrorists, in the maritime environment.[3] USCG implemented the Biometrics At Sea System (BASS) on 23 of its cutters in the District 7 Area of Responsibility to assist in meeting this requirement.[4] USCG uses BASS to collect and send biometric information to DHS' Automated Biometric Identification System (IDENT), a repository of biometric and associated biographic data used for, among other purposes, national security, law enforcement, and immigration and border management.[5] DHS' Office of Biometric Identity Management (OBIM) maintains IDENT.

BASS consists of a portable handheld device to capture fingerprints, a laptop, and an encrypted hard drive. The BASS process works as follows:

- During Alien and Migrant Interdiction Operations (AMIO), authorized personnel on board a USCG cutter personnel issue a numbered armband to the intercepted alien. This armband serves as the main identifier linking the alien to the captured biometrics and biographic information (name, date of birth, sex, and nationality). Authorized personnel record the biographic information in an AMIO log.
- Authorized personnel use the handheld device to collect fingerprints and capture a facial image of aliens the USCG intercepted during AMIO.

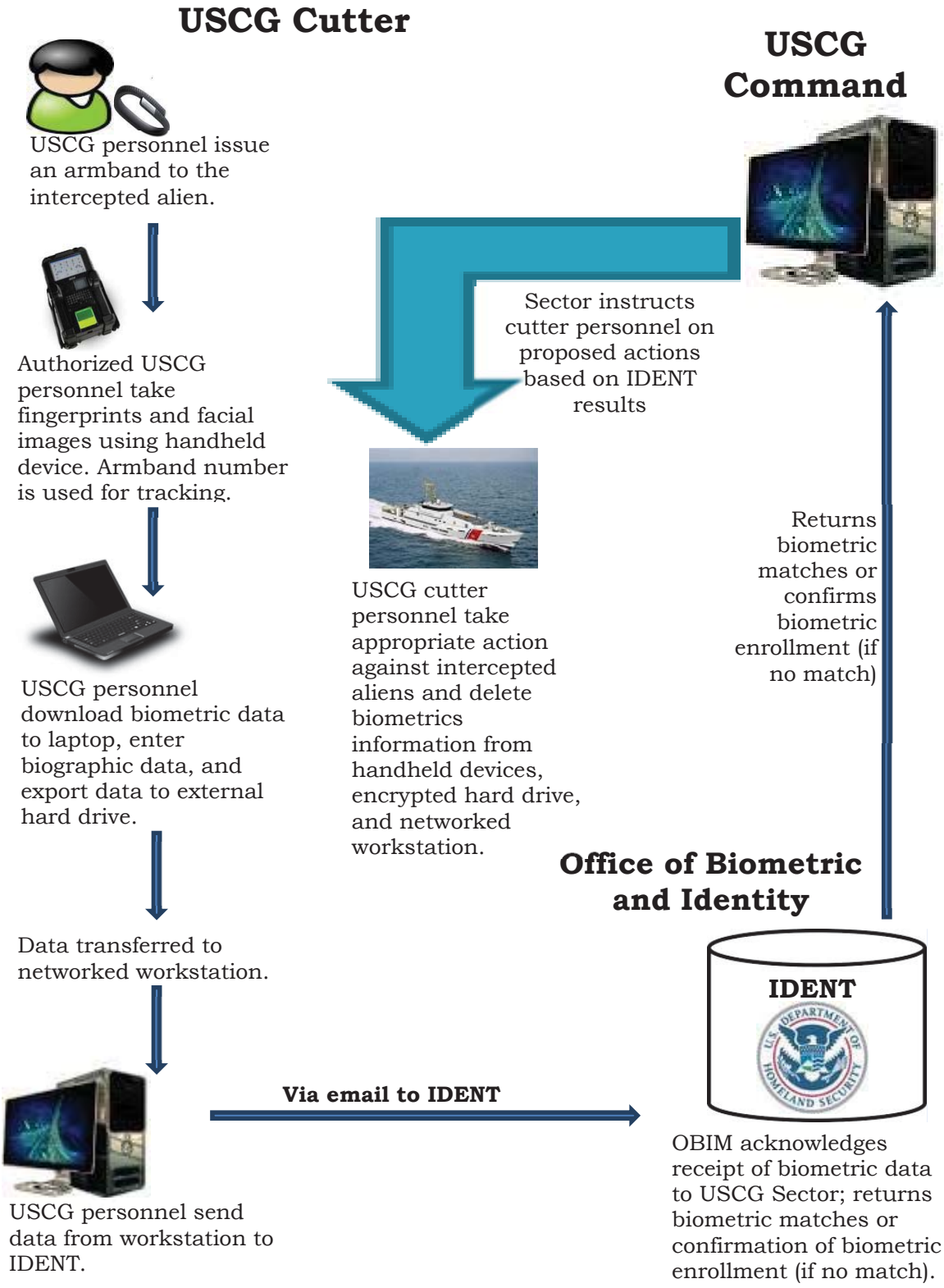
[3] Public Law 111-281; 46 U.S.C. §70123.
[4] Other USCG biometrics components include the Transportation Worker Identification Credentials Program, which the Transportation Security Administration administers, and the Biometrics-Enabled Identity Intelligence program.
[5] The Office of Biometric Identity Management (OBIM), formerly US-VISIT, manages IDENT. IDENT stores and processes biometric data—digital fingerprints, photographs, iris scans, and facial images—and links biometrics with biographic information to establish and verify identities. On behalf of USCG, OBIM shares biometrics information with authorized users for national security, law enforcement, immigration, intelligence, and other DHS mission-related functions that require its use to identify or verify the identity of individuals.

- The handheld device has built-in algorithms to recognize whether a fingerprint meets acceptable handheld device standards, i.e., is a good print. If the fingerprint does not meet standards, the handheld device prompts USCG personnel to retake the print. If the second fingerprint is not acceptable, a third is required.
- USCG personnel download captured biometrics to a dedicated laptop and enter biographic information. A laptop formats the data and exports the records to an encrypted external hard drive.
- USCG personnel transfer the biometric and biographic information to a USCG networked workstation and email it to IDENT.
- IDENT automatically compares the biometrics received from USCG against existing biometrics within the IDENT database and sends a match or no match response to the appropriate USCG Command Center—a shore-based operational unit that supports and coordinates cutter operations. This response serves as a confirmation from IDENT that it has received and compared the biometric information against existing information in its database. When there is no match, IDENT enrolls the new biometrics in its database.[6]
- In the event that IDENT encounters an issue with the captured biometrics, IDENT automatically sends the issue to the USCG Command Center and the BASS system support agent at the Command, Control, and Communications Engineering Center (C3CEN) to resolve the issue. The Command Center may instruct personnel on the cutter to retake the fingerprint if necessary to complete the identification and enrollment process.
- Depending on the result of the IDENT match, the USCG Command Center instructs cutter personnel to detain the alien for prosecution, repatriate the alien, or take other appropriate actions.
- Biometric and biographic information from BASS is stored in IDENT. USCG clears all biometric data from the handheld devices, encrypted hard drives, and networked workstations once IDENT receives and acknowledges the results.

Figure 1 illustrates the process.

[6] In a biometric security system, enrollment refers to the initial process of collecting biometric data samples from a person and subsequently storing the data in a reference template representing an individual's identity that the organization uses later for comparison against other biometric data.

Figure 1. BASS Biometric Capture Process



Source: Coast Guard and Office of Inspector General (OIG) Analysis

Homeland Security Presidential Directive 24, issued June 5, 2008, "establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law." The Directive describes standards for biometric identification. In August 2012, USCG piloted a program to upgrade the collection of biometric information from a 2-fingerprint to a 10-fingerprint system. In March 2013, USCG started implementing the 10-fingerprint capability across the 23 cutters. The 10-fingerprint system allows the capture of all 10 fingerprints, comparable to the standard fingerprint captured by most law enforcement agencies.

USCG Did Not Routinely Reconcile Biometrics Information with IDENT

USCG did not have controls to monitor the quality of the BASS interface with IDENT. Specifically, USCG did not maintain an independent, aggregate count of the total number of biometrics sent to IDENT and did not perform routine reconciliations to validate that the biometric data posted to IDENT were reasonably complete. USCG officials cannot provide assurance that the number of biometrics stored in IDENT is complete. Consequently, USCG and other law enforcement agencies are hampered in their ability to properly identify whether intercepted persons are known or suspected terrorists, aggravated felons, or individuals previously ordered to be deported or already deported from the United States.

According to Federal standards and the National Institute of Standards and Technology (NIST), reconciliations allow agencies to ensure the integrity, accuracy, and completeness of data.[7] A regular reconciliation process assists agencies in promptly identifying issues and taking corrective actions.

[7] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* and OMB Circular A-123, *Management's Responsibility for Internal Control,* December 21, 2004.

USCG did not have procedures to compare the total number of biometrics the 23 cutters captured against numbers IDENT reported. According to USCG personnel, each Command Center maintains a daily count of biometric activities. USCG also receives an acknowledgement from IDENT each time IDENT receives a biometric capture from USCG. The confirmation provides USCG assurance that IDENT has received and compared the biometric capture against existing information in its database. However, USCG did not have a process to routinely and periodically compare the aggregate total number of biometrics all 23 cutters transmit to IDENT to the number IDENT reports as having received and posted to its database. A routine reconciliation process will assist USCG in identifying and ensuring that the data it transmits to IDENT are reasonably accurate and complete.

USCG did not implement a regular reconciliation process because there was confusion as to the owner of the biometrics information sent from the cutters. At the beginning of this audit, USCG officials stated that they did not own the biometrics captured, and had no further responsibility after the biometric information left the cutters. Subsequent to our additional discussions with OBIM officials, USCG officials acknowledged ownership of the data.

Because it did not maintain its own aggregate count, USCG was unable to explain the source of the difference between the number of BASS entries maintained in IDENT and a revised number used frequently for reporting purposes. Specifically, an OBIM official originally reported to us that IDENT contained over 4,600 BASS transactions from October 2006 through May 2013. Subsequently, despite the fact that USCG did not maintain its own aggregate count, the same OBIM official provided a report prepared by USCG stating that the transactions totaled over 5,100 transactions, an almost 10 percent discrepancy. USCG officials who relied on the OBIM totals attributed the discrepancy to a system error at the beginning of the BASS program. However, despite repeated requests for documentation, USCG officials did not provide us with evidence as to why the discrepancy occurred.

Without periodically comparing totals and resolving discrepancies as they arise, USCG officials cannot provide assurance that the number of biometrics USCG submitted to IDENT matches the number of biometrics stored in IDENT as USCG submissions. When system interruptions, communication failures or other events occur that result in a discrepancy in IDENT, USCG would not

have the ability to positively identify or cross-reference encountered individuals with information available in law enforcement databases.

Recommendation

We recommend that the USCG Chief Information Officer:

Recommendation #1:

Establish a BASS aggregate control log to verify biometric transactions from the 23 cutters, and perform periodic reconciliation with IDENT.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the USCG Assistant Commandant for Resources and Chief Financial Officer. We have included a copy of the comments in their entirety at appendix C. We also obtained technical comments on the draft report, which we incorporated in the final report where appropriate. The USCG Assistant Commandant for Resources and Chief Financial Officer concurred with all recommendations.

USCG Response to Recommendation #1: USCG concurs with this recommendation. The USCG proposes to establish a BASS aggregate control log of all 23 cutters to verify the total number of biometric entries sent to and received by IDENT. According to USCG's response, USCG did not believe that "maintenance of biometric/biographic data for long-term reconciliation" is feasible due to privacy, storage, and resource issues.

OIG Analysis: The actions USCG proposes satisfy, in part, the intent of the recommendation. To fully satisfy this recommendation, USCG should take additional steps and use the aggregate control log as a tool to assess the reasonableness of the numbers that IDENT reports periodically. This recommendation is considered unresolved and will remain open until USCG provides documentation that the planned corrective actions are completed, as well as a plan for implementing procedures to periodically compare the total number of biometrics USCG captures against IDENT-reported numbers.

BASS Security Management Needs Improvement

USCG did not have effective security management controls to protect the integrity of BASS. Specifically, USCG did not have up-to-date security documentation, allowed shared passwords among privileged users, and did not clearly define system roles and responsibilities between information security and program development personnel. Without effective security controls, USCG risked exposing BASS to security risks that can adversely impact the system's integrity.

Up-To-Date BASS Documentation Was Not Prepared

NIST standards require that organizational officials review all security plans and update them when significant changes occur, if appropriate, to reflect system and organizational changes, problems identified during plan implementation, and security control assessments or audit reports.[8]

We found that USCG did not have updated security documentation for BASS, including the System Security Plan, Security Impact Analysis, and the BASS Interface Control Agreement. USCG started implementing the 10-fingerprint system across 23 USCG cutters in March 2013. As of May 2014, 15 months after the migration, USCG had not updated the BASS System Security Plan to reflect the 10-print operational environment. In addition, despite repeated requests, USCG did not provide us with an approved System Security Plan for the previous 2-fingerprint system. A System Security Plan provides a blueprint for a system's overall security and communicates to system personnel the security controls that are in use, or the security controls management plans to use, to protect all aspects of the system.

The BASS Information System Security Officer (ISSO) recognized the need to maintain an up-to-date System Security Plan, but partly attributed the limited progress in completing the plan to a new DHS mandate. Specifically, in September 2013, DHS required that DHS Components update all critical systems needing certification and accreditation in a new risk management and compliance system called the Information Assurance Compliance Systems

[8] NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

(IACS).[9] However, the DHS Chief Information Security Officer designed the new risk management system so that DHS components could not update a security plan (or other security and system documentation) without recording a new certification and accreditation, even if one was not necessary. The official informed us that recording a new certification and accreditation would trigger a predetermined set of timelines that, if not met, would affect USCG's score on its *Federal Information Security Management Act* (FISMA) compliance. Consequently, USCG was in the process of determining how to best generate security plans without adversely affecting its FISMA compliance. According to the official, this effort was not restricted to BASS but was applied to a number of systems impacted by the new DHS mandate.

We also found that USCG had not prepared a Security Impact Analysis for the transition from the 2-print to 10-print application system. The ISSO typically conducts a Security Impact Analysis to determine the extent to which changes to an information system affect the security posture of the system. Without a security impact analysis, USCG could not provide assurance that it 1) identified and considered all threats and vulnerabilities, 2) identified the greatest risks, and 3) made appropriate decisions regarding which risks to accept and which to mitigate through security controls. The transition from 2-print to 10-print necessitated a change in BASS' software, hardware, vendor, and bandwidth. These changes should have resulted in the application of DHS *Sensitive Systems Policy Directive 4300A, Section 3.9.h*, which requires components to authorize systems every 3 years or whenever a major change occurs, whichever occurs first.

We further found that an updated agreement does not exist to describe the software and hardware for the 10-fingerprint process. The BASS Interface Control Agreement, used to document the agreement between USCG and IDENT related to the transfer of biographic data, was outdated. It detailed, among other things, the process by which biometric information would flow from USCG to OBIM, and the process by which OBIM would match and/or enroll the fingerprints of individuals that USCG interdicted. OBIM issued the agreement on December 7, 2011, which covered the 2-fingerprint system.

[9] Certification and Accreditation is a systematic process for evaluating, describing, testing, and authorizing systems or activities prior to or after the authorizing official place a system in operation. Information system and information security professionals from around the world use this process.

Outdated documentation crucial to ensuring the security of BASS and the integrity of data flow could be indicative of a need for improved management monitoring and attention to BASS operations. USCG management designed BASS to assist in the identification and capture of biometric information from intercepted aliens who could be potentially dangerous, persons of interest, or repeat offenders. USCG needs to ensure that BASS is secure and its data are complete and accurate, which is crucial to USCG's AMIO activities.

Management of Administrative Passwords Can Be Improved

The *DHS Sensitive Systems Policy Directive 4300A* requires that DHS Components protect information systems from unauthorized access. It states that DHS users shall not share personal passwords. Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. According to the directive, the authorizing official needs to approve specifically the use of a group user ID and password.

We found that 13 C3CEN individuals in system development and system support functions used a common password to access administrator accounts for BASS.[10] These administrator accounts provide unrestricted and unlimited access, giving system administrators control over the systems they are managing. This includes the ability to change security settings, install software and hardware, make changes to user accounts, and access all files. We did not find formal approval for use of a group password for the C3CEN programmers.

USCG officials we met with believed the risk of allowing a common password was minimal as BASS is a stand-alone system application not connected to USCG's network. However, the *Federal Information System Controls Audit Manual* states that users and devices should be appropriately identified and authenticated through the implementation of adequate logical access controls. User authentication establishes the validity of a user's claimed identity, typically during access to a system or application (for example, login). If more than one person knows a password, USCG management cannot enforce a user's responsibility for all activity within an account. The SANS Institute, a private U.S. company that specializes in Internet security training, determined

[10] C3CEN develops, builds, fields, trains, and supports advanced electronic command, control, and navigations systems. It provides design, maintenance, and troubleshooting assistance on its assigned systems.

that shared passwords on privileged accounts create unacceptable risk by allowing individuals to, among other things, breach personal data, complete unauthorized transactions that can be used to cause denial of service activities, and hide these activities by deleting audit data. For example, a disgruntled employee in possession of a shared password can make unauthorized system changes, or share the passwords with unauthorized outside parties without USCG management identifying the responsible individual. Implementing controls over these accounts is necessary to ensure the integrity of USCG information systems.

Confusion Exists as to Roles and Responsibilities, and Segregation of Duties Needs Improvements

We found that USCG can improve on its communication and enforcement of BASS ownership responsibilities. Despite DHS requirements, we also found inadequate segregation of duties between C3CEN staff and the ISSO. As a result, unauthorized changes or modification to data and programs may occur and not be detected.

DHS Sensitive Systems Policy Directive 4300A states that the proper administration of security requires that all systems have, in writing, a designated system owner. A clearly designated owner plays an instrumental role in ensuring that systems operate effectively. However, we found that USCG can improve the ways in which it designated BASS ownership and communicated that designation. Although the USCG's *C4&IT System Development Life Cycle Designation for the Biometrics at Sea System* appointed the Law Enforcement Policy Directorate as the designated BASS sponsor (system owner), throughout the audit, we found that there was often confusion as to the identity of the designated owner. USCG officials we met with informed us that BASS operated under the management of three different units, with different understanding of ownership responsibilities. Without clear communication and enforcement of management responsibilities, USCG risks not having the appropriate oversight and control of BASS.

Further, OMB Circular A-130 states that the rules of the system and application shall clearly delineate responsibilities and expected behavior of all individuals with access. Security guidance and job descriptions assign ISSO key roles in ensuring the confidentiality, integrity, and availability of the DHS

information technology security programs, systems, applications, and infrastructure.

However, we found that the BASS ISSO did not perform some of the tasks typically associated with an ISSO's security function. For example, the BASS ISSO did not exercise oversight over the issuance and maintenance of BASS authorized user IDs and passwords or monitor access rights/privileges for users and programming staff. Instead, the C3CEN's system development agents and system support agents carried out these functions. USCG management defined these individuals' responsibilities to include application programming support (development and maintenance) and technical expertise for design, integration, and implementation of systems.

Allowing system development and support staff to perform ISSO functions resulted in improper segregation of duties. Without proper segregation of duties, individuals can make unauthorized or erroneous changes to data and programs that could remain undetected.

We also found that the segregation of duties between the system development and system support functions was weakened by the use of a common password discussed in the previous section. System development agents are responsible for program design and testing while system support agents are responsible for program implementation and maintenance. Testing and implementation are generally two separate functions designed so that one person cannot perform the diverse and critical functions and cause errors that would remain undetected in a timely manner. However, as discussed previously, all 13 individuals in the C3CEN core technology group, whether in the testing or implementation function, shared the same administrative user password. The administrative user password allowed access to BASS' operating system so that any of the 13 users could make changes to BASS without the changes being logged to a specific individual. The failure to ensure segregation of duties between development and support functions through the use of common passwords may result in system developers making unauthorized changes to the production environment, thereby adversely impacting the integrity of BASS.

Recommendations

We recommend that the USCG Chief Information Officer:

Recommendation 2:

Update the BASS Security Plan, Security Impact Analysis, and Interface Control Agreement, including ensuring that security controls are consistent with appropriate security requirements.

Recommendation 3:

Limit the use of common passwords and, if common passwords are necessary, establish compensating controls to limit the risks associated with them.

Recommendation 4:

Define BASS system owner responsibilities in the security plan.

Recommendation 5:

Define the roles and responsibilities of the BASS Information System Security Officer and the Command, Control, and Communications Engineering Center Support and Development programming staff, and address issues with segregation of duties.

Management Comments and OIG Analysis

USCG Response to Recommendation #2: USCG concurs with this recommendation. USCG said that it will prepare the BASS Security Plan, Security Impact Analysis, and Interface Control Agreement as part of the new Security Authorization slated to begin in March 2015.

OIG Analysis: The actions USCG intends to take in fiscal year 2015 begin to satisfy the intent of this recommendation. This recommendation is considered open and resolved until USCG provides documentation that the planned corrective actions are completed.

USCG Response to Recommendation #3: USCG concurs with this recommendation. USCG plans to incorporate unique administrative user names and passwords in future versions of BASS, to be completed by May 2015.

OIG Analysis: The actions that USCG proposes satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCG provides documentation that the planned corrective actions are implemented.

USCG Response to Recommendation #4: USCG concurs with this recommendation. USCG has identified system owner responsibilities in the *USCG Security and Information Assurance Manual*.

OIG Analysis: Defining owner responsibilities in the *USCG Security and Information Assurance Manual* satisfies the intent of this recommendation. This recommendation is considered closed.

USCG Response to Recommendation #5: USCG concurs with this recommendation. USCG said that it had defined roles and responsibilities in the *USCG Security and Information Assurance Manual*. In addition, it will clarify responsibilities for assigning and managing system passwords in the BASS Security Plan during the next Security Authorization process.

OIG Analysis: The actions that USCG proposes satisfy, in part, the intent of this recommendation. The USCG should also implement processes to ensure that the roles and responsibilities defined in the *USCG Security and Information Assurance Manual* are communicated and followed. This recommendation is considered unresolved and will remain open until USCG provides documentation that the planned corrective actions are completed.

USCG Did Not Implement Effective BASS Change Management Procedures

USCG did not implement an effective change management process for the transition to the 10-fingerprint process. Specifically, the USCG change management request form did not include all required signatures to move to the new 10-fingerprint environment and also created confusion for users. As a

result, USCG had no assurance that the changes were approved and communicated to all affected parties.

According to the USCG Systems Development Life Cycle (SDLC), to proceed from one phase of an SDLC to the subsequent phase, all activities and products specified in the SDLC Tailoring Plan for each phase must be completed, reviewed through a Phase Exit Review, approved by the designated approval authority, and documented. Further, the NIST *Guide for Security-Focused Configuration Management of Information Systems* recommends the use of Secure Change Management practices, including a Configuration Control Board (CCB) to review and approve changes to an information system.[11]

We found that the BASS CCB did not maintain proper documentation showing that the change from the 2-fingerprint to 10-fingerprint system was properly authorized. Specifically, the authorization form for BASS did not contain the signatures of all USCG representatives identified as required signatories. For example, at one point in the audit, the CCB form provided to us contained only the signature of a representative of the BASS contractor, who was not one of the parties previously identified as signatories. After repeated requests, USCG provided us with an updated form containing the signature of one member of the BASS CCB, despite the CCB form requiring signatures from several different commands. The CCB form did not contain signatures of senior executives authorizing the transition.

In addition, the BASS CCB Authorization Form did not contain the requestor's name or the requested implementation date. Despite repeated requests, USCG was not able to provide us with the BASS CCB minutes or other documentation indicating that BASS CCB formally approved the change.

The current form created confusion for some users because it contained three separate, distinct approval processes, including 1) change management request, 2) user acceptance, and 3) project authorization. The USCG Configuration Policy had delegated responsibilities for preparing the change management form to each Center of Excellence. In its delegation to BASS, USCG did not set minimum standards as to what the CCB Authorization

[11] Special Publication 800-128, *Section 2.2.3, Controlling Configuration Changes* and *2.3.3 Configuration Control Board.*

Form for BASS should contain. Without a properly completed change management request, USCG had no assurance that the assigned officials approved and communicated the change to all affected parties.

Recommendations

We recommend that the USCG Chief Information Officer:

Recommendation 6:

Issue minimum requirements for the BASS CCB authorization form used to document change management approval.

Recommendation 7:

Establish standards requiring that BASS properly document authorization for system changes.

Management Comments and OIG Analysis

USCG Response to Recommendation #6: USCG concurs with this recommendation. USCG will ensure that the configuration change management policies are redistributed and followed.

OIG Analysis: The actions that USCG proposes, particularly its proposed actions with respect to ensuring that USCG change management policies are followed, satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCG provides documentation that the planned corrective actions are implemented.

USCG Comments to Recommendation #7: USCG concurs with this recommendation. USCG will ensure that the configuration change management policies are redistributed and followed.

OIG Analysis: The actions that USCG proposes, particularly with respect to ensuring that USCG change management policies are followed, satisfy the intent of this recommendation. This recommendation is considered resolved, but will remain open until USCG provides documentation that the planned corrective actions are implemented.

Appendix A

Transmittal to Action Official

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security
Washington, DC 20528 / www.oig.dhs.gov

March 3, 2015

MEMORANDUM FOR: Rear Admiral Todd Sokalzuk
Chief Financial Officer and Assistant
Commandant for Resources
United States Coast Guard

FROM: Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *The Security Posture of the United States Coast Guard's Biometrics at Sea System Needs Improvements*

Attached for your action is our final report, *The Security Posture of the United States Coast Guard's Biometrics at Sea System Needs Improvements*. The report identified measures USCG can take to enhance the program's overall effectiveness.

Please provide our office with a written response within 90 days that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. The OIG considers recommendation 4 closed, recommendations 2, 3, 6 and 7 open and resolved, and recommendations 1 and 5 open and unresolved. Please email a signed pdf copy of responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Refer to the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations* for guidance on audit resolution.

Please call me with any questions, or your staff may contact Tuyet-Quan Thai, Director, Forensics Division, at (425) 582-7861.

Appendix B

Scope and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

We audited the BASS/IDENT reconciliation process, security management, and documentation of change management operations. We interviewed USCG officials from Headquarters and Centers of Excellence in Virginia and Connecticut and OBIM staff regarding the interface between BASS and IDENT. We examined the system owner involvement in BASS application process. We reviewed relevant criteria, policies, procedures and conducted a walkthrough of the internal control process for mobile biometrics.

We based our audit methodology for testing BASS general and application controls on the Government Accountability Office's *Federal Information System Controls Audit Manual*. The Manual presents a methodology for performing information system (IS) control audits of Federal and other governmental entities in accordance with professional standards the Government Accountability Office originally issued in January 1999. Specifically, this audit methodology incorporates IS controls for business process applications that are consistent with generally accepted government auditing standards and current with NIST and Office of Management and Budget information security guidance (including all NIST Special Publication 800-53 controls).

We conducted this performance audit between December 2013 and August 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the cooperation by USCG management and staff in providing the information necessary to accomplish this audit.

Appendix C

USCG Comments to the Draft Report

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King, Jr. Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-8
Phone: (202) 372-3533
Fax: (202) 372-4960

5730
15 September 2014

MEMORANDUM

From: T. A. Sokalzuk
COMDT (CG-8)

Reply to Attn of: Audit Manager
Mark Kulwicki
(202) 372-3533

To: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

Subj: DHS OIG DRAFT REPORT: THE SECURITY POSTURE OF THE U.S. COAST GUARD'S BIOMETRICS AT SEA SYSTEM NEEDS IMPROVEMENTS

Ref: (a) OIG Project No. 14-009-ITA-USCG of August 12, 2014

1. This memorandum transmits the Coast Guard's response to the draft report identified in reference (a).

2. The Coast Guard concurs with all the recommendations listed in the draft report. Our response in enclosure (1) demonstrates that the Coast Guard has measures in place to ensure that the Biometrics at Sea System (BASS) program is managed properly and information is properly protected. Accordingly, the Coast Guard requests that you consider recommendation four as Closed and Implemented.

3. If you have any questions, my point of contact is Mr. Mark Kulwicki who can be reached at 202-372-3533.

#

Enclosure: (1) USCG Response to OIG Draft Report on BASS

UNITED STATES COAST GUARD STATEMENT ON DHS OIG DRAFT REPORT: THE SECURITY POSTURE OF THE U.S. COAST GUARD'S BIOMETRICS AT SEA SYSTEM NEEDS IMPROVEMENT
OIG Project No. 14-009-ITA-USCG

OIG Recommendation #1: Establish a Biometrics At Sea System (BASS) aggregate control total log and procedures to perform routine reconciliations with the information in IDENT to ensure that all data from USCG cutters capable of performing mobile 10-fingerprint biometrics collection at sea has been captured by IDENT.

Response: Concur. The Coast Guard (USCG) will establish a BASS aggregate control log that will enable USCG cutters capable of performing mobile 10-fingerprint biometrics collection at sea to verify the total number of biometrics entries sent to and received by IDENT. "Result Messages" that are transmitted from IDENT to the USCG for each biometric file sent to IDENT will continue to serve as verification that IDENT has received, processed and stored the biometric information in accordance with the Interface Control Agreement (ICA). The Coast Guard will enter this confirmation in the aggregate control log. The Coast Guard believes this action will sufficiently address the recommendation by OIG to perform routine reconciliation of biometrics data sent to IDENT. Maintenance of biometric/biographic data for long-term reconciliation would create a bevy of privacy, data storage and system configuration concerns that would necessitate a complete overhaul of the BASS program—an initiative the Coast Guard is not currently resourced to perform. Estimated completion date is May 2015.

OIG Recommendation #2: Update the BASS Security Plan, Security Impact Analysis and Interface Control Agreement including ensuring that the security controls are consistent with appropriate security requirements.

Response: Concur. BASS is scheduled to begin a new Security Authorization (SA) in March of 2015. Using the new XACTA tool the SA is estimated to take up to 12-months to complete. The SA will evaluate the system for risk using the latest and most up to date security controls mandated by the Department of Homeland Security (DHS) and the USCG. The BASS Security Impact Analysis and Interface Control Agreement will be updated during that process. The SA's estimated completion date is May 2016.

OIG Recommendation #3: Limit the use of common passwords and, if common passwords are necessary, establish compensating controls to limit the risks associated with them.

Response: Concur. Current BASS system architecture requires unique individual user accounts and passwords and proposed future versions of the BASS system will incorporate unique admin user names and passwords. Estimated completion date is May 2015.

OIG Recommendation #4: Define BASS system owner responsibilities in the security plan.

Response: Concur. As outlined in the USCG Security and Information Assurance (SIA) Manual (COMDTINST M5500.13D), system owner responsibilities have already been identified.

OIG Recommendation #5: Define the roles and responsibilities of the BASS Information System Security Officer and the Command, Control, and Communications Engineering Center Support and Development programming staff; and address issues with segregation of duties.

Enclosure (1)

Response: Concur. Information System Security Officer (ISSO) responsibilities are identified in the US Coast Guard Security and Information Assurance (SIA) Manual (COMDTINST M5500.13D). However the Coast Guard will clarify responsibilities for assigning and managing system passwords in the BASS Security Plan during the next Security Authorization Process.

Estimated start date: May 2015

Milestone: TISCOM Information Assurance Division (IAD) checklist. Estimated completion date: June 2015

Milestone: Security Control Selection Phase: Estimated due date: June 2015

Estimated completion date: March 2016

OIG Recommendation #6: Issue minimum requirements for the BASS CCB authorization form used to document change management approval.

Response: Concur. The BASS system is governed by DHS, USCG, Command, Control, Communications and Computers Service Center (C3CEN) and configuration management policies and practices. USCG will ensure cognizant configuration change management policies are redistributed and followed. Estimated completion date is January 2015.

OIG Recommendation #7: Establish standards requiring that BASS properly document authorization for system changes.

Response: Concur. The BASS system is governed by DHS, USCG, Command, Control, Communications and Computers Service Center (C3CEN) and configuration management policies and practices. USCG will ensure cognizant configuration change management policies are redistributed and followed. Estimated completion date is January 2015.

Enclosure (1)

Appendix D

Major Contributors to This Report

Tuyet-Quan Thai, Director
Ann Brooks, Audit Manager
Dave Bunning, Referencer

Appendix E

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, General Accountability Office/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Privacy Officer

United States Coast Guard

USCG Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305