DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Better Administration of Automated Targeting System Controls Can Further Protect Personally Identifiable Information (Redacted)

NOTICE: The Department of Homeland Security, Office of Inspector General (OIG), has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.

OIG-08-06

October 2007

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

October 16, 2007

Preface

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.

This report addresses the adequacy and effectiveness of the department's protection of personally identifiable information (PII) collected, transmitted, and stored in Customs and Border Protection's (CBP) Automated Targeting System (ATS). It includes an evaluation of the operational and system controls implemented to reduce the risks associated with the loss, misuse, unauthorized access to, or modification of PII captured and stored in ATS. Our review was based on direct observations, system security vulnerability assessments, queries of ATS user data, and analyses of applicable documents. We obtained additional supporting information through interviews with employees and officials located in CBP's Program Office, Office of Field Operations, and Office of Information Technology.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ATS	Automated Targeting System
ATS-P	Automated Targeting System -Passenger
CBP	Customs and Border Protection
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
OIG	Office of Inspector General
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SQL	Structured Query Language

Executive Summary

The Automated Targeting System (ATS) is an information system that captures and stores personally identifiable information (PII), and is one of the most advanced targeting systems in the world. Customs and Border Protection (CBP) officers use the system to effectively and efficiently identify cargo, individuals, or conveyances that may present a risk to the United States and its citizens.

We evaluated whether the Department of Homeland Security is protecting the PII collected, transmitted, and stored within ATS. In addressing our audit objective, we focused on specific controls implemented for the ATS' passenger database. The passenger database of ATS contains the majority of PII stored within ATS that is used in CBP's targeting efforts.

Generally, CBP has implemented robust operational and system security controls to protect the PII contained within ATS. These controls are outlined in the *Privacy Impact Assessment for the Automated Targeting System* and provide for the protections needed to secure its data. CBP is effectively employing these controls in protecting individuals' PII. Control measures, based on user's roles and responsibilities, have been established for granting access to system data. Additionally, all users are required to receive initial and refresher computer security and privacy awareness training in order to obtain and retain system access. Furthermore, network protection mechanisms, such as firewalls and encryption, have been deployed to protect the transmission of PII that is stored in ATS' passenger database.

While a number of ATS controls have been implemented, CBP management still needs to ensure that other established controls are better used in the protection of PII. Specifically, management should ensure that periodic reviews of users' access privileges are being conducted and that user privileges granted were properly authorized; user accounts that have not been accessed within 90 days are disabled; and CBP's Office of Internal Affairs independently conduct internal reviews of user access according to department and component policies. In addition,

management needs to remediate the system security vulnerabilities we detected pertaining to passwords and critical security patches.

We recommended that the Commissioner direct CBP's Offices of Field Operations and Internal Affairs to review access control lists to ensure they are current, and disable user accounts that have not been used in 90 days. We also recommended that CBP's Chief Information Officer address the system security vulnerabilities identified.

In response to our draft report, CBP concurred with our recommendations. CBP's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The public's sensitivity to the protection of PII heightened and generated concerns in the post 9/11 era. Many agencies capture PII and store it on their information systems, which causes great anxiety for both agencies and the public.

PII is defined as information in a system or online collection that directly or indirectly identifies a specific individual. PII includes information about an individual's education, financial transactions, medical history, criminal or employment history, and other information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, date and place of birth, mother's maiden name, and biometric records, including fingerprints.

One of the systems storing PII is ATS, which became operational within CBP in 1993. ATS is the cornerstone for all CBP targeting efforts. CBP uses ATS to improve the collection, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and weapons from entering the United States.

Automated Targeting System-Passenger (ATS-P), a database within ATS, is deployed at all ports-of-entry (air, ship, and rail) and has been used in evaluating ("target") passengers prior to arrival into the United States since 1999. ATS-P contains PII collected directly from commercial carriers in the form of a passenger name record, which is then used to target suspicious individuals. ATS-P also receives various real-time information from other CBP systems and law enforcement databases. [redacted].

The ATS architecture and data sources are depicted on the next page.

[redacted]

Note: This diagram depicts the ATS architecture and the flow of data, including passenger airline manifests, immigration and customs information, and passenger name record data, from multiple sources (on the right) transmitted to the ATS application and into the ATS-P database. Users (on the left) access the data through a World Wide Web (i.e., Internet) connection to CBP's local area network.

A significant amount of data regarding passengers and crew members entering or departing the United States is collected and maintained in ATS, including name, address, dates of travel, contact information, frequent flier and benefit information, all available payment and billing information, travel itinerary, ticketing information, baggage information, passenger and crew manifests, and immigration control information. DHS has a duty to protect that information from loss and misuse. The loss or compromise of ATS data can have severe consequences, affecting national security, United States citizens, and the department's missions.

There is substantial public and foreign interest in DHS' collection and use of ATS data and the potential privacy implications in the event of disclosure. The privacy implications include:

- Potential threats to personal information during transmission.
- Violations of passenger rights.
- Unauthorized access to PII stored within ATS, especially ATS-P.
- Personal identity theft.

Results of Audit

Overall, CBP has implemented adequate privacy and system security controls over the PII collected, transmitted, and stored in ATS-P to effectively protect the information from loss, misuse, unauthorized access, or modification. We determined that CBP has implemented robust controls for the protection of PII maintained in ATS and shared with external agencies. We also identified that CBP can better administer its management and oversight to strengthen the effectiveness of its privacy controls. Our audit included a review of the ATS Privacy Impact Assessment (PIA) and operational and system security controls implemented.

Effective Privacy Controls Implemented

The ATS PIA, dated November 22, 2006, accurately documents the privacy protections implemented to protect the PII that is collected, transmitted, and stored within ATS-P. The PIA adequately describes the administrative, technical, and physical controls established for storing and safeguarding PII data to prevent unauthorized access. It also documents the privacy risks associated with the potential misuse of PII data or breach of the system. To mitigate the risks pertaining to the number of users with access to PII, the PIA lists specific controls related to:

- User profile management.
- Definition of a user's rights and responsibilities.
- Audit log generation to document all users' access to ATS.
- Sharing of data, based on a need-to-know, case-by-case basis, consistent with federal, DHS and CBP policies, and applicable arrangements and agreements.
- Information security and privacy awareness training.

CBP has established guidelines and procedures to ensure that ATS use is consistent with the PIA and privacy policy. CBP also has implemented a number of operational and system security controls to govern user access and information sharing. Furthermore, CBP requires that all of its officers be trained on the limited uses for which ATS information may be used in connection with their official duties.

Operational Controls

CBP has implemented effective operational safeguards to protect the PII data within ATS, specifically ATS-P. These measures are designed to reduce the risks associated with the intentional and unintentional actions of system users, which could potentially result in the loss, misuse, modification, or unauthorized disclosure of ATS data. For example, CBP has:

- Established interconnection security agreements with internal and external agencies, as well as foreign countries. The agreements stipulate the privacy safeguards needed to protect the transmission of PII shared between the connecting information systems.

- Created a formal Computer Security Incident Response Center (CSIRC). All incidents of misuse of CBP systems are to be reported to CBP's CSIRC. The CSIRC provides real-time network monitoring, intrusion detection, and incident handling.

- Developed security and privacy awareness training requirements. All ATS users are required to receive initial computer security and privacy awareness training before system access may be granted; users who have system access need to attend refresher training to keep it. From a random sample of [redacted] of the [redacted] ATS-P users, we determined that [redacted] of the users had received the required security and privacy awareness training. The account for the one user who did not receive the training was locked to prevent that user from any further access to ATS-P.

System Security Controls

Along with operational controls, CBP has implemented technical and logical access controls to effectively protect sensitive PII data in the ATS-P database. The following processes are in place:

- User access - Access to ATS is granted only after the completion of a background investigation, the submission of a supervisor-approved access request form, and the completion of initial security and privacy training. Data can only be accessed using encrypted passwords and user sign-on functionality. All users are assigned "Read Only" access to ATS-P, and all authorized access is based on a user's "need-to-know." CBP's process for granting ATS access limits the number of users who are allowed to view PII data and protects ATS from unauthorized changes.

- Separation of duties - CBP has clearly defined separation of duties to prevent any one person from subverting a critical process or otherwise compromise ATS system controls or data. We noted that the database administrator and programmer roles ensure a complete separation of duties between maintaining the ATS-P database and maintaining the ATS application.

- Transmission of data - CBP has implemented point-to-point encryption of information between ATS users and the ATS web servers to protect PII data in transit. The encryption device settings indicated all ATS traffic in and out of the CBP network at the National Data Center is encrypted.

Administrative Oversight Concerns

CBP policies and procedures clearly indicate that ATS-P user roles are highly restricted and audited; however, the greatest risk to the security and privacy of PII housed in ATS stems from insider threats. To ensure data is adequately protected from insider threats, management has to be vigilant in protecting ATS and the ATS-P database from potential misuse. To protect against threats involving potential misuse, it is imperative that CBP management actively monitor the administrative controls implemented to reduce security risks.

Better oversight is needed to ensure that periodic reviews of user access and the timely deployment of system security patches and updates occur. Additionally, management needs to ensure that system security controls related to the enforcement of DHS' password policy are properly configured and implemented.

Periodic Reviews of User Access to ATS-P

CBP is not reviewing user access privileges on a periodic basis, nor are they disabling user accounts after 90 days of inactivity. According to the *DHS 4300A Sensitive Systems Handbook*, supervisors have a responsibility to ensure that access control lists are current and up-to-date by reviewing access privileges. Information Systems Security Officers are responsible for ensuring that access control reviews are being conducted. Furthermore, the ATS PIA and CBP policy require that CBP management and the Office of Internal Affairs conduct periodic reviews of ATS and the user access control list. DHS policy and the ATS System Security Plan require that CBP disable user accounts after 90 days of inactivity.

From a sample of [redacted] users with access to ATS-P, [redacted] of the [redacted] users were granted privileges that they were not authorized to receive. We also analyzed the ATS-P user access list to determine whether user accounts were disabled after 90 days of inactivity. We identified that [redacted] users have active accounts although they had not logged onto the system in more than 5 months (October 1, 2006 to March 28, 2007). Furthermore, as of May 7, 2007, CBP's Office of Internal Affairs had not conducted any reviews of ATS this fiscal year.

Since user access privileges may change over time, it is imperative that reviews are conducted more frequently than on an annual basis. These reviews should ensure that user access privileges are current and the privileges granted are authorized. Users should be granted only the most restrictive set of privileges needed to perform tasks authorized. Furthermore, by not disabling accounts after 90 days of inactivity, management is allowing users, who may no longer require access to ATS, the opportunity to misuse PII.

Configuration Management

Generally, CBP has implemented configuration and logical access controls to effectively protect the PII data contained within ATS-P. However, additional measures could be implemented to further secure PII and comply with DHS policies.

Configuration management is a set of technical controls designed to provide system administrators with tools to maintain information systems in a secure manner to ensure that agency requirements are applied to specific system security settings. These controls afford a layer of protection from internal and external threats to privacy data through the use of security mechanisms, such as password complexity rules, session timeouts, lockout thresholds, and manufacturer-supplied security patches and updates.

We conducted system security vulnerability assessments of the ATS-P database to identify system vulnerabilities, determine [redacted]. Based on these assessments, the majority of high-risk vulnerabilities detected related to the enforcement of strong passwords and application of critical security patches:

- ATS' Information Systems Security Officer did not implement DHS' policy for [redacted] until [redacted], after our system security vulnerability assessments were completed. Our assessments detected that [redacted] of the [redacted] ATS-P accounts were [redacted]. For [redacted] of those accounts, the assigned [redacted].

- Further, [redacted]. Although CBP has [redacted] policies and procedures, [redacted].

Appendix C contains a summary of the high vulnerabilities identified and the potential threats.

DHS 4300A Sensitive Systems Handbook requires [redacted], [redacted]. [redacted].

DHS policy also requires that components [redacted].

[redacted]. [redacted]. [redacted]. [redacted].

[redacted]. [redacted]. [redacted].

Recommendations

We recommend that the Commissioner, CBP, direct the Office of Field Operations and the Office of Internal Affairs to:

Recommendation #1: Periodically review ATS access control lists to verify that users were granted only the level of access privileges authorized.

Recommendation #2: Disable ATS user accounts that have been inactive for 90 days or perform a risk assessment to determine whether management is willing to accept the risk of not disabling user accounts according to CBP policies.

We recommend that the Commissioner, CBP, direct its Chief Information Officer to:

Recommendation #3: Address ATS security vulnerabilities regarding [redacted].

Management Comments and OIG Analysis

CBP concurred with recommendation 1. CBP managers will review the ATS access control list on at least a biannual basis to verify users have received only the level of access authorized.

We agreed that the steps CBP plans to take satisfy this recommendation.

CBP concurred with recommendation 2. CBP managers are conducting a review to identify ATS-P user accounts that have been inactive for 90 days in order to disable the accounts. Subsequently, in conjunction with CBP [redacted], CBP will implement a procedure to inactivate ATS accounts that have had 30 days of consecutive inactivity. CBP also will make a determination whether to seek a waiver of the 30-day policy for ATS-P accounts with "Quick Query –only" access.

We agreed that the steps CBP plans to take satisfy this recommendation.

CBP concurred with recommendation 3. [redacted]. [redacted]

[redacted].

[redacted]. [redacted].

We agreed that the steps CBP plans to take satisfy this recommendation.

The overall objective of this audit was to determine whether the department is properly protecting PII collected, transmitted, and stored in ATS. Specifically, we determined whether:

- ATS' PIA adequately depicted the operational controls implemented for protecting PII data.
- Operational, technical, and system logical access controls were effective in protecting ATS' PII data.

Our audit focused on the controls implemented to protect the privacy of the data contained in ATS-P, which contains the majority of PII. We analyzed the security posture of the ATS-P database only. Other operational and system security controls relating to ATS' other modules will be tested at a later date.

To accomplish our audit objective, we evaluated the ATS PIA and the information technology controls implemented to protect sensitive ATS data. We also reviewed:

- *DHS 4300A Sensitive Systems Handbook* (dated March 1, 2007).
- DHS Management Directive 0470.2 – Privacy Act Compliance.
- DHS' [redacted].
- CBP's [redacted].
- The Privacy Act of 1974.
- Office of Management and Budget Memorandum (OMB) Memorandum M-06-15, *Safeguarding Personally Identifiable Information* (dated May 22, 2006).
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (dated May 22, 2007). Additionally, we conducted interviews, documented on-site observations, conducted system security vulnerability testing, and performed analytical queries of ATS-P user data.

We ensured that security and privacy awareness training policies and procedures had been established. To determine whether ATS users were complying with CBP's security and privacy awareness training policy, we randomly selected and analyzed the training documentation for a sample of [redacted] ATS-P users.

In determining whether the operational controls CBP implemented were effective in protecting ATS' PII data, we interviewed CBP personnel regarding the processes and procedures for granting access to the ATS-P database and system security. We interviewed the Privacy Office personnel regarding the handling procedures for incidents involving PII issues. Additionally, we interviewed the Office of Internal Affairs personnel regarding periodic reviews of ATS-P user access privileges and activity.

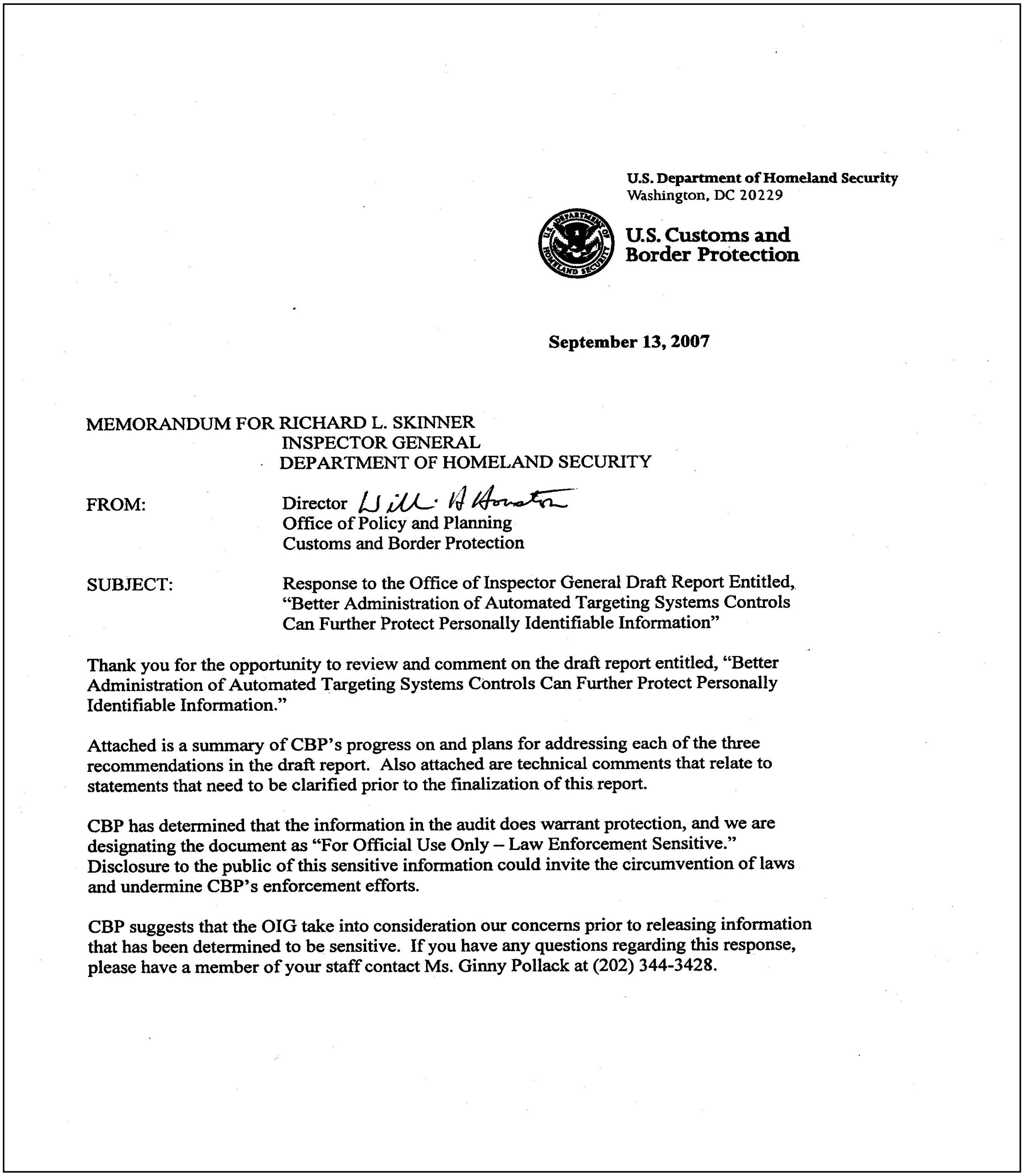
We analyzed the ATS-P user access list to evaluate users' roles and privileges. We judgmentally sampled the ATS-P users to verify whether required background investigations were conducted and supervisory authorizations were submitted before granting and creating ATS user accounts.

We conducted system security vulnerability assessments to determine whether technical and logical and access controls were effective in protecting ATS' PII data. We analyzed the security controls over servers, databases, and network devices that supported ATS at the [redacted]. Furthermore, we determined that network protection mechanisms, such as firewalls and intrusion detection, had been deployed. Encryption and authentication methods used to protect ATS data were evaluated.

[redacted]. [redacted]. [redacted].

[redacted]. We coordinated our audit efforts with CBP headquarters, CBP's Office of Field Operations, and CBP's Office of Information Technology. Fieldwork was completed from March 2007 through July 2007 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix D.

The principal OIG points of contact for the audit are Frank W. Deffer, Assistant Inspector General, Information Technology Audits, at (202) 254-4100, and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.



U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and
Border Protection

September 13, 2007

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Director
Office of Policy and Planning
Customs and Border Protection

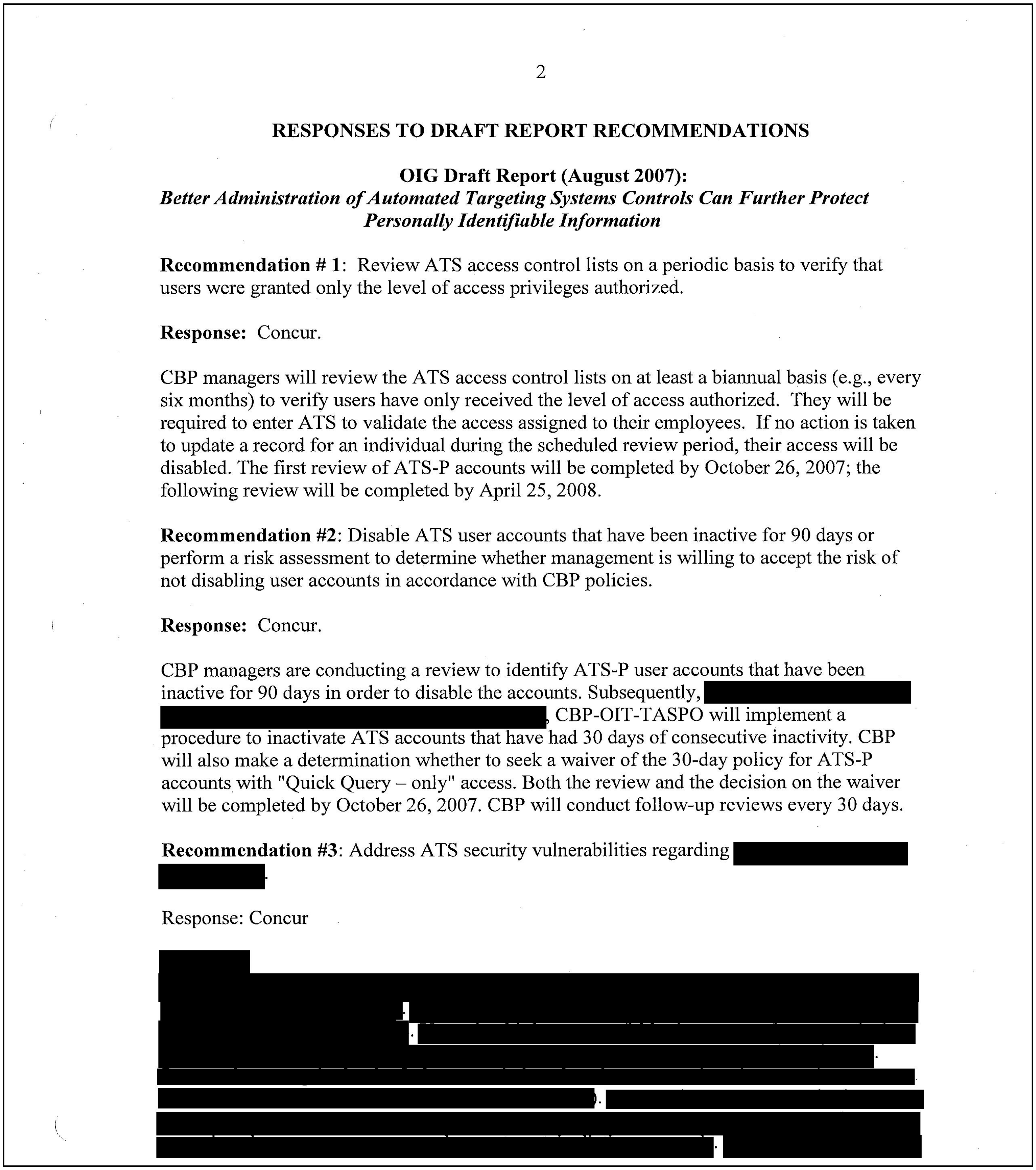
SUBJECT: Response to the Office of Inspector General Draft Report Entitled, "Better Administration of Automated Targeting Systems Controls Can Further Protect Personally Identifiable Information"

Thank you for the opportunity to review and comment on the draft report entitled, "Better Administration of Automated Targeting Systems Controls Can Further Protect Personally Identifiable Information."

Attached is a summary of CBP's progress on and plans for addressing each of the three recommendations in the draft report. Also attached are technical comments that relate to statements that need to be clarified prior to the finalization of this report.

CBP has determined that the information in the audit does warrant protection, and we are designating the document as "For Official Use Only – Law Enforcement Sensitive." Disclosure to the public of this sensitive information could invite the circumvention of laws and undermine CBP's enforcement efforts.

CBP suggests that the OIG take into consideration our concerns prior to releasing information that has been determined to be sensitive. If you have any questions regarding this response, please have a member of your staff contact Ms. Ginny Pollack at (202) 344-3428.



2

RESPONSES TO DRAFT REPORT RECOMMENDATIONS

OIG Draft Report (August 2007):
Better Administration of Automated Targeting Systems Controls Can Further Protect Personally Identifiable Information

Recommendation # 1: Review ATS access control lists on a periodic basis to verify that users were granted only the level of access privileges authorized.

Response: Concur.

CBP managers will review the ATS access control lists on at least a biannual basis (e.g., every six months) to verify users have only received the level of access authorized. They will be required to enter ATS to validate the access assigned to their employees. If no action is taken to update a record for an individual during the scheduled review period, their access will be disabled. The first review of ATS-P accounts will be completed by October 26, 2007; the following review will be completed by April 25, 2008.

Recommendation #2: Disable ATS user accounts that have been inactive for 90 days or perform a risk assessment to determine whether management is willing to accept the risk of not disabling user accounts in accordance with CBP policies.

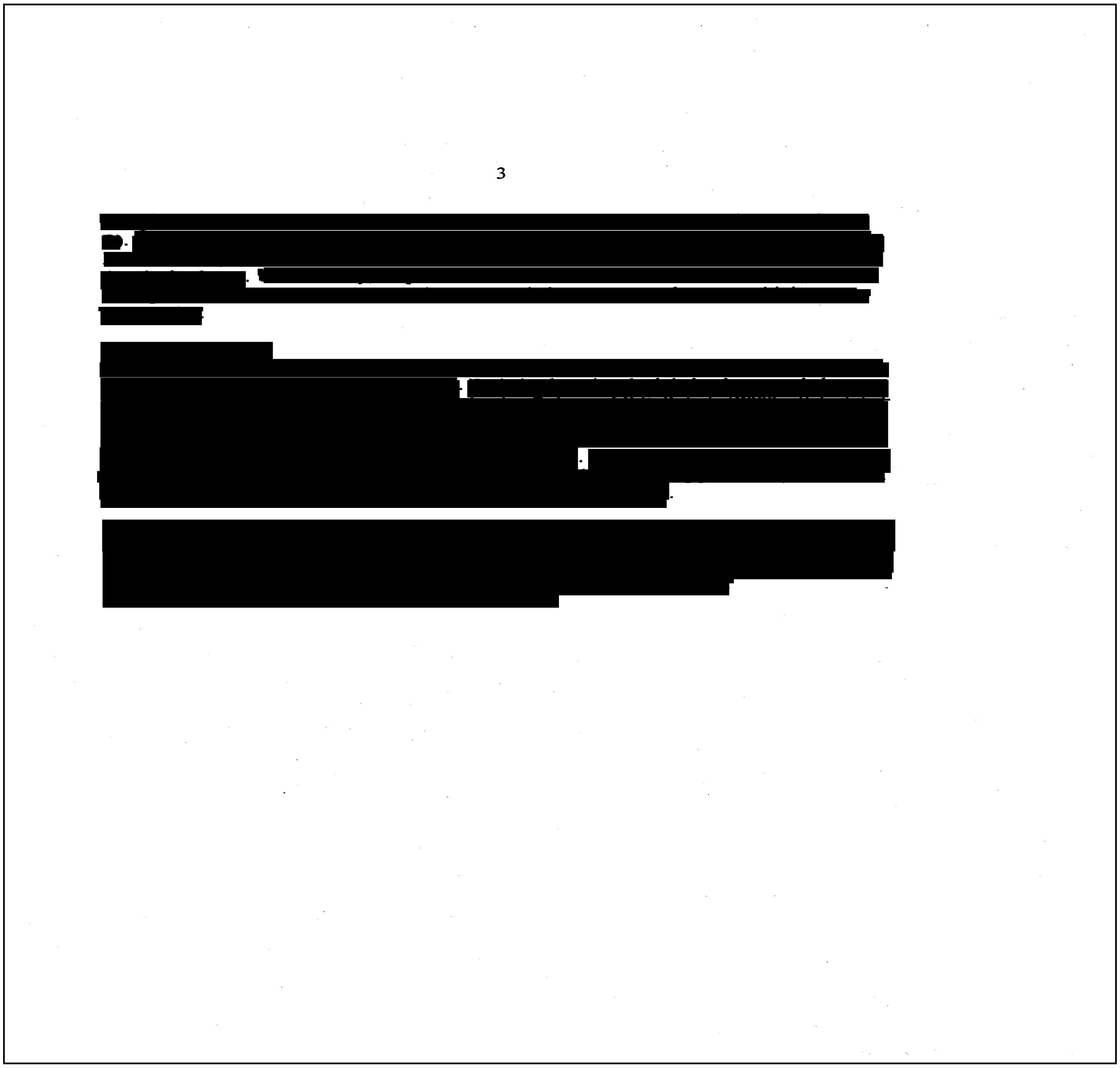
Response: Concur.

CBP managers are conducting a review to identify ATS-P user accounts that have been inactive for 90 days in order to disable the accounts. Subsequently, [redacted], CBP-OIT-TASPO will implement a procedure to inactivate ATS accounts that have had 30 days of consecutive inactivity. CBP will also make a determination whether to seek a waiver of the 30-day policy for ATS-P accounts with "Quick Query – only" access. Both the review and the decision on the waiver will be completed by October 26, 2007. CBP will conduct follow-up reviews every 30 days.

Recommendation #3: Address ATS security vulnerabilities regarding [redacted].

Response: Concur

[redacted]



3

[redacted]

[redacted]

[redacted]

High Risk Vulnerabilities

Vulnerability	[redacted]	[redacted]	Potential Threats
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]	√		[redacted]
[redacted]	√		[redacted]
[redacted]	√		[redacted]
[redacted]	√		[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]
[redacted]		√	[redacted]

Information Security Audit Division
Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Tarsha Ross, Senior IT Auditor
Mike Horton, IT Specialist
Swati Mahajan, IT Specialist
Thomas Rohrback, Management and Program Assistant
Shannon Frenyea, Referencer

Advanced Technology Division
Marcus Badley, Senior Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
Executive Secretary
Assistant Secretary, Legislative Affairs
Assistant Secretary, Policy
Assistant Secretary, Public Affairs
General Counsel
Office of Security
Office of Privacy
Chief Information Officer (CIO)
Deputy CIO
Chief Information Security Officer
CIO, Customs and Border Protection (CBP)
Deputy CIO & Information Systems Security Manager, CBP
Director, Departmental Government Accountability Office/OIG Liaison Office
Director, Compliance and Oversight Program
Audit Liaison, CBP
Audit Liaison, CIO
Director, Information Security Audit Division

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 obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG website at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call** our Hotline at 1-800-323-8603;
- **Fax** the complaint directly to us at (202) 254-4292;
- **Email** us at DHSOIGHOTLINE@dhs.gov; or
- **Write** to us at:
  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller**.**