



Department of Homeland Security Office of Inspector General

Letter Report:

Review of Customs and Border Protection's Certification of Automated Targeting System— Passenger Enhancements





Homeland Security

March 23, 2009

MEMORANDUM FOR: The Honorable Elaine C. Duke
Under Secretary for Management

FROM: 
Richard L. Skinner
Inspector General

SUBJECT: *Letter Report: Review of Customs and Border Protection's
Certification of Automated Targeting System—Passenger
Enhancements (OIG-09-44)*

We reviewed the certification by Customs and Border Protection (CBP) pertaining to enhancements of the Automated Targeting System-Passenger (ATS-P) according to congressional requirements for the FY 2009 funding for such enhancements.¹ CBP's certification is to describe how ATS-P enhancements will improve targeting while fully complying with statutory requirements for handling and securing personal data. Congress requires CBP to certify that such enhancements comply with all applicable laws, including privacy-protection laws, and that the Office of Inspector General (OIG) review the certification.

We are unable to determine whether CBP properly certified the proposed ATS-P enhancements based on the limited information CBP provided for our review. CBP did not provide sufficient information about the enhancements or the applicable statutory requirements to enable us to determine whether the proposed enhancements comply with the requirements for handling and securing personal data. Information that would have aided in our review includes documents such as a current risk assessment, security testing and evaluation plan, or a draft, revised privacy impact assessment (PIA). These documents would have provided an additional level of assurance that CBP is fully considering the impact of the proposed enhancements.

However, after reviewing CBP's Operational Program Enhancements Plan, the controls outlined in the August 2007 PIA, and the additional supporting documentation provided,

¹ *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009*, P.L. 110-329, September 30, 2008; Explanatory Statement, 154 Cong. Rec. H9434, H9741, 9794 (daily ed., September 24, 2008); House Committee Report 110-862, p. 28, 30, 37.

we do not foresee any significant risks to the personal data being collected and stored within ATS-P brought about by the proposed system enhancements. Additionally, in October 2007, we reported that system controls and internal processes were in place to protect personally identifiable information maintained in the ATS-P database.²

We are not making any recommendations in this report. Should you have any questions, please call me, or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology Audit, at (202) 254-4100.

Background

The Automated Targeting System (ATS) is the cornerstone for all CBP targeting efforts. ATS-P, one of the databases that make up ATS, is deployed at all ports-of-entry (air, ship, and rail) and has been used in evaluating (“targeting”) passengers before they arrive in the U.S. since 1999. ATS-P contains most of the personally identifiable information (PII) stored in ATS and used in CBP’s targeting efforts.³ PII is collected directly from commercial carriers in the form of a passenger name record, which is then used to target suspicious individuals.⁴ ATS-P also maintains various real-time information from other CBP systems and law enforcement databases.

The Department of Homeland Security (DHS) has a duty to protect PII from loss and misuse. The loss or compromise of ATS data can have severe consequences, affecting national security, U.S. 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.

Reporting Requirements

Pursuant to congressional requirements accompanying the FY 2009 *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act*, the OIG must review CBP’s certification of the proposed ATS-P enhancements and report on it to the

² OIG-08-06, *Better Administration of Automated Targeting System Controls Can Further Protect Personally Identifiable Information* (October 2007).

³ 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.

⁴ Passenger name records contain a significant amount of data about passengers and crew members entering or departing the U.S., including an individual’s 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.

Appropriations Committees.⁵ Before FY 2009 appropriated funds are obligated for any ATS-P enhancements, Congress requires CBP to certify that such enhancements comply with all applicable laws, including privacy protection laws, and that the OIG reviewed its certification.⁶

Our conclusion was based on a review of information provided by CBP with its certification letter. Although CBP certified that proposed enhancements would comply with all applicable privacy laws, it did not certify whether the enhancements would comply with all laws, not just privacy laws, as required. Further, we were not provided with sufficient information to determine whether we agree with CBP's certification of the proposed enhancements.

Prior Audit Results

From March 2007 through July 2007, we evaluated whether DHS was protecting the PII collected, transmitted, and stored within ATS. In October 2007, we reported that CBP had implemented robust operational and system security controls to protect the PII contained within ATS.⁷ Those controls, to mitigate the privacy risks identified, were outlined in the *Privacy Impact Assessment for the Automated Targeting System*, dated November 22, 2006. CBP was effectively employing these controls in protecting individuals' PII. Other control measures, including those for granting access to system data, providing users with computer security and privacy awareness training, and deploying network protection mechanisms, contributed in protecting the PII captured and retained in the ATS-P database. During this audit, we did not evaluate other management or administrative-type controls that might be employed to fully protect PII data.

Certification Documentation

In December 2008, CBP requested that we review its proposed certification letter to the U.S. House of Representatives Committee on Appropriations, Subcommittee on Homeland Security. The letter incorrectly asserted that we had "reviewed" CBP's certification and "verified" that the ATS-P enhancements fully complied with applicable laws, providing as support our October 2007 ATS audit report. CBP, however, had not provided us with information on the ATS-P enhancements to review. Shortly thereafter, we met with CBP and ATS officials to voice our concerns with the certification.

At the meeting, we requested supporting documentation for our review, including the methodology used to support the enhancements, a breakdown of the specific hardware/software to be used in the enhancements, and the specific laws that applied to the ATS-P enhancements. In January 2009, CBP provided us with a document, entitled "ATS-P Operational Enhancements," but did not provide any additional information

⁵ Explanatory Statement, 154 Cong. Rec. H9434, H9741 (daily ed. September 24, 2008); House Committee Report 110-862, p. 28, 37.

⁶ Explanatory Statement, 154 Cong. Rec. at H9794; House Committee Report 110-862, p. 30, 37.

⁷ OIG-08-06, *Better Administration of Automated Targeting System Controls Can Further Protect Personally Identifiable Information* (October 2007)

concerning the statutory requirements applicable to the enhancements. Uncertainty remains as to what security controls CBP would implement to protect PII and which laws are relevant to the proposed ATS-P enhancements. We asked CBP officials a second time for additional information, and were provided with an updated certification letter, but it did not address the issues we discussed at our December meeting or our subsequent request for additional supporting documentation.

ATS-P Enhancements

CBP's updated certification letter outlines the following proposed ATS-P enhancements to improve its targeting methodology:

- Develop a simulation and testing environment to achieve benefits realized by a similar effort deployed for CBP's cargo targeting system.
- Incorporate a refresh of existing high-availability focused technology.
- Convert the current ATS-P client and server application designs to a new architecture (conversion to a Microsoft .NET architecture).
- Establish a data warehouse and reporting facility to facilitate ad hoc reporting, queries, and other tasks requiring the use of depersonalized data elements.

In an effort to evaluate whether the proposed enhancements to ATS-P will affect CBP's compliance with statutory requirements for handling and securing personal data, we first reviewed the privacy risks associated with maintaining the information in ATS as documented in the updated PIA (dated August 3, 2007). While we identified that those risks were addressed in the updated PIA, we could not determine whether the enhancement of ATS-P will comply with all applicable laws, including the *Privacy Act of 1974*.⁸ At a minimum, CBP needs to identify the specific laws that apply to the ATS-P enhancements.

In February 2009, we requested more detailed information supporting the proposed enhancements. Our request included CBP's security testing and evaluation plan, network layout for both the data warehouse and the simulation and testing environment, and whether live PII would be used in the simulation and testing environment. We also requested what web-based controls would be implemented as part of the new architecture and whether CBP had assessed the vulnerabilities and risks that may be inherent in the proposed .NET architecture. Additionally, we asked whether a revised PIA had been drafted.

Based upon our review of the information received, we continue to have concerns in relation to the ATS-P enhancements and the risks and controls that should be considered in association with those enhancements. For example, risks associated with the conversion to a Microsoft .NET platform lie in its configuration. Vulnerabilities inherent in any .NET architecture include custom errors, tracing data, debugging, cookie management, and session timers. Default and/or poorly configured web-based

⁸ 5 U.S.C. § 552a

applications can allow attackers access to critical information about the web application, server, and services, compromising assets and information.

While we recognize that it may be necessary to upgrade the existing software platform because the current platform may no longer be supported, CBP did not provide us with a risk assessment or its security testing and evaluation plan to address:

- Vulnerabilities and risks associated with the security of PII in the proposed ATS-P .NET architecture.
- Storage and maintenance of ATS-P privacy information in the proposed data warehouse and reporting facility.
- Use of PII in the proposed simulation and testing environment.

Additionally, CBP did not provide us with documentation of any additional web-based security controls being considered as a result of the proposed enhancements or a revised, updated draft of the PIA. Overall, we were not provided with documentation that we expected, to provide an additional level of assurance that CBP is fully considering the impact of the proposed enhancements.

Current Position

Based on our review of the ATS-P Operational Enhancements Program Plan, the August 2007 ATS PIA, our prior audit work, and supporting documentation provided, we do not foresee that the proposed enhancements would pose significant changes to the internal control processes CBP currently has in place to protect ATS-P privacy data. Though we cannot determine whether the impact of the proposed enhancements is being fully considered or verify that the proposed enhancements were properly certified, it is our opinion that CBP will ensure that the PII contained within ATS-P is secure and that access is limited in accordance with applicable laws. Therefore, based on our understanding of the existing ATS-P system environment and the limited supplementary information CBP provided, we do not expect the introduction of additional significant risks to the personal data being collected and stored in ATS-P once the proposed enhancements are implemented.

We conducted our review from December 2008 through February 2009. We did not follow generally accepted government audit standards in performing this review. We performed this nonaudit service in response to a congressional request. We are providing our professional opinion on whether the proposed ATS-P enhancements fully comply with all applicable laws as documented in CBP's certification

Appendix A
Major Contributors to This Report

Information Security Audits Division

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Michael Horton, Information Technology Officer

Office of Counsel

Jennifer Ashworth, Assistant Counsel to the Inspector General

Appendix B Report Distribution

Department of Homeland Security

Secretary
Acting Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretary
Under Secretary, Management
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer
Chief Information Security Officer
DHS Audit Liaison
CBP Commissioner
CBP 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 obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site 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.