OFFICE OF INSPECTOR GENERAL

DHS Has Controls to Safeguard Watchlist Data

Homeland
Security

July 25, 2022
OIG-22-53

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

July 25, 2022

MEMORANDUM FOR: The Honorable Randolph D. Alles
Acting Under Secretary for Management
U.S. Department of Homeland Security

The Honorable Chris Magnus
Commissioner
U.S. Customs and Border Protection

The Honorable David P. Pekoske
Administrator
Transportation Security Administration

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2022.07.25 11:39:49 -04'00'

SUBJECT: *DHS Has Controls to Safeguard Watchlist Data*

Attached for your action is our final report, *DHS Has Controls to Safeguard Watchlist Data*. We incorporated the technical comments provided by your office. This report contains no recommendations, and the Department of Homeland Security chose not to submit formal comments to our draft report.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over DHS. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

DHS Has Controls to Safeguard Watchlist Data

July 25, 2022

Why We Did This Audit

DHS uses and shares terrorist screening data to support mission-related functions, such as counterterrorism, law enforcement, border security, and inspections. In July 2021, DHS learned of an alleged exposure of more than 1.9 million Federal terrorist watchlist records. Because of the nature of this allegation, we initiated an audit to determine whether DHS has an effective approach to safeguard and share terrorist screening data.

What We Recommend

This report does not contain recommendations.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

Based on our audit work, we determined the Department of Homeland Security has an approach to safeguard and share terrorist screening data. We confirmed that DHS' policies and procedures comply with Federal standards for safeguarding sensitive data, including terrorist watchlist records that are used, stored, and shared by the Department.

We also determined that on July 19, 2021, after learning of an alleged online exposure of more than 1.9 million Federal terrorist watchlist records, DHS responded appropriately by immediately notifying the Federal Bureau of Investigation's Terrorist Screening Center, the owner of terrorist watchlist records. We confirmed with DHS officials that DHS was not involved in the alleged incident.

DHS Response

The Department chose not to submit management comments to the draft report.

Background

The Federal Bureau of Investigation's Terrorist Screening Center (TSC) was established to share terrorism-related information across the U.S. Government and with other law enforcement agencies. The TSC consolidates information into the Federal Terrorist Screening Database (watchlist), a single database containing integrated terrorist identity information from Federal agencies. The watchlist helps Federal agencies positively identify known or suspected terrorists who attempt to enter the country, obtain visas, or board an aircraft.

The Department of Homeland Security uses TSC watchlist data to conduct frontline operations in counterterrorism, law enforcement, border security, and inspections. For example, U.S. Customs and Border Protection (CBP) officers use watchlist data and other information contained in various Federal and partner-agency information technology systems to inspect travelers seeking entry into the United States to ensure they are eligible for admission. Similarly, Transportation Security Administration (TSA) agents use watchlist data to identify and prevent known or suspected terrorists, or other individuals who may pose threats to transportation security or public safety, from boarding an aircraft or accessing sterile areas[1] of airports.

On July 19, 2021, DHS learned of a social media post alleging more than 1.9 million TSC terrorist watchlist records were exposed publicly online. Subsequently, media outlets reported the records contained sensitive information on people, including their names and personal information such as citizenship, gender, date of birth, passport details, and no-fly list status. The exposed data also included the data identifier "TSC_ID," which may have referred to a TSC watchlist identification number. The nature of the allegation prompted us to conduct this audit. Our objective was to determine whether DHS has an effective approach to safeguard and share terrorist screening data.

Results of Audit

Based on our audit work, we determined DHS has an approach to safeguard and share terrorist screening data. We confirmed that DHS' policies and procedures comply with Federal standards for safeguarding sensitive data, including terrorist watchlist records that are used, stored, and shared by the Department.

We also determined that on July 19, 2021, after learning of an alleged online exposure of more than 1.9 million Federal terrorist watchlist records, DHS responded appropriately by immediately notifying the Federal Bureau of

[1] Sterile area is defined as a portion of the airport in which passengers have access to boarding aircraft, and to which access is generally controlled by TSA or by an aircraft operator.

Investigation's TSC, the owner of terrorist watchlist records. We confirmed with DHS officials that DHS was not involved in the alleged incident.

DHS' Policies and Procedures Adhere to Federal Standards for Protecting Sensitive Systems and Data

We determined that DHS has appropriate policies, procedures, and guidance for safeguarding and sharing terrorist watchlist data. We noted five key policies and procedures, listed in Table 1, that document department-wide requirements for management and oversight of sensitive information and information systems. We verified that DHS' sensitive systems policy and procedural guidance generally comply with Federal standards for operational, privacy, and technical controls for protecting data, including National Institute of Standards and Technology publications.

Table 1. Key DHS Policies for Safeguarding and Sharing Sensitive Data

Relevant Policy	Description
DHS Sensitive Systems Policy Directive 4300A[2]	Establishes DHS' Information Security Program for sensitive systems.[3]
DHS Directive 262-03, *DHS Information Sharing Environment Technology Program*	Establishes information technology practices and standards to facilitate information sharing across all components. Implements the national and DHS strategies for sharing and safeguarding information, in conjunction with the Office of Intelligence and Analysis (I&A).
DHS Directive 262-05, *Information Sharing and Safeguarding*	Establishes the policy and governance framework for sharing and safeguarding information within the Department and with Federal, state, local, tribal, territorial, private sector, and international partners.
DHS Instruction 264-01-013, *Sharing Intelligence Information with the Private Sector*	Establishes responsibilities and procedures for sharing reports containing classified national security information and unclassified information with U.S. and foreign private sector entities.
DHS Directive 047-01, *Privacy Policy and Compliance*	Establishes DHS' privacy policy for collecting, using, maintaining, disclosing, deleting, and destroying personally identifiable information.

Source: DHS Office of Inspector General analysis of DHS-provided data

During our audit, we sought to determine whether the Department's policies and guidelines are sufficient to set standards and practices to sufficiently safeguard watchlist data. We received consistent feedback from DHS officials

[2] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017.
[3] A companion publication, DHS 4300A, *Sensitive Systems Handbook*, Version 12.0, Nov. 15, 2015, outlines implementation procedures.

that the Department's policies and guidance established practices to safeguard sensitive data, including watchlist records, and to govern information sharing between DHS components and with partner agencies and external stakeholders, such as contractor personnel. Moreover, I&A established the Department's Information Sharing Environment in 2014 to facilitate sharing of information related to terrorism and homeland security. This enables the Department to share terrorism information internally, and externally through an established set of standards, architecture, security measures, access controls, policies, agreements, and management practices.

We also determined that DHS components have policies and procedures for safeguarding and sharing sensitive information. Specifically, DHS requires[4] each component to maintain its own information security program with policies to administer management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity in DHS information systems infrastructure and operations. We reviewed the policies from CBP and TSA[5] and determined they conform with DHS requirements. Both components' policies contain specific guidance for employees, contractors, and other users who access CBP and TSA systems. Examples of information security guidance include user access controls, information sharing controls, user training requirements, audit and accountability controls, system security controls, and privacy controls.

The Federal Bureau of Investigation's TSC compiles and owns the data in the watchlist. TSC creates tailored exports of watchlist records and sends updates to DHS through a secured connection. Specifically, TSC sends the data to the DHS Watchlist Service, which was created in 2010 to receive synchronized copies of the watchlist in a secure, centralized manner. The Watchlist Service then electronically transmits watchlist data to technology systems across DHS components and offices.[6] Once received, watchlist data is stored in certain DHS systems[7] on the Department's secure network. DHS' frontline personnel use the data to inspect persons seeking entry to the United States through air, land, or sea ports of entry, or transiting the country using domestic airline travel.

[4] *DHS Sensitive Systems Policy Directive 4300A*.

[5] CBP HB 1400-05D, *Information Systems Security Policies and Procedures Handbook*, Version 7.0, Nov. 16, 2017; and TSA Management Directive No. 1400.3, *Information Technology Security*, Jan. 31, 2022.

[6] CBP, TSA, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, I&A, and the Office of Biometric Identity Management.

[7] Watchlist Service, TECS, Automated Targeting System-Passenger, Secure Flight, and Traveler Verification Service.

According to DHS officials, users of CBP's TECS[8] (not an acronym) and TSA's Secure Flight[9] have limited access to watchlist data. We confirmed that more than 99 percent of TECS users and more than 95 percent of Secure Flight users have read-only access to watchlist data when inspecting travelers. These personnel cannot view the watchlist in its entirety; instead, they can only view data associated with each specific traveler they inspect.

We also determined that DHS meets the intent of Federal standards mandating protection of sensitive data. For example, to access systems containing watchlist data, all CBP employees, contractors, partner agencies, and stakeholders must successfully complete background screenings, complete required privacy and system security training, and sign Rules of Behavior.[10] Further, according to CBP's Office of Information and Technology, very few individuals can edit watchlist data. For example, as of March 2022, CBP's TECS system had 85,651 active users, but just 16 of those users could edit watchlist data stored in TECS. All other TECS users had read-only access to view watchlist data. Based on this example and similar information we obtained about other systems, we determined DHS' controls meet the intent of Federal standards mandating protection of sensitive data. We did not perform independent testing to determine whether watchlist data is fully secured within DHS systems.

DHS Responded Promptly to the Alleged Exposure of Watchlist Data

We inquired about the Department's response to the alleged July 2021 exposure of more than 1.9 million TSC terrorist watchlist records online. Based on DHS documentation and statements by senior officials, we concluded that on July 19, 2021, the date of the incident, DHS notified TSC of the alleged exposure of watchlist data. In doing so, DHS complied with its requirement to immediately notify TSC of any unauthorized use or disclosure of information.[11] According to DHS, TSC reviewed the matter and notified the Department that the exposed data contained old screenshots of useless information.

[8] TECS facilitates information sharing among Federal, state, local, tribal, and international partners to input, access, or maintain law enforcement, inspection, intelligence-gathering, and operational records.

[9] Secure Flight matches the identifying information of aircraft passengers and certain nontravelers against records in the Federal terrorist watchlist.

[10] DHS 4300A, Attachment G, *Rules of Behavior*, Aug. 5, 2014, outlines user responsibilities when accessing DHS systems and information technology resources capable of accessing, storing, receiving, or transmitting sensitive information. DHS Rules of Behavior apply to every employee and contractor.

[11] *Memorandum of Understanding Between the Department of Homeland Security and the Terrorist Screening Center Regarding the Use of Terrorist Identity Information for the Department of Homeland Security Watchlist Service.*

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine whether DHS has an effective approach to safeguard and share terrorist screening data. During this audit, we focused on the policies, procedures, and technology systems DHS uses to safeguard terrorist screening data.

We assessed internal controls related to safeguarding watchlist data. Because our audit was limited to addressing our objective, it may not disclose all internal control deficiencies that may have existed at the time of our audit. As discussed in the body of this report, we did not identify weaknesses with DHS components' policies and procedures for safeguarding and sharing sensitive information nor with how DHS staff members safeguard the data.

We researched and applied Federal, Department, and component criteria related to DHS requirements. We obtained and analyzed reports, testimony, and other documents, and reviewed previous Government Accountability Office and DHS OIG reports to identify relevant findings, recommendations, and associated follow-up actions.

Focusing specifically on CBP's and TSA's inspection of travelers, we used documentary and testimonial evidence to evaluate whether DHS has policies, procedures, and information technology system capabilities to meet Federal standards for safeguarding and sharing watchlist data. We analyzed 87 documents and interviewed 106 officials, program managers, and technology specialists from DHS headquarters offices, CBP, and TSA. Officials also responded to numerous requests for detailed written information relating to information technology security and protection procedures, including governance and oversight, access, monitoring, security controls, privacy considerations, and user access and training.

We conducted this performance audit between January and March 2022 pursuant to the *Inspector General Act of 1978*, as amended, and generally accepted government auditing standards except that we did not conduct data reliability testing of the watchlist. 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We did not conduct a data reliability assessment of the watchlist because DHS does not own the data. Therefore, it was not applicable.

The Office of Audits major contributors to this report are Kristen Bernard, Assistant Inspector General for Audits; Craig Adelman, Director; Christopher Browning, Audit Manager; Swati Nijhawan, Analyst-in-Charge; Maria Holmes, Auditor; and Telogia Moore, Auditor.

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Acting Undersecretary for Management
Commissioner, U.S. Customs and Border Protection
Administrator, Transportation Security Administration
Audit Liaison, Office of Strategy, Policy, and Plans
Audit Liaison, Office of Biometric Identity Management
Audit Liaison, Office of Intelligence and Analysis
Audit Liaison, U.S. Customs and Border Protection
Audit Liaison, Transportation Security Administration

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

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