United States House of Representatives
Committee on Oversight and Government Reform
Majority Staff
January 2008

INFORMATION SECURITY BREACH AT TSA:
THE TRAVELER REDRESS WEBSITE

Prepared for

Chairman Henry A. Waxman

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In October 2006, the Transportation Security Administration launched a website to help travelers whose names were erroneously listed on airline watch lists. This redress website had multiple security vulnerabilities: it was not hosted on a government domain; its homepage was not encrypted; one of its data submission pages was not encrypted; and its encrypted pages were not properly certified. These deficiencies exposed thousands of American travelers to potential identity theft. After an internet blogger identified these security vulnerabilities in February 2007, the website was taken offline and replaced by a website hosted on a Department of Homeland Security domain.

At the request of Chairman Henry Waxman, Committee staff have been investigating how TSA could have launched a website that violated basic operating standards of web security and failed to protect travelers' sensitive personal information. As this report describes, these security breaches can be traced to TSA's poor acquisition practices, conflicts of interest, and inadequate oversight.

The report finds:

- **TSA awarded the website contract without competition.** TSA gave a small, Virginia-based contractor called Desyne Web Services a no-bid contract to design and operate the redress website. According to an internal TSA investigation, the "Statement of Work" for the contract was "written such that Desyne Web was the only vendor that could meet program requirements."

- **The TSA official in charge of the project was a former employee of the contractor.** The TSA official who was the "Technical Lead" on the website project and acted as the point of contact with the contractor had an apparent conflict of interest. He was a former employee of Desyne Web Services and regularly socialized with Desyne's owner.

- **TSA did not detect the website's security weaknesses for months.** The redress website was launched on October 6, 2006, and was not taken down until after February 13, 2007, when an internet blogger exposed the security vulnerabilities. During this period, TSA Administrator Hawley testified before Congress that the agency had assured "the privacy of users and the security of the system" before its launch. Thousands of individuals used the insecure website, including at least 247 travelers who submitted large amounts of personal information through an insecure webpage.

- **TSA did not provide sufficient oversight of the website and the contractor.** The internal TSA investigation found that there were problems with the "planning, development, and operation" of the website and that the program managers were "overly reliant on contractors for information technology expertise" and had failed to properly oversee the contractor, which as a result, "made TSA vulnerable to non-performance and poor quality work by the contractor."

Neither Desyne nor the Technical Lead on the traveler redress website has been sanctioned by TSA for their roles in the deployment of an insecure website. TSA continues to pay Desyne to host and maintain two major web-based information systems: TSA's claims management system and a government-wide traveler redress program. TSA has taken no steps to discipline the Technical Lead, who still holds a senior program management position at TSA.

I. BACKGROUND

A. The Traveler Watch Lists

TSA was created on November 19, 2001, just two months after the 9/11 attacks. The agency was charged with "day-to-day Federal security screening operations for passenger air transportation."[1] One of its earliest actions was to split the Federal Aviation Administration's "watchlist" of persons not allowed to board commercial airlines into two separate lists: a "No-Fly List" and a "Selectee List." Individuals on the No-Fly List are not allowed to board commercial flights, while travelers on the Selectee List are allowed to board only after additional security screening procedures.

TSA does not publicly confirm the names on the lists or the criteria it uses to add names to the lists. [2] According to press accounts, the size of these lists increased rapidly after September 11, 2001, as a variety of government agencies submitted names. One consequence of the growth of the No-Fly and Selectee Lists was the dramatic increase in "false positives," cases in which travelers with names identical or similar to names of suspected terrorists were prevented from boarding flights or were singled out for additional security inspections. Well-known false positives include Senator Ted Kennedy, whose name was close to the name of a suspected terrorist, and Catherine Stevens, the wife of Senator Ted Stevens, whose name was similar to "Cat" Stevens, the former name of the singer Yusuf Islam.[3]

Investigations by GAO and the Department of Justice Inspector General have revealed significant inaccuracies in the two watch lists. In June 2005, the Justice Department IG reported a number of "weaknesses in the completeness and accuracy" of the Terrorist Screening Center (TSC) database, the central database maintained by the FBI from which names for the No-Fly Lists are extracted.[4] A 2007 follow-up to this audit found that weaknesses persist in the management of the TSC database and that 43% of the names reported to the TSC are false positives.[5] A 2006 GAO report produced a similar result,

[1] P.L. 107-71, 115 Stat. 597, 49 USC 114(h).

[2] Department of Homeland Security Privacy Office, Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Apr. 27, 2006). See also Department of Homeland Security, Notice of Privacy Act System of Records, 72 Fed. Reg. 2298 (Jan. 18, 2007) (waiving Privacy Act rights of travelers for the new DHS TRIP program).

[3] *Aviation Security Chief Says No-Fly List is Being Reduced by Half,* Associated Press (Jan. 18, 2007). *See also Sixty Minutes*, CBS News (June 10, 2007) (multiple cases involving travelers named Robert Johnson); Robert O'Harrow, Jr., *No Place to Hide*, 229 (2005) (case involving United States single-sculls rowing champion Aquil Abdullah); *Fla. 7-Year-Old on Terrorist No-Fly List*, The News-Press (Fort Myers, Florida) (July 24, 2007) (case involving seven–year old Michael Martin and four-year old Edward Allen).

[4] U.S. Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center* (Audit Report No. 05-27) (June 2005).

[5] U.S. Department of Justice, Office of the Inspector General, *Follow-Up Audit of the Terrorist Screening Center* (Audit Report 07-51) (Sept. 2007).

finding that roughly half of the tens of thousands of potential matches sent to the FBI were not found to match known or suspected terrorists.[6]

In early 2007, TSA Administrator Kip Hawley announced that the agency had completed a "scrub" of the No-Fly List that reduced it by approximately 50% and promised a similar review for the Selectee List.[7] According to a recent audit conducted by the Department of Justice Inspector General, this "scrub" reduced the No-Fly List from 71,872 records to 34,230 records.[8]

B. The Need for a Redress Program

To address concerns about the high incidence of mistakes in the TSA watch lists, Congress directed TSA in 2004 to develop a prescreening process that would "not produce a large number of false positives" and would give misidentified airline passengers an effective way to correct the information in the database.[9]

In accordance with this legislation, TSA established the Office of Transportation Security Redress as a central point of contact for travelers with complaints about the watch lists. This new office created a "Traveler Identity Verification Program," through which individuals could submit documents showing they were not the same persons listed on the watch lists.[10] When this office verified that an individual was not a suspected terrorist, it placed the individual's name on a "cleared list," which was updated and shared with the airlines.

TSA required travelers seeking redress to provide the following personal information, in addition to identity documents such as passports, birth certificates, or certificates of citizenship:

- Name
- Social Security Number
- Birth Date
- Birth Place
- Sex
- Height
- Weight
- Hair Color

[6] U.S. General Accounting Office, Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public (Sept. 2006) (GAO-06-1031).

[7] Senate Committee on Commerce, Science, and Transportation, Statement of Kip Hawley. *Aviation Security — Reviewing the Recommendations of the 9/11 Commission,* 110th Cong. (Jan. 17, 2007). *See also* Schneier on Security blog, *Interview with Kip Hawley* (online at http://www.schneier.com/interview-hawley.html) (Aug. 1, 2007).

[8] DOJ OIG Sep. 2007, *supra* note 5. *See also Sixty Minutes*, CBS News (June 10, 2007) (reporting that the No-Fly list has 44,000 names and Selectee list has 75,000 names).

[9] Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, 118 Stat. 3714, 4012 (A), amending 49 U.S.C. 44903(j)(2).

[10] GAO Report, *supra* note 6.

- Eye Color
- Address
- Home and Work Telephone Numbers

TSA was quickly overwhelmed with traveler verification requests. According to TSA officials, only two or three officials were handling tens of thousands of paper requests that came in from around the country.[11]

To address these problems, TSA began planning for a website to speed the processing of identity verification submissions.[12] In February 2006, TSA's Redress Office completed a basic business plan for the online program. This plan, as modified, led to the creation of the traveler redress website at TSA.

II. AWARD OF THE NO-BID CONTRACT

In evaluating the plan for the traveler redress website, TSA's Information Technology Division determined that TSA's current platform could not accommodate a new redress website.[13] The Redress Office responded to this determination by asking outside contractors for a solution. On April 10, 2006, TSA issued a "Request for Quote" (RFQ) seeking bids from outside contractors to build, host, and maintain "a secure web-based system to receive and record and process data received for persons requiring redress."[14]

According to TSA investigators, the RFQ was written in such a way that a small northern Virginia web marketing firm called Desyne Web Services was "the only vendor that could meet program requirements."[15] Desyne had been doing work for TSA since 2004 under several contracts awarded without competition.[16] Under these contracts, Desyne performed hosting and other services for TSA's claims management website, a site that allows travelers to file online claims against TSA for damaged property. The "Statement of Work" included in the RFQ specified that the design of the website had to be consistent with that of the claims management website. It also required that the site be hosted on the server that already hosted the claims management site. According to the internal TSA review, these requirements "precluded another contractor from hosting and maintaining RMS [Redress Management System]."[17]

Desyne Web Services was the only company to respond to TSA's offer to develop the watch list redress website. On April 13, 2006, three days after the RFQ was issued, Desyne submitted a bid to develop, host, and maintain the redress website for one year.

[11] Briefing by Staff, Transportations Security Administration, to House Committee on Oversight and Government Reform Staff (Sept. 14, 2007).

[12] *Id.*

[13] Transportation Security Administration, Office of Inspection, *Review of Redress Management System Information Security* (IR-07-0012) (May 2007).

[14] TSA Request for Quotation, HSTS03-06-Q-OSC001.

[15] TSA Office of Inspection Review, *supra* note 13.

[16] TSA Contract #s HSTS03-04-P-AOP134 (with two modifications) and HSTS04-05-P-AOP057.

[17] TSA Office of Inspection Review, *supra* note 13.

One week later, TSA and Desyne executed a fixed price contract identical to Desyne's proposal.[18] The value of this contract was $48,816.[19]

Accompanying the contract document was the "Justification for a Single Source Award" required under federal acquisition regulations. This document explained that because Desyne could re-use some of the code it used when it created the claims management website, it would be able to develop the traveler redress website more quickly and at a lower cost than any other vendor. The justification document concluded that "Desyne Web Services Inc. is the only company capable of meeting our development timeline and avoid [sic] substantial cost duplication."[20]

III. CONFLICTS OF INTEREST

TSA investigators found that the primary author of the April 2006 statement of work was the director of the Claims Management Office, Mr. Nicholas Panuzio. Mr. Panuzio, who was also assigned the key role of "Technical Lead" on the redress website project, had a prior relationship with Desyne Web Services. Mr. Panuzio told TSA investigators he had known Desyne's owner since high school, had worked for Desyne for eight months in 2001 and 2002, and still met regularly with Desyne's owner and others for drinks or dinner in Tysons Corner.[21]

Mr. Panuzio played a key role in the development of the traveler redress website. For example, one e-mail exchange shows that the Redress Management project director, Mr. James Kennedy, relied on Mr. Panuzio's recommendation to pay Desyne's December 2006 invoice.[22] Although he had earlier disclosed this conflict of interest to the TSA Office of Chief Counsel, Mr. Panuzio did not disclose it to the project manager or to the lead contracting officer on the project.[23]

According to TSA investigators, Mr. Panuzio's close relationship with Desyne seemed to blur the lines between the contractor's performance of the contract and TSA's contract oversight. Mr. Panuzio told the investigators that he had remote access into Desyne's website to update the content portion of the website, even though the contract specified that Desyne was responsible for content changes.[24] According to the internal TSA report, "the Technical Lead [Mr. Panuzio] was positioned to become the single point of failure for system errors and security vulnerabilities."[25]

[18] TSA Contract #HSTS03-06-P-OSC001.

[19] *Id.*

[20] *Id.*

[21] Transportation Security Administration, Office of Inspection, *Report of Investigation # I070143* (Aug. 10, 2007).

[22] E-mail from Director, Office of Transportation Security Redress, Transportation Security Administration, to Contracts Manager/COTR, Office of Special Counselor, Transportation Security Administration (Jan. 8, 2007).

[23] *TSA Report, supra* note 21.

[24] TSA Office of Inspection Review, *supra* note 13.

[25] *Id.*

TSA investigators were also critical of the project director for failing to properly oversee Mr. Panuzio's activities. The investigators found that although the project director, Mr. Kennedy, was appointed as both the "System Owner"[26] and "Information System Security Officer,"[27] he did not have the technical expertise to effectively perform these functions and in practice delegated them to Mr. Panuzio.[28] According to the investigators, Mr. Panuzio in turn "did not have the necessary information technology security knowledge to ensure that RMS was developed in a secure environment."[29]

IV. WEBSITE SECURITY VULNERABILITIES

After conducting a detailed security accreditation review of the traveler redress website, TSA's Chief Information Security Officer (CISO) granted the website a 12-month "Authority to Operate" in September 2006. The CISO did not detect a number of glaring security problems affecting the website when it went live on October 6, 2006.

The security vulnerabilities of the website included the following:

- **The Site Was Not Hosted on a Government Domain.** Instead of being hosted on a government web domain (*e.g.*, "tsa.gov"), the redress system was hosted on a commercial domain operated by the contractor (http//rms.desyne.com). When they left the government domain, visitors to the redress management site lost any assurance they were visiting a legitimate government website.[30]

- **The Home Page Was Not Encrypted.** The website home page did not have an encrypted "secure socket layer" (SSL) with an "https" protocol identifier. As a result, every time travelers visited the site to check on the status of their applications, the control numbers they entered to access their files were

[26] "The *information system owner* is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The information system owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements." National Institute of Standards and Technology, *Guide for the Security Certification and Accreditation of Federal Information Systems*, 15 (NIST Special Publication 800-37) (May 2004).

[27] "The *information system security officer* is the individual responsible to the … information system owner … for ensuring the appropriate operational security posture is maintained for an information system or program … The information system security officer typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations of the system." *Id.*

[28] TSA Office of Inspection Review, *supra* note 13.

[29] *Id.*

[30] *Id. See also Homeland Security Site Hacked by Phishers? 15 Signs Say Yes,* Wired News Threat Level Blog (Feb. 14, 2007) (online at http://blog.wired.com/27bstroke6/2007/02/homeland_securi.html) (exhibiting an image of the TSA Traveler Identification Verification Program web page captured during the time it used the rms.desyne.com domain address).

vulnerable to theft. Once they obtained these numbers, attackers would have access to travelers' personal information.[31]

- **The Submission Page Was Not Encrypted.** One of the site's links that allowed travelers to submit personal information was also unsecured. Although travelers could access an encrypted page to submit personal information, a link reading "file your application online" transferred users to an unsecured site. Travelers submitting their name, address, Social Security numbers, eye color, place of birth, and other sensitive personal information through this link had no protection from attack.[32]

- **Encrypted Pages Were Not Properly Certified.** Although other web pages within the site were SSL-protected, they were not properly certified. Under standard web security practices, operators of SSL-protected websites obtain third-party certifications to assure users that an outside party has approved the web site's security measures. Instead of the proper third-party certification, the site had only an expired certification that Desyne itself had generated.[33]

These were serious security deficiencies. As one commentator noted:

> Consider what this means for a passenger who is stewing in the airport terminal after missing his flight because a TSA screener confused him with that *other* Robert Johnson on the TSA's special list. The good Mr. Johnson is told he can try to prevent this misunderstanding from happening again if he submits data requested by the travel identity verification site. He pops open his laptop, hops on the airport's terminal wireless network, completes the form and clicks "submit." Meanwhile, a digital terrorist has just captured the data Johnson has submitted because it was sent without SSL.[34]

V. FAILURE TO DETECT THE SECURITY VULNERABILITIES

The security vulnerabilities in the traveler redress website were discovered by Chris Soghoian, a Ph.D. student at the University of Indiana's School of Informatics. On February 13, 2007, Mr. Soghoian posted his analysis of the website's security weaknesses on his "Slight Paranoia" blog. Mr. Soghoian reported that the site was hosted on a commercial domain, that some pages were not protected by a "secure socket layer,"

[31] *Id.*

[32] TSA Office of Inspection Review, *supra* note 13.

[33] *Id. See also TSA Not Living Up to Its Middle Name*, www.washingtonpost.com "Security Fix" Weblog (online at http://blog.washingtonpost.com/securityfix/2007/02/tsa_ not_living_up_to_its _middl_1.html) (Feb. 14, 2007) (reporting that the Internet Explorer web browser provided a warning that read: "There is a problem with this Web site's security certificate. We recommend that you close this webpage and do not continue to this website").

[34] *Id.*

and that pages that were SSL-protected were not properly certified.[35] His findings were quickly picked up by several other computer security blogs on the morning of February 14, 2007, which added additional details to Mr. Soghoian's analysis.[36]

Mr. Soghoian told Committee staff that the website captured his attention because it required users to submit a great deal of personal information. He said the appearance of the site was so poor that he first suspected it was a "phishing" site, a site internet hackers had created to look like a TSA website.[37] Other commentators observed that these deficiencies, such as the failure to have a valid third-party certificate, should have been easily detected by TSA:

> Incredible that they would take the site live using a self-signed certificate. It shows major incompetence (elementary oversight should have caught this) and at Desyne, Inc. Someone is either too stupid or too cheap to purchase a real SSL certificate before putting up a site that asks for personal data. This is Web Development 101. Anyone who has ever worked on an ecommerce site should [be] aware of the issues.[38]

Prior to Mr. Soghoian's posting, nobody at TSA appears to have detected these problems. As a result, the website operated from October 6, 2006, to February 13, 2007, with significant, easily identifiable, and correctable security weaknesses. According to TSA investigators, thousands of travelers submitted their personal information to TSA through the traveler redress website during this period. At least 247 travelers submitted their personal information through the unsecured "file your application online" link.[39]

During the four months the redress website was operating with these security weaknesses, TSA appears to have been under the impression that the site had no security problems. On January 17, 2007, TSA Administrator Hawley testified before the Senate Committee on Commerce, Science, and Transportation:

> After assuring the privacy of users and the security of the system, RMS [Redress Management System] was launched on October 6, 2006, enabling travelers to submit and check the status of their applications electronically via the internet.[40]

[35] Slight Paranoia Web Blog, *TSA Has Outsourced the TSA Traveler Identity Verification Program?* (Feb. 13, 2007) (online at http://paranoia.dubfire.net/2007/02/tsa-has-outsourced-tsa-traveler.html).

[36] *See TSA Not Living Up to Its Middle Name*, www.washingtonpost.com, *supra* note 33. *Homeland Security Site Hacked by Phishers? 15 Signs Say Yes*, Wired News Weblog (Feb. 14, 2007).

[37] Telephonic Interview with Christopher Soghoian by Committee Staff, House Committee on Oversight and Government Reform (Apr. 12, 2007).

[38] *TSA Not Living Up to Its Middle Name*, www.washingtonpost.com "Security Fix" Weblog (Feb. 14, 2007) (Comment posted by "Mark A. Gollin" at 10:32 a.m.).

[39] TSA Office of Inspection Review, *supra* note 13.

[40] Senate Committee on Commerce, Science, and Transportation, Statement of Kip Hawley. *Aviation Security — Reviewing the Recommendations of the 9/11 Commission,* 110th Cong. (Jan. 17, 2007).

TSA's own internal investigation, completed in May 2007, concluded:

> OI [Office of Inspection] found problems with the planning, development, and operation of the RMS [Redress Management System]. The existing business environment at TSA causes program management to be overly reliant on contractors for information technology expertise. Further, although the oversight activities of the Office of the Chief Information Security Officer (CISO) identified several high risks during the initial evaluation of RMS, they were not sufficient to ensure that critical issues were properly resolved before the system became operational. Finally, a lack of adequate contractor oversight made TSA vulnerable to TSA non-performance and poor quality work by the contractor.[41]

VI. THE TSA RESPONSE

After Mr. Soghoian posted his analysis of the security vulnerabilities affecting the traveler redress website, TSA moved quickly to transfer the site to a more secure Department of Homeland Security domain. TSA also contacted the individuals who had submitted their personal information through the unsecured "file your application online" link to inform them that they were at a heightened risk of identity theft.[42]

TSA did not take action, however, to sanction Desyne for poor performance. As of late 2007, Desyne continued to operate both TSA's claim management website and the DHS-wide online traveler redress program.[43] To date, TSA has awarded Desyne almost $500,000 worth of no-bid contracts to provide web services to TSA and DHS.

TSA also did not sanction Mr. Panuzio. The internal TSA investigation found he had not profited personally from the Desyne contract. For this reason, TSA closed the investigation without recommending any administrative action against him.

VII. CONCLUSION

There were multiple factors that contributed to security vulnerabilities in the TSA traveler redress website. They included poor procurement practices, conflicts of interest, and weak oversight. The result of these shortcomings was that an insecure website collected sensitive personal information from American travelers for months without detection by TSA.

[41] *Id.*

[42] TSA Office of Inspection Review, *supra* note 13.

[43] Sept. 14, 2007 TSA staff briefing, *supra* note 11.