

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 governmentwide traveler redress program. TSA has taken no steps to discipline the Technical Lead, who still holds a senior program management position at TSA.

Documents and Links

- [Report: Information Security Breach at TSA: The Traveler Redress Website](#)