



### Why This Matters

Radio Frequency Identification (RFID) is a form of automatic identification and data capture technology that uses radio frequencies to transmit information. The flexibility and portability of RFID technology has introduced new security risks to agency systems, such as cloning of an RFID tag and the security of the database that stores personal data. U.S. Customs and Border Protection (CBP) employs RFID technology as part of its Trusted Traveler Programs (TTP) to allow pre-screened travelers expedited processing at designated ports of entry.

### DHS Response

CBP concurred with the two recommendations and is taking actions to address these recommendations.

## Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs

### What We Determined

CBP maintains the integrity of the TTP through a stringent screening process that includes automated searches against multiple law enforcement databases, 24-hour system checks to verify status of enrolled travelers, and random selections of registered travelers for secondary inspection. CBP developed a TTP handbook that includes procedures for inspecting travelers at the ports of entry and policies for enrolling travelers into the TTP. To reduce the risk of theft of personally identifiable information, CBP stores a unique identification number embedded in TTP cards and locks the RFID memory chip to prevent modification of stored data. Further, CBP has implemented effective physical controls over the readers and computer equipment supporting the trusted traveler systems at the ports of entry visited. Lastly, CBP has established a system test environment that simulates land border inbound and outbound inspection operations at CBP's government test lane facility.

While CBP has taken actions to secure travelers' personally identifiable information, including safeguards to lessen the risks of using RFID technology, we identified deficiencies in other areas of TTP that need improvements. Specifically, we identified deficiencies in CBP's implementation of DHS' baseline configuration settings, and personnel overseeing TTP systems have not received the required specialized training within the past year.

### What We Recommend

We recommend that the Assistant Commissioner and Chief Information Officer, CBP

- (1) Implement the required DHS sensitive systems configuration settings on Windows and Oracle-Linux servers that support the TTP or accept the risk by documenting the deviations in the system security plan.
- (2) Provide technical staff with the required specialized trainings and skills necessary to properly secure the global enrollment system and the sensitive information residing within the system.

### For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)