



OST

Report ZA2023030
May 24, 2023

Fragmented Processes Weaken DOT's Accountability for Contractor Employee PIV Cards



Fragmented Processes Weaken DOT's Accountability for Contractor Employee PIV Cards

Self-initiated

Office of the Secretary of Transportation | ZA2023030 | May 24, 2023

What We Looked At

The Personal Identity Verification (PIV) card is the Department's foundation for securely identifying every individual seeking access to the Department of Transportation's (DOT) secure facilities and information systems. Once contractor employees no longer need that access, DOT officials must promptly collect and deactivate their PIV cards. In fiscal years 2020 and 2021, just over 1,000 DOT service contracts—which may have granted contractor staff access to secure DOT facilities and information systems—came to an end. Given that most of these contracts ended during the COVID-19 pandemic when DOT employees were in a state of maximum telework, there is an elevated risk that prompt and appropriate PIV card collection and deactivation may not have occurred. Accordingly, DOT-OIG initiated this audit to assess DOT's oversight of contractor employee PIV cards issued in connection with performance of agency contracts.

What We Found

DOT's timely collection and deactivation of contractor employee PIV cards is compromised by fragmented processes and a lack of clear accountability. Counter to Federal and departmental procurement regulations and policies, DOT contracting officials do not always include required PIV card-related security clauses in contracts that grant contractor employees routine physical access to a federally controlled facility or information system. Without these required clauses in its contracts, DOT neglected to establish an important and legally enforceable accountability mechanism to help protect its secure facilities and systems. Further, DOT does not always promptly collect and deactivate contractor employee PIV cards as required, because it has not established clear accountability over this process. As a result, DOT is exposed to heightened security risks, potentially compromising the safety of its staff and achievement of its mission.

Our Recommendations

We made six recommendations to improve DOT's collection and deactivation of contractor employee PIV cards. DOT concurred with all six recommendations and provided appropriate actions and completion dates. We consider all recommendations resolved but open pending completion of the planned actions.

All OIG audit reports are available on our website at www.oig.dot.gov.

For inquiries about this report, please contact our Office of Government and Public Affairs at (202) 366-8751.

Contents

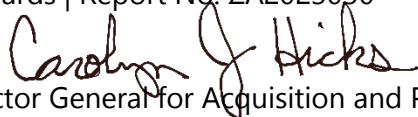
Memorandum	1
Results in Brief	3
Background	4
Fragmented Processes and Unclear Accountability Impede DOT's Timely Collection and Deactivation of Contractor Employee PIV Cards	6
Conclusion	15
Recommendations	15
Agency Comments and OIG Response	16
Actions Required	16
Exhibit A. Scope and Methodology	17
Exhibit B. Organizations Visited or Contacted	19
Exhibit C. List of Acronyms	20
Exhibit D. Details of the 64 Sample Contracts	21
Exhibit E. Major Contributors to This Report	22
Appendix. Agency Comments	23



Memorandum

Date: May 24, 2023

Subject: ACTION: Fragmented Processes Weaken DOT's Accountability for Contractor Employee PIV Cards | Report No. ZA2023030

From: Carolyn J. Hicks 
Assistant Inspector General for Acquisition and Procurement Audits

To: Assistant Secretary for Administration

To enhance security, increase Government efficiency, and reduce identity fraud, a 2004 Presidential Directive¹ required Federal agencies to use a standard, secure form of identification for employees and contractors who access federally controlled facilities and information systems. In response, the Department of Transportation (DOT) began issuing Personal Identity Verification (PIV) cards—the common authentication mechanism across the Federal Government²—to its employees and contractor staff. The PIV card is now the foundation of the Department's process for securely identifying every individual seeking access to DOT's valuable and sensitive resources, including facilities and information systems.³

Each year, DOT awards billions in contracts and orders for services that support achievement of its mission. When necessary to execute a particular service, DOT officials must issue PIV cards to contractor employees, granting them access to secure, and sometimes sensitive, DOT facilities and information technology (IT) systems. However, when DOT does not take prompt action to collect and deactivate these cards, it risks potentially compromising the safety of its staff and achievement of its mission. For example, a former DOT contractor employee retained his PIV card during the 12 days between his transfer from a DOT facility in Illinois to one in Hawaii. Then he entered the Illinois facility and deliberately

¹ Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

² Federal Information Processing Standards (FIPS 201-3), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022.

³ A PIV card is a photo identification card that contains a computer chip, which allows it to receive, store, recall, and send information in a secure method. The card's main function is to encrypt or code data to strengthen the security of employees, information systems, and secured facilities.

started a fire. In the process, he destroyed critical infrastructure equipment, disrupted the national transportation system for weeks, and cost the public over \$350 million.⁴

In this audit, we looked at DOT contracts with a total value greater than \$250,000. We estimate that 518 DOT service contracts and orders⁵ meeting this threshold and granting contractors access to secure DOT facilities and information systems came to an end in fiscal years 2020 and 2021.⁶ With a total value of approximately \$890 million, these contracts provided mission critical services such as research and development, testing, security, and IT support at DOT Headquarters and other facilities across the country. Most of these contracts ended during the COVID-19 pandemic—when DOT employees were in a state of maximum telework. Thus, there was an increased risk that prompt and appropriate PIV card collection and deactivation did not occur.

Accordingly, we initiated this audit with the objective to assess DOT's oversight of contractor employee PIV cards issued in connection with performance of agency contracts. Given the Federal Aviation Administration's (FAA) unique procurement requirements and the scope of its facilities and systems, we excluded it from this audit.⁷

We conducted this audit in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology. Exhibit B lists the organizations we visited or contacted, and exhibit C lists the acronyms used in this report.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please contact me or Jill Cottonaro, Program Director.

cc: The Secretary
DOT Audit Liaison, M-1

⁴ This 2014 incident occurred at an FAA facility in Illinois at a time when Agency policy did not address collection and deactivation requirements for such a situation. The incident exemplifies how critical prompt collection and deactivation of DOT contractor employee PIV cards is to the safety and security of Department personnel and our Nation's transportation systems.

⁵ Throughout this document, we refer to our universe and sample as "contracts," although they include both direct contracts and orders.

⁶ The 518 contract estimate has a 90-percent confidence interval of 440 to 595. The \$890 million estimate has a 90-percent confidence interval of \$765 million to \$1,016 million.

⁷ One of the sample contracts was awarded off an FAA contract vehicle. Therefore, the clauses in the FAA vehicle were incorporated into the terms of the sample contract awarded by another DOT Operating Administration (OA). As such, we considered FAA PIV card-related requirements when applicable.

Results in Brief

Fragmented processes and unclear accountability impede DOT's timely collection and deactivation of contractor employee PIV cards.

Contract clause omissions. Counter to Federal and departmental procurement regulations and policies, DOT contracting officials do not always include required PIV card-related security clauses in contracts that grant contractor employees routine physical access to a federally controlled facility or information system. Specifically, 27 of the 64 DOT contracts in our sample, valued at \$161.1 million, did not include all required PIV card-related security clauses. This includes clauses that hold contractors accountable for responsibilities such as notifying the contracting officer (CO) when access to DOT systems or facilities is no longer necessary and returning employee PIV cards as soon as they are no longer needed. The officials who awarded these contracts stated the clause omissions were an oversight on their agency's part, which suggests that DOT lacks an adequate control process to verify these required clauses are included when applicable. Some Operating Administrations (OA) have started taking actions to address this deficiency. Still, by omitting these required clauses from applicable contracts, DOT has neglected to establish an important and legally enforceable accountability mechanism to help ensure contractors return their employees' PIV cards.

Untimely collection and deactivation. Timely PIV card collection and deactivation is critical for mitigating security risks to Government facilities, systems, and employees. However, we found that DOT does not always promptly collect and deactivate contractor employee PIV cards as required by departmental and Federal policy, because DOT has not established clear accountability over this process. Specifically, DOT did not collect and/or deactivate 294 (25 percent) of the 1,184 contractor employee PIV cards analyzed. Further, DOT officials did not collect 77 (7 percent) of the remaining contractor employee PIV cards in a timely manner. These 77 cards were collected anywhere from 1 to 646 days after the cards were no longer needed, and 56 of the cards were not deactivated until a time ranging from 1 to 598 days after the cards were no longer needed. Several OAs are now taking steps to help improve timely collection and deactivation of their contractor employee PIV cards. Nevertheless, when DOT does not promptly collect and deactivate contractor employee PIV cards, it leaves the Department's secure and sensitive facilities and systems more vulnerable to a threat of malicious actors gaining unwarranted access.

We are making recommendations to improve DOT's inclusion of required PIV card-related security clauses in contracts and its collection and deactivation process for contractor employee PIV cards.

Background

In order for a contractor employee to obtain a PIV card, the DOT Office of Security must receive a completed PIV application for that employee. This application includes information about why the contractor employee needs a PIV card. The contractor employee must also pass a background investigation. The PIV card's expiration date can be no more than 3 years from issuance and is typically set based on the contract's period of performance. If the period of performance is longer than 3 years or the PIV card expires, the contractor employee must renew it by completing a new PIV application and, if required, another background investigation.

DOT's PIV Card Program is governed by DOT Order 1681.2A, which complies with the Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standards (FIPS 201-3). The actual processes and accountability for overseeing contractor PIV cards—including collecting and deactivating them—typically involve various DOT employees including Office of Security personnel, COs and Contracting Officer Representatives (COR), Security Coordinators, Sponsors, and Trusted Agents. See table 1 for a summary of PIV Card Program responsibilities by title or office.

Table 1. Responsibilities of DOT Employees Involved in PIV Card Program Processes per DOT Order 1681.2A

Title or Office	PIV Card Responsibilities
DOT's Office of Security (Serves OST and all OAs, except FAA, which has its own security office.)	<ul style="list-style-type: none"> • Manages implementation of policy, procedures, and standards for PIV card issuance. • Monitors PIV program effectiveness and recommends corrective actions and improvements. • Develops new policies and techniques to improve PIV card security. • Gives OAs advice, guidance, and direction on PIV card policy interpretation and application. • Maintains DOT's PIV Card Program website with relevant and updated information for all Department stakeholders. • Reviews PIV card application data and processes employee background investigations. • Issues, revokes, reactivates, and deactivates PIV cards.
COR/CO (Located in each OA/OST. COR role is usually a collateral duty.)	<ul style="list-style-type: none"> • Promptly collects PIV cards and immediately forwards to the Office of Security or Trusted Agents. • Ensures applicable security clauses are included in assigned contracts. • Ensures contractors are aware of and understand security clauses in assigned contracts.
Security Coordinator (Located in each OA/OST. A collateral duty.)	<ul style="list-style-type: none"> • Serves as the PIV Card manager for each DOT OA. • Selects and maintains a list of Trusted Agents, providing updates to the Office of Security. • Coordinates with the Office of Security for Trusted Agent training and technical support.
Sponsor (Located in each OA/OST. A collateral duty usually assumed by a COR.)	<ul style="list-style-type: none"> • Nominates an individual for a PIV card and justifies the need for a PIV card. • Confirms PIV card applicants are valid DOT employees or contractors and meet requirements. • Approves and submits a PIV application after the applicant completes it. • Approves PIV applications for contractor employees.
Trusted Agent (Located in each OA/OST. A collateral duty.)	<ul style="list-style-type: none"> • Serves as an OA's point-of-contact for DOT's PIV card program. • Manages the PIV card issuance process in accordance with program requirements. • Communicates with the Office of Security regarding policy changes. • Ensures PIV Cards have been authorized by the appropriate approvers. • Authorized to also issue, collect, revoke, and deactivate PIV cards. • Requires specialized training.

Source: OIG analysis

Our sample of 64 DOT contracts—comprising 5 direct contracts and 59 orders—totals \$542 million⁸ and represents the Office of the Secretary of Transportation (OST) and 6 OAs. In September 2021, while planning our audit, we pulled data from the Federal Procurement Data System (FPDS) for these 64 contracts; according to FPDS, they all ended in fiscal year 2020 or 2021. However, during the audit, we determined that two contracts are still active. According to DOT officials, these sample contracts involve over 1,250 contractor employees who were issued PIV cards. See exhibit D for details on the 64 sample contracts.

⁸ The total values reported throughout this report were calculated based on the final amount expended for sample contracts whose periods of performance have ended and the total potential value (base plus all option periods) for sample contracts whose performance was active at the time of our audit field work.

Fragmented Processes and Unclear Accountability Impede DOT's Timely Collection and Deactivation of Contractor Employee PIV Cards

DOT's timely collection and deactivation of contractor employee PIV cards is compromised by fragmented processes and a lack of clear accountability. Specifically, contracting officials do not consistently include required PIV card-related security clauses in applicable DOT contracts. In addition, Department officials do not always promptly collect and deactivate contractor employee PIV cards that are no longer needed.

DOT Does Not Consistently Include Required PIV Card-Related Security Clauses in Applicable Contracts

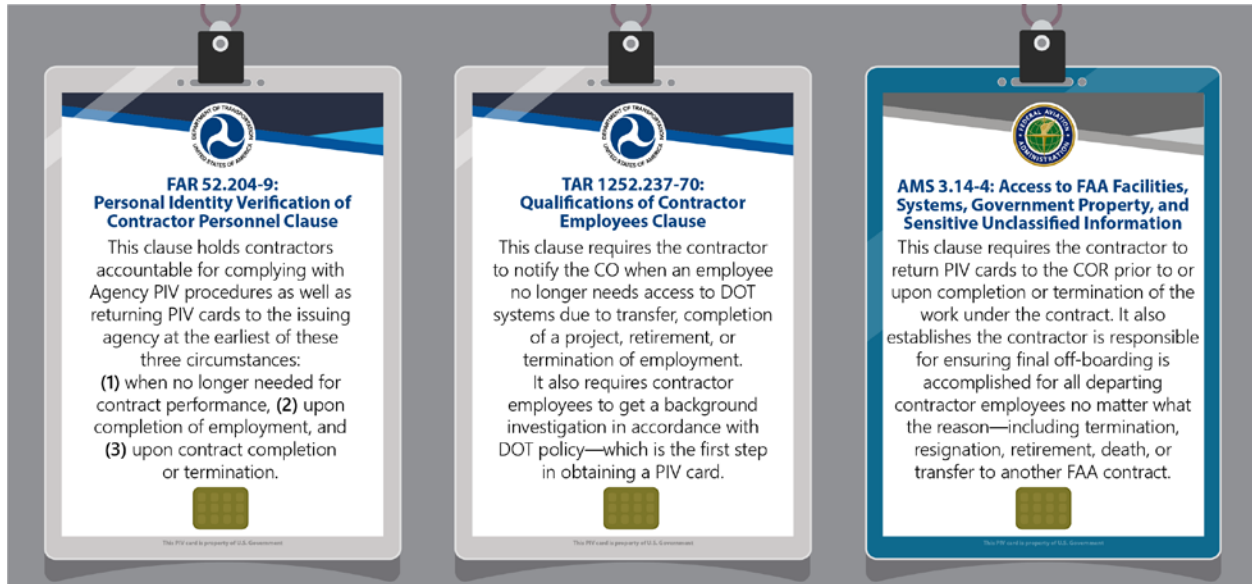
A contract is a legally binding agreement, and its clauses define its terms and conditions—including the obligations of each party involved. Federal and DOT procurement regulations and policies require COs to include specific PIV card-related security clauses in contracts that give contractor employees routine physical access to a federally controlled facility or information system.⁹ Specifically, DOT-awarded (non-FAA) contracts must include two PIV card-related security clauses,¹⁰ and FAA-awarded contracts must include one.¹¹ These clauses hold contractors accountable for obtaining background investigations for their employees; notifying the CO when access to DOT systems or facilities is no longer necessary; and returning employee PIV cards as soon as they are no longer needed for any reason. Reasons PIV cards may no longer be needed include contract completion, employee termination, or because access is unnecessary for continued contract performance. See the figure for a summary of the relevant clauses.

⁹ DOT Order 1681.2A(8)(h)(1), FAR 4.1303, Transportation Acquisition Regulations (TAR) 1237.110, and Acquisition Management System (AMS) 3.14-4.

¹⁰ FAR 52.204-9 and TAR 1252.237-70.

¹¹ AMS 3.14-4. Although FAA was exempt from this review, AMS clause requirements are relevant to our analysis because one of the FHWA contracts in our sample was awarded off an FAA contract vehicle.

Figure. Summary of DOT- and FAA-Required PIV Card Security Clauses



Source: OIG analysis

We found that 27 of the 64 sample DOT contracts valued at \$161.1 million did not include all the required clauses. Specifically, 11 contracts valued at \$39.1 million were missing the required Federal Acquisition Regulation (FAR) clause, and another 13 contracts valued at \$102.8 million did not include the required Transportation Acquisition Regulation (TAR) clause. Three other contracts valued at \$19.2 million were missing both required FAR and TAR clauses. The Acquisition Management System (AMS) clause was appropriately incorporated into one of the Federal Highway Administration's (FHWA) sample contracts valued at \$721,863—which was awarded off an FAA contract vehicle. See table 2 for more details on the noncompliant contracts awarded by OST and four of the OAs. We did not find any issues with the Federal Railroad Administration (FRA) and Pipeline and Hazardous Materials Safety Administration (PHMSA) contracts in our sample.

Table 2. Sample Contracts Missing Required PIV Card-Related Security Clauses

OA	Missing Only FAR Clause		Missing Only TAR Clause		Missing both FAR and TAR Clauses	
	Count	Total Value	Count	Total Value	Count	Total Value
FHWA	10 out of 24	\$31,946,606	5 ^a out of 24	\$55,443,784	2 out of 24	\$5,007,876
FMCSA	0 out of 6	-	2 out of 6	\$13,264,000	0 out of 6	-
FRA	0 out of 2	-	0 out of 2	-	0 out of 2	-
FTA	0 out of 10	-	1 out of 10	\$1,628,772	0 out of 10	-
NHTSA	1 ^b out of 4	\$7,122,318	0 out of 4	-	0 out of 4	-
OST	0 out of 12	-	5 out of 12	\$32,422,232	1 out of 12	\$14,234,390
PHMSA	0 out of 6	-	0 out of 6	-	0 out of 6	-

^a OST awarded four of these five contracts before transferring them to FHWA.

^b Although the FAR clause regarding personal identity verification of contractor employees was not included, the contract terms contain elements of the missing clause.

Source: OIG analysis

DOT's PIV Card Program Order also identifies the Heads of each OA and OST as responsible for ensuring standard security clause language is included in all applicable contracts.¹² Yet, when we asked why the 27 contracts did not include the required PIV card-related security clauses, the DOT officials from the 4 OAs and OST who awarded the contracts stated it was an oversight on their agency's part. This suggests that these OAs and OST lack an adequate control process to verify that their COs include the appropriate PIV card-related security clauses in applicable contracts.

Since the award of these contracts, some OAs have made changes to ensure PIV card-related security clauses are not omitted from future contracts. For example, as an FHWA official explained to us, beginning in fiscal year 2021, the Agency implemented standardized contract solicitation templates to help its COs ensure all required contract clauses are included. According to this official, these templates are regularly updated based on changes to the FAR and Departmental acquisition guidance. However, in using these templates, FHWA must rely upon

¹² DOT Order 1681.2A(8)(e)(9).

the CO for each contract to determine when to include the PIV card-related security clauses, as they are not always applicable.¹³

By failing to include required PIV card-related security clauses in its contracts, DOT has also neglected to establish an important and legally enforceable accountability mechanism. Making such a mechanism part of the terms and conditions of the contract could help the Department ensure proper use and management of contractor employee PIV cards. Encouraging contractors to return their contractor employees' PIV cards would also lessen DOT's vulnerability to the threat of malicious actors gaining access to its secure and sensitive facilities and systems, which could threaten the Department's critical missions and potentially compromise the safety of the traveling public.

DOT Does Not Always Promptly Collect and Deactivate Contractor Employee PIV Cards

DOT's PIV Card Program Order requires the COR—or the CO if a COR has not been appointed—to “promptly collect” contractor employees' PIV cards that are no longer needed and immediately forward them to the Office of Security or a Trusted Agent.¹⁴ The Order also states the contractor is responsible for ensuring its employees “promptly return” PIV cards that are no longer needed to their immediate supervisor, the COR, or the Office of Security.¹⁵ Regarding deactivation, Federal policy requires agencies to terminate and invalidate (i.e., deactivate)¹⁶ a PIV card when a person is no longer eligible to possess it.¹⁷ When collection is not possible, termination occurs within 18 hours of notification that a PIV card is no longer authorized. DOT's Order addresses deactivation only regarding lost, stolen, or compromised PIV cards. In these instances, Office of Security personnel or a Trusted Agent—the only people authorized to deactivate PIV cards—must deactivate the card within 18 hours of learning about the issue.¹⁸

We reviewed the PIV card history for the contractor employee PIV cards associated with the contracts in our sample. DOT initially identified 1,269 contractor employees with PIV cards; however, Department officials stated

¹³ Based on the scope of our audit, we cannot assert that this change affected FHWA's PIV contract clause compliance rates.

¹⁴ DOT Order 1681.2A(8)(h)(2).

¹⁵ DOT Order 1681.2A(8)(g)(8).

¹⁶ Deactivating a PIV card involves electronically disabling the logical and physical access the card granted to a contractor employee so they are no longer able to access Federal facilities and systems.

¹⁷ FIPS 201-3 Section 2.9.4, PIV Card Termination Requirements.

¹⁸ DOT Order 1681.2A(11)(d) & appendix C (f)(11).

they could not find any record of the contractor employee names or that PIV cards had been issued for 85 of these employees, reducing the number of cards we analyzed to 1,184. While most of the contractor employee PIV cards associated with the contracts in our sample did not have collection or deactivation issues, we found DOT officials did not promptly collect and deactivate a significant number of these cards once they were no longer needed. DOT officials did not collect and/or deactivate 294 of these cards. See table 3 for the summary results of our PIV card collection and deactivation analysis.

Table 3: OIG’s Analysis of DOT’s PIV Card Collection and Deactivation for the 64 Sample Contracts

OA	No. of DOT-Identified Contractor Employees With PIV Cards	No PIV Card Record	No Collection/Deactivation Issues	Untimely Collection/Deactivation	Deactivated but Not Collected	Collected but Not Deactivated	Not Collected or Deactivated
FHWA	571	21	353	44	151	0	2
FMCSA	27	5	13	2	7	0	0
FRA	12	0	9	3	0	0	0
FTA	61	2	41	9	9	0	0
NHTSA	68	0	61	7	0	0	0
OST	459	54	284	11	110	0	0
PHMSA	71	3	52	1	14	1	0
Totals	1,269	85	813	77	291	1	2

Source: OIG analysis

Details of our analysis of the contractor employee PIV cards associated with the 64 sample contracts are as follows:

- **No PIV card record.** At the onset of our review, we asked for the names of all contractor employees who were issued PIV cards under the 64 sample contracts. This resulted in a list of 1,269 contractor employees. However, when we asked for the PIV card collection and deactivation

details, DOT officials reported the Department's security database¹⁹ had no record of the names or any PIV card issuance for 85 of the 1,269 contractor employees they had originally identified. DOT officials were unable to explain these reporting discrepancies.

- **No collection and deactivation issues.** We did not identify any collection or deactivation issues for 813 of the 1,184 contractor employee PIV cards we analyzed. This includes 156 cards that were appropriately collected and deactivated when no longer needed, as well as 657 cards that remained active although the contracts' performance periods had ended. In the latter case, the contractor employees were transferred to new DOT contracts that required them to retain their PIV cards. Overall, we did not find any issues with the contractor employee PIV cards associated with 10 of the 64 sample contracts totaling \$54 million. These 10 contracts ended between fiscal years 2020 and 2022 and represent 5 OAs.
- **Untimely collection and deactivation.** Another critical method to mitigate security risks to Government facilities, systems, and employees is to carry out PIV card collection and deactivation in a timely manner. However, we determined that DOT officials did not collect 77 contractor employee PIV cards until anywhere from 1 to 646 days after the cards were no longer needed—an average of 131 days and a median of 83 days. Further, in 56 instances, DOT officials took anywhere from 1 to 598 days to deactivate the cards—an average of 133 days and a median of 60 days. For example, a contractor employee worked under a \$4.2 million contract to provide support for Federal Transit Administration (FTA) safety and grant oversight programs. This contract ended in April 2021. However, DOT officials did not collect or deactivate the contractor employee's PIV card until February 2022—325 days after the contract ended.
- **Deactivated but not collected.** Neglecting to physically collect a PIV card, even when it is deactivated, creates a serious security risk. An individual could continue to use that card as valid Government identification for things like gaining unwarranted access to Federal facilities and obtaining benefits intended for active Federal Government employees. Yet DOT officials did not collect 291 of the 1,184 contractor employee PIV cards we analyzed, although they were deactivated. These 291 PIV cards represent a total of 46 sample contracts valued at

¹⁹ MyID is a software system DOT and other Federal agencies use to issue and manage secure digital identities, such as PIV cards. This system records PIV issuance dates and deactivation status. At DOT, this system is only accessible by the Office of Security and Trusted Agents.

\$388 million that ended between fiscal years 2018 and 2022 and represent 4 OAs and OST. Moreover, although all 291 cards were deactivated, in 48 instances, the deactivations did not occur for anywhere from 1 to 902 days after they were no longer needed. For example, DOT officials did not collect the PIV cards for 56 contractor employees providing program and organizational support for the Department's IT infrastructure under a \$20.5 million FHWA contract that ended in June 2021. Moreover, the deactivations for those 56 cards occurred between 16 and 481 days after they were no longer needed.

- **Collected but not deactivated.** A PIV card that is collected but not deactivated can still be used to access secure and sensitive Government systems and facilities. There is a risk that the collected card will be misplaced or stolen and then used for malicious or adverse purposes. Nevertheless, DOT officials collected but did not deactivate one contractor PIV card associated with a \$438,218 PHMSA contract for administrative support services that ended in September 2020. According to a PHMSA official, the PIV card was hand-carried to the Office of Security for deactivation. However, Office of Security officials stated they have no record that this card was turned in and, therefore, did not deactivate it. Further, 21 days elapsed from the time the COR received the PIV card from the contract employee to when the PHMSA official reported taking the card to the Office of Security for deactivation.
- **Not collected or deactivated.** Collecting and deactivating PIV cards that are no longer needed protects the security of Government systems, facilities, and employees from malicious, fraudulent, or otherwise harmful acts. Such actions also revoke an official form of Government identification and its associated benefits. Nevertheless, DOT officials did not collect or deactivate the PIV cards for two contractor employees—one working under a \$20.5 million FHWA contract for organizational support services that ended in June 2020 and another working under a \$31 million FHWA contract providing operational and engineering support services that ended in September 2021.²⁰

Several factors have contributed to DOT's contractor employee PIV card collection and deactivation issues. Primarily, DOT has not established clear accountability over its contractor employee PIV card collection and deactivation process. The PIV Card Program Order assigns the Office of Security overarching accountability for managing PIV card issuance policy, procedure, and standards. However, the Order does not establish overarching accountability for collection

²⁰ In October 2022, during this audit, we notified Office of Security personnel about these two instances, and they immediately deactivated both PIV cards.

and deactivation. As such, DOT's contractor employee PIV card collection and deactivation process is fragmented and lacks clear accountability. Specifically:

- **Regarding collection:** DOT's PIV Card Program Order states the COR shall "promptly collect" PIV cards that are no longer needed and immediately forwarding them to a Trusted Agent or the Office of Security. Presumably, this action is intended to lead to the deactivation of the cards, as a COR does not have authority to do so. However, another section of the Order states the "DOT components" (i.e., the OAs and OST), non-specific to any individual, have the responsibility for doing this. Yet another section of the Order gives the contractor the responsibility to "promptly return" its employees' PIV cards to a COR and also allows contractor employees to mail their cards directly to the Office of Security. Additionally, the Order does not define "promptly," leaving the term subject to individual interpretation. Further, despite providing various options for collecting and returning contractor employee PIV cards, the Order does not require DOT officials to document when this occurs.

As a result, the OAs and OST lack clear accountability over the collection process. This is exemplified by the fact that in response to a questionnaire we sent to the 33 CORs²¹ associated with our sample contracts, 17 stated they are not responsible for collecting contractor employee PIV cards. Several others stated that non-COR staff within their OAs or in OST, such as Security Coordinators, help collect the cards.

- **Regarding deactivation:** The Order only addresses the deactivation process for lost, stolen, or compromised contractor employee PIV cards. While both Trusted Agents and Office of Security personnel can deactivate cards, the Order does not establish clear accountability to ensure this process takes place in a timely manner.

In addition, Office of Security personnel or Trusted Agents can deactivate a contractor employee PIV card only when one of the following occurs: (1) an OA or OST official collects and forwards a card to them; (2) an OA or OST official explicitly notifies them that a card is no longer needed; or (3) a contractor returns a card to them. However, no Department or OA-specific entity or person is accountable for overseeing all collection and deactivation actions or for establishing a standard documentation requirement for these intertwined processes.

Due to this fragmented approach, there is an increased likelihood that the collection and deactivation of DOT's contractor employee PIV cards will be

²¹ There were only 33 unique CORs associated with our 64 sample contracts because some CORs were assigned to multiple contracts.

untimely, inefficient, or overlooked, increasing the Department's vulnerability to security risks. This is particularly concerning given that the OAs and OST do not have a reliable method for tracking contractor employees and their PIV cards.²² We asked the 33 CORs associated with the 64 sample contracts how they track contractor employees' PIV cards so they know when to collect them. Twenty CORs stated they did not have an established process and lacked a complete inventory of their current contractor employees. The other 13 CORs stated they use things like spreadsheets or communicated regularly with the project managers to monitor the status of contractor employee PIV cards. Moreover, OST officials were unable to provide us with the total number of DOT contractor employees by fiscal year. Without an adequate method to track contractor employees and their PIV cards, DOT lacks the ability to promptly collect and deactivate the cards when they are no longer needed.

Some OAs are taking steps to address this deficiency. For example, FTA is updating its Operations and Staff Information System (OASIS), which will now document when a contractor employee is issued a PIV card and when that card expires. However, OASIS still does not record the collection date. FTA is also updating its PIV card collection guidance, which includes a form both the COR and contractor employee must sign to certify that the PIV card was returned. FHWA told us it is developing a database solution—which it intends to roll out in 2023—to help CORs and Trusted Agents track when PIV cards are assigned to a contract employee, turned in, and deactivated. FHWA officials also told us they will institute mandatory training to help educate CORs and Trusted Agents about their responsibilities for maintaining accountability of PIV cards from issuance to collection/deactivation and instruct CORs to regularly and promptly update PIV card assignment, collection, and deactivation information. Federal Motor Carrier Safety Administration (FMCSA) officials stated they provided training on the process for returning PIV cards to all CORs. National Highway Traffic Safety Administration (NHTSA) officials told us they are in the process of purchasing an automated contractor onboarding and offboarding system that will prompt CORs to collect contractors' PIV cards.

Finally, as discussed in the previous section, DOT's omission of PIV card-related security clause(s) in applicable contracts may also have contributed to the collection and deactivation issues. These clauses require the contractor to return employee PIV cards as soon as they are no longer needed.

When contractor employee PIV cards are not promptly collected and deactivated, DOT is exposed to heightened security risks, potentially compromising the safety of its staff and achievement of its mission. As noted at the beginning of this report, this risk is not theoretical: On September 26, 2014, a DOT contractor

²² See the section titled "No PIV Card Record" earlier in this report.

employee used his PIV card to enter an Air Route Traffic Control Center in Illinois and deliberately start a fire. In the process, he destroyed critical FAA telecommunications infrastructure equipment and delayed or canceled thousands of flights going into and out of Chicago O'Hare and Midway airports for more than 2 weeks. This contractor employee's last scheduled shift at the Illinois control center facility had been 8 days earlier, and he was not scheduled to start his new assignment at a different FAA facility in Hawaii until October 1, 2014. However, during this 12-day lapse between assignments, DOT did not collect or deactivate his PIV card or remove his access to the Illinois facility. The incident cost the public over \$350 million and threatened the safety and security of not only employees at the Center but the entire U.S. airspace.

Timely collection and deactivation of contractor employee PIV cards is vital to protecting the Department's mission critical systems and facilities. It also will help prevent incidents like this with costly and nationwide impact from occurring in the future.

Conclusion

Like all Federal agencies, DOT has established the PIV card as the fundamental tool for securely giving its contractor (and Federal) employees access to the Department's secure and sensitive resources, including its facilities and information systems. However, until DOT establishes explicit processes and clear accountability for the timely collection and deactivation of contractor employee PIV cards, it will continue to face the risk that its facilities and systems could be penetrated and manipulated by unauthorized personnel. Addressing this vulnerability will help enhance the Department's security and operational efficiency. This is particularly important given the magnitude of contractor support DOT relies on to carry out its mission-critical operations to help ensure the safety of the traveling public.

Recommendations

To improve DOT's collection and deactivation of contractor employee Personal Identity Verification (PIV) cards, we recommend that the Assistant Secretary for Administration coordinate with the Office of Security and Heads of each Operating Administration (OA) to:

1. Verify that each OA has a documented process in place to confirm that required PIV card-related security clauses are included in all applicable DOT contracts prior to award.

2. Establish, document, and implement a process for the Department to track contractor employees' PIV cards and record the dates the cards are collected and deactivated.
3. Designate in writing points of accountability for overseeing the entirety of contractor employee PIV card collection and deactivation processes.
4. Update or supplement the DOT PIV Card Program Order to define "promptly" in all uses throughout the Order.
5. Develop and implement required annual training for all staff involved in contractor employee PIV card processes and a procedure to verify the training has occurred. The training attendees should include all staff listed in the DOT PIV Card Program Order who could potentially be involved and anyone else an individual OA assigns to this task.
6. Update or supplement the DOT PIV Card Program Order to address the deactivation process in all instances where PIV cards are no longer needed. This should include establishing the accountable officials as well as concrete metrics when deactivation should occur from when the card is no longer needed.

Agency Comments and OIG Response

We provided DOT with our draft report on March 31, 2023, and received its formal response on May 15, 2023. That response, which is dated May 12, 2023, is included in its entirety as an appendix to this report. DOT concurred with recommendations 1 through 6 as written, and provided appropriate actions and completion dates. Accordingly, we consider all recommendations resolved but open pending completion of the planned actions.

Actions Required

We consider recommendations 1 through 6 resolved but open pending completion of DOT's planned actions.

Exhibit A. Scope and Methodology

This performance audit was conducted between November 2021 and March 2023. We conducted this audit in accordance with generally accepted Government auditing standards. 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 objectives.

The objective of this self-initiated audit was to assess DOT's oversight of contractor employee PIV cards issued in connection with performance of agency contracts. Given FAA's unique procurement requirements and the scope of its facilities and systems, we excluded it from this audit.

To address our objective, we developed a universe by pulling all DOT (non-FAA) contracts reported in the FPDS as of September 2, 2021, with a total value over \$250,000 and a period of performance end date in fiscal year 2020 or 2021. We then removed any contracts that were not service-related and would likely not involve contractor employees with PIV cards.²³ This resulted in a universe of 1,001 contracts valued at \$1,461,319,805.

From this universe, we selected a probability proportional to size statistical sample where the size variable is the total contract value. After validating with DOT officials that each of our sample contracts involved contractor employees with PIV cards, our final sample included 64 DOT contracts with a total value of \$542,064,342. We used the results of our validated sample to update the entire universe. As a result, we estimated the audit universe represented 518 contracts and orders²⁴ valued at \$890,492,722. As such, the value of our 64 sample contracts represents approximately 61 percent of the estimated total universe value.

Our 64 sample DOT contracts included 5 direct contracts and 59 orders associated with OST and 6 OAs including FHWA, FTA, FMCSA, FRA, NHTSA, and PHMSA. While the FPDS data reported that all 64 contracts ended in fiscal year 2020 or 2021, we determined during our audit work that 2 were extended to March 24, 2023, and May 31, 2023, respectively. According to DOT officials, these 64 sample contracts involved approximately 1,200 contractor employees with PIV cards.

²³ Examples of contracts we removed included those for construction, bridge inspection, and canal maintenance.

²⁴ The 518 contract estimate has a 90-percent confidence interval of 440 to 595. The \$890 million estimate has a 90-percent confidence interval of \$765 million to \$1,016 million.

Our audit field work included reviewing Federal, departmental, and Agency procurement policies, including the FAR, TAR, TAM, FAA's AMS, and other relevant Federal and DOT guidance and standards related to PIV cards. We obtained and analyzed contract award documents—including the applicable base contract if the sample was an order—to determine if they included the required security clauses. We also obtained the PIV card history for each contractor employee associated with our sample contracts and analyzed the cards' collection and deactivation dates versus the contracts' periods of performance. Further, we followed up with the 33 CORs associated with our sample by sending them a standard questionnaire to learn more about their roles and responsibilities in the PIV card process. We also interviewed various DOT officials involved in different aspects of PIV card processes, including members of the Office of Security, as well as Security Coordinators and Trusted Agents from OST and the six OAs represented in our sample.

In addition to working with DOT officials to validate that the sample contracts involved contractor employee PIV cards, we also validated the accuracy and completeness of the audit universe. To accomplish this, we compared the FPDS and DOT-provided data for our sample contracts to the actual contract documentation collected during our field work. We did not have a database or systems we could use to independently validate the list of contractor employees with PIV cards provided by DOT officials. However, we were able to reasonably validate this list through our data requests and by following up throughout the field work. In this way, we determined the universe and sample data were sufficient for the purpose of this audit.

Exhibit B. Organizations Visited or Contacted

Department of Transportation

Office of the Secretary of Transportation

Federal Highway Administration

Federal Motor Carrier Safety Administration

Federal Railroad Administration

Federal Transit Administration

National Highway Traffic Safety Administration

Pipeline and Hazardous Materials Safety Administration

Exhibit C. List of Acronyms

AMS	Acquisition Management System
CO	Contracting Officer
COR	Contracting Officer Representative
DOT	Department of Transportation
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FMCSA	Federal Motor Carrier Safety Administration
FPDS	Federal Procurement Data System
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HSPD	Homeland Security Presidential Directive
IT	Information Technology
NHTSA	National Highway Traffic Safety Administration
OA	Operating Administrations
OASIS	Operations and Staff Information System
OIG	Office of Inspector General
OST	Office of the Secretary of Transportation
PHMSA	Pipeline and Hazardous Materials Safety Administration
PIV	Personal Identity Verification
TAR	Transportation Acquisition Regulation

Exhibit D. Details of the 64 Sample Contracts

OA	Total Contracts	Direct Contract vs. Order	Total Value	Completed Period of Performance	Active Period of Performance	No. of Contractor Employees Identified With PIV Cards
FHWA ^a	24	0 Direct Contracts	\$166,225,247	23	1 ^b	571
		24 Orders				
FMCSA	6	0 Direct Contracts	\$141,319,923	6	0	27
		6 Orders				
FRA	2	0 Direct Contracts	\$5,131,127	2	0	12
		2 Orders				
FTA	10	3 Direct Contracts	\$29,163,456	10	0	61
		7 Orders				
NHTSA	4	0 Direct Contracts	\$29,684,993	3	1 ^c	68
		4 Orders				
OST	12	2 Direct Contracts	\$107,658,958	12	0	459
		10 Orders				
PHMSA	6	0 Direct Contracts	\$27,815,565	6	0	71
		6 Orders				
Totals	64		\$506,999,269	62	2	1,269

^a Of the 24 FHWA contracts, 4 were awarded by OST before they were transferred to FHWA to manage.

^b FPDS reported the contract's end date was March 24, 2021, but it was extended to March 24, 2023.

^c FPDS reported the contract's end date was May 31, 2020, but it was extended to May 31, 2023.

Source: OIG analysis

Exhibit E. Major Contributors to This Report

JILL COTTONARO	PROGRAM DIRECTOR
ANGELA SAVINI	PROJECT MANAGER
CURTIS DOW	SENIOR ANALYST
JONATHON NUCKLES	SENIOR ANALYST
ANDREA PARRA-DELEON	STUDENT TRAINEE ANALYST
AMY BERKS	DEPUTY CHIEF COUNSEL
JANE LUSAKA	SENIOR WRITER-EDITOR
MORGAN ATHERTON	WRITER-EDITOR (STUDENT TRAINEE)
GEORGE ZIPF	SUPERVISORY MATHEMATICAL STATISTICIAN
WILLIAM SAVAGE	IT SPECIALIST

Appendix. Agency Comments



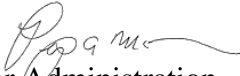
**U.S. Department of
Transportation**

Office of the Secretary
of Transportation

Memorandum

Subject: OIG Draft Report, Fragmented Processes Weaken DOT's
Accountability for Contactor Employee PIV Cards

Date: May 12, 2023

From: Philip A. McNamara 
Assistant Secretary for Administration

To: Carolyn J. Hicks
Assistant Inspector General for Acquisition and
Procurement Audits

The Department of Transportation (DOT or the Department) is committed to the security of its Federal workforce. Through the implementation of the 2016 DOT Homeland Security Presidential Directive 12 and Personal Identity Verification (PIV) Program, the Department ensures the safety of its people, facilities, and systems. To further enhance the efficiency of the PIV Program for Federal contractors, the Department's Office of Security and Office of the Senior Procurement Executive has actions underway to mitigate vulnerabilities addressing the timely collection and deactivation of contractor employee PIV cards across operating administrations, including updating guidance, training materials, and the establishment of a DOT-wide working group.

The OIG refers to the 2014 Chicago Center fire involving an FAA contractor who was being transferred to another facility. DOT conducted a security review and modified its policies and procedures to prevent similar incidents. DOT continues to assess its security posture.

Based on our review of the draft report, the Department concurs with the six recommendations as written. We plan to complete actions to implement recommendation 1 by December 31, 2023, recommendations 2 and 5 by April 30, 2024, recommendation 3 by May 31, 2024, and recommendations 4 and 6 by December 31, 2024.

We appreciate the opportunity to review the OIG draft report. Please contact Gary Middleton, Director of Audit Relations and Program Improvement, at gary.middleton@dot.gov or 202-366-6512 with any questions.

U.S. Department of Transportation
Office of Inspector General

Fraud & Safety Hotline

<https://www.oig.dot.gov/hotline>
hotline@oig.dot.gov
(800) 424-9071

OUR MISSION

OIG enhances DOT's programs and operations by conducting objective investigations and audits on behalf of the American public.



1200 New Jersey Ave SE
Washington, DC 20590
www.oig.dot.gov