VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Mismanagement of the Personal Identity Verification Processes

June 5, 2017
15-04365-328

ACRONYMS

OIG	Office of Inspector General
OPM	Office of Personnel Management
PIV	Personal Identity Verification
SAC	Special Agreement Check
SIC	Security and Investigations Center
VA	Department of Veterans Affairs

To report suspected wrongdoing in VA programs and operations, contact the VA OIG Hotline:

Website: www.va.gov/oig/hotline

Email: vaoighotline@va.gov

Telephone: 1-800-488-8244

Highlights: Review of Alleged Mismanagement of VA's PIV Processes

Why We Did This Review

The Office of Inspector General (OIG) conducted this review to determine the merits of allegations involving the mismanagement of the Personal Identity Verification (PIV) Program and related systems. In June 2015, we received a Hotline complaint alleging that VA's Security and Investigations Center (SIC) was inappropriately permitting the issuance of PIV cards and VA network system access to individuals who did not have completed background investigations or adjudicated fingerprinting. SIC personnel process and adjudicate the background investigations for all moderate- and high-risk public trust and national security positions for Federal employees within VA. They also process all levels of investigation for contractors performing jobs and functions for VA.

What We Found

We determined that SIC personnel appropriately authorized the issuance of PIV cards in accordance with VA policies and procedures. More specifically, we did not find any instances where VA's SIC was inappropriately authorizing the issuance of PIV cards and allowing VA network system access to individuals who did not have completed a Special Agreement Check (SAC) and a scheduled background investigation as required by VA policy. We reviewed VA local policies and procedures as they related to PIV card authorizations. To evaluate business processes and compliance with VA policies, we judgmentally selected 32 cases to sample from VA's Security Manager system of record. The 32 cases included 25 individuals chosen randomly, six personnel who were SIC management, and one individual who was named in the complaint as having received a PIV card without meeting VA policy requirements. We observed SIC personnel accessing each of these cases in the system of record and reviewing the electronic records, SAC, background investigation dates, and any relevant comments associated with each case. We found that each case we reviewed met VA policy requirements for PIV card authorization. As a result, we concluded that SIC personnel appropriately authorized the issuance of PIV cards in accordance with VA policy.

What We Recommended

We did not substantiate the allegations of SIC's mismanagement of the PIV Program and related systems. Additionally, we did not find any instances of improper processing of selected cases. Accordingly, we have no recommendations for improvement.

Agency Comments

Management concurred with our report and did not provide any comments.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

The Office of Inspector General (OIG) conducted this review to determine the merits of allegations concerning the Security and Investigations Center's (SIC) management of the Personal Identity Verification (PIV) program and related systems. The SIC is located in North Little Rock, AR.

Allegation and Background

In June 2015, the OIG received a Hotline complaint alleging that the SIC was inappropriately authorizing the issuance of PIV cards and allowing VA system access for individuals who did not have completed background investigations or adjudicated fingerprinting. PIV cards, issued by VA Human Resources to employees and contractors, enable access to VA computer resources and information technology.

The SIC has 41[1] full-time employees located in North Little Rock, AR. Human Resources personnel rely on the SIC to identify applicant security risks before issuing PIV cards. SIC personnel process and adjudicate background investigations for all VA employees in moderate- and high-risk public trust positions and investigations for all contractors. SIC personnel identify security risks through investigation and adjudication processes so it can advise customers on the proper course of action regarding position suitability when considering individuals for VA employment and network access. Services include preliminary reviews, investigations performed in partnership with the Office of Personnel Management (OPM), and final security clearance and suitability determinations. Ultimately, Human Resources personnel will verify the applicant's background investigation status using the Office of Personnel Management's Personnel Investigations Processing System.

Prior to obtaining PIV credentials, applicants must have a Special Agreement Check (SAC) with fingerprinting completed. Applicants must have an investigation on file or scheduled that meets Federal background investigation and reciprocity requirements. If no investigation is on file, applicants must complete background investigation forms prior to issuance of PIV credentials.

[1] This number was derived from the organization chart received from the SIC Director on May 12, 2017.

RESULTS AND RECOMMENDATIONS

Finding Security and Investigations Center Followed Federal and VA PIV Authorization Processes

We did not substantiate the allegations of the SIC's mismanagement of the PIV Program and related systems. In addition, within our sample of transactions, we did not find any instances where VA's SIC was inappropriately authorizing the issuance of PIV cards and VA network system access to individuals who did not have completed a SAC or scheduled background investigation. As a result, we concluded that there is reasonable assurance that SIC business processes were performed in accordance with VA policy from January through June 2015. Accordingly, we have no recommendations for improvement.

What We Did

In November 2015, we performed an onsite review of the SIC in North Little Rock, AR. To evaluate the PIV Program and authorization processes, we used VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, that establishes minimum criteria for employees, contractors, and affiliates to be issued a PIV card. The handbook states that before gaining system access, applicants must have completed a SAC and have scheduled a National Agency Check or higher-level background investigation with OPM.

We interviewed the deputy director of the SIC as well as supervisors, security assistants, and an IT specialist. We observed the SIC staff demonstrating how they perform the PIV card authorization process. We reviewed VA local policy and procedures related to the PIV card authorization process. To evaluate supporting business processes, we obtained a listing from SIC management of more than 8,100 background investigation cases from January through June 2015. From this listing, we judgmentally selected 32 cases to sample. The 32 cases included 25 individuals selected randomly from a letter of the alphabet, six personnel who were SIC management, and one individual who was named in the complaint as having received a PIV card without meeting VA policy requirements. The cases were reviewed to determine whether a SAC was completed and a background investigation was scheduled or completed. We found that each case we reviewed met VA policy requirements for PIV card authorization.

Each case reviewed included an individual's application to obtain a PIV card to authenticate the person's identity on the network and access VA's network resources. As the team did not have access to the system, we observed SIC personnel accessing each of these cases in the VA Security Manager system of record and we reviewed electronic records, SAC and background investigation dates, and any relevant comments associated with each case. We also interviewed a Human Resources specialist and had him explain and demonstrate how they issue PIV cards. We reviewed relevant VA policies and procedures, SIC's system of record, and sample cases. We also observed SIC users processing electronic cases. In addition, we conducted interviews with management, system users, and IT staff located at the SIC in North Little Rock, AR.

What We Found

We determined that SIC personnel were appropriately authorizing the issuance of PIV cards in accordance with VA policy and procedures. For the 32 selected cases tested, the system of record showed that each applicant had completed a SAC and had a scheduled or completed National Agency Check or higher-level background investigation with OPM. From our sample, we noted that one applicant had received a PIV card after completing the application process but the OPM background investigation was scheduled but not completed. In accordance with VA policy, an applicant may receive a PIV card after completing a SAC and initiating a background investigation with OPM. Consequently, we did not find any cases where PIV cards were inappropriately issued prior to the completion of the application steps defined above.

We observed SIC personnel accessing selected cases in VA's Security Manager system of record and reviewing electronic documentation. Applicants must complete background investigation forms online at OPM's Electronic Questionnaire for Investigations Processing prior to obtaining PIV credentials. VA Human Resources personnel verify the applicant's SAC and background investigation status using the OPM's Personnel Investigations Processing System and issues the PIV card. Human Resources staff rely on the SIC to identify applicant security risks before issuing PIV cards to VA employees and contractors, which enable access to VA facilities and information technology. Accordingly, we have no recommendations for improvement.

Appendix A Scope and Methodology

Scope

We conducted our review work from October 2015 through April 2017. The scope of our review included determining applicable criteria and obtaining sufficient and credible evidence in order to address the allegations.

Methodology

In November 2015, we performed an onsite review of the SIC in North Little Rock, AR. To evaluate the PIV Program and authorization processes, we used VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, that establishes minimum criteria for employees, contractors, and affiliates to be issued a PIV card. We interviewed the deputy director of the SIC as well as supervisors, security assistants, and an IT specialist. We observed the SIC staff demonstrating how they perform the PIV card authorization process. We reviewed VA local policy and procedures related to the PIV card authorization process.

Data Reliability

To evaluate supporting business processes, we obtained a listing from SIC management of more than 8,100 background investigation cases from January through June 2015. The data were retrieved from VA's Security Management system of record and were used to create a sample of cases to review the PIV authorization process. The data within the Security Manager system are entered and maintained by SIC personnel. This system is used to manage the suitability decisions and security clearance determinations for employees, contractors, and detailees. We did not establish the completeness of these data because we did not have access to the data independently from the SIC staff. Therefore, we could not provide assurance that the data were complete for the period of our review. To assess the accuracy of the data from the Security Manager system, we observed SIC personnel retrieve each selected case and review the electronic cases so we could verify that SAC and background investigation dates were entered into the system. We compared the data on the selected cases with the system of record data and concluded that the data were sufficiently accurate to achieve our review objectives. Therefore, we believe the conclusion in this report is valid.

Government Standards

We performed limited testing that provided support for the conclusions in this report. We complied with the Council of Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* to the extent possible.

Appendix B OIG Contact and Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Jack Henserling George Ibarra Ryan Nelson

Appendix C Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans Appeals
Franchise Fund Board of Directors
VA Security and Investigations Center

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report is available on our website at www.va.gov/oig.