Federal Election Commission
Office *of the* Inspector General

INVESTIGATIVE SUMMARY I21INV00063 DATE: NOVEMBER 23, 2021

HSPD-12 Personal Identity Verification (PIV) Card Incident

The Federal Election Commission (FEC) Office of Inspector General (OIG) initiated an investigation on June 3, 2021, at the request of the Office of the Staff Director concerning an incident on June 1, 2021 that involved a potential information systems breach associated with agency-provided employee identification cards. Specifically, an FEC employee logged into the agency's performance management system with a Personal Identity Verification (PIV) card and discovered they were logged into the system under the credentials of another FEC employee. After the employee reported the incident, the FEC Staff Director, who also serves as the agency's Chief Information Officer, promptly convened the FEC Breach Notification and Response Team and requested an OIG investigation to respond to the incident.

By way of background, the FEC contracts with an outside vendor to provide support services for issuing PIV cards onsite at the FEC office located in Washington, D.C. Due to office closures related to the COVID-19 pandemic, the FEC held discussions with the vendor and ultimately decided for the vendor to issue the PIV cards offsite at its location in Fairfax, Virginia. The FEC directed current employees with expiring PIV cards and new employees who needed new cards to obtain them in Fairfax or to work with the Office of Chief Information Officer (OCIO) for a workaround to access the agency's network.

The OIG investigation sought answers to the following questions:

- **What were the proximate and root causes of the PIV card incident?**
- **What, if any, steps could the FEC and/or the vendor have taken to prevent this incident?**
- **Did the PIV card incident result in a Privacy Act violation or other unauthorized disclosure of sensitive information?**

In order to answer the foregoing questions, the OIG reviewed relevant guidance and policies, and interviewed FEC staff from the Office of Chief Financial Officer, the OCIO, the Office of Management and Administration, and the Office of the Staff Director, as well as the vendor's representatives. The OIG issued a Report of Investigation to the Commission on November 12, 2021 that detailed the following findings.

First, the OIG found that the June 1, 2021 incident resulted from the vendor's assignment of a constant number (rather than a unique number) to an identifier after a workflow change. Specifically, in accordance with the executed contract, the vendor provides a support service to

the FEC by conducting periodic updates to the vendor software, which is used to issue PIV cards. According to testimony by the vendor's personnel, during testing in the latter part of 2017, the vendor became aware of a workflow change that was not going to be included in future releases by the software company that provides PIV card support software.

As a result, the vendor modified a part of the workflow to allow the registrar to add the applicant's information during PIV card registration. In addition, the modified workflow did not assign a unique number to the identifier; instead, it assigned a constant number because the vendor was unaware the FEC was using that particular identifier. Similarly, the OCIO staff was not aware of the workflow change made by the vendor.

The OIG inquired into whether this incident may have resulted in a Privacy Act violation or other unauthorized disclosure of sensitive information. The preponderance of the evidence established that the incident was limited to a small number of employees within the FEC. In addition, the FEC OCIO took prompt action to address the issue upon discovery, including identifying and disabling affected PIV cards. As such, there was no apparent disclosure of personally identifiable information or other sensitive information.

Given the miscommunication between the vendor and the FEC OCIO regarding the coding of the identifier, and that the FEC became aware that the identifier used for the performance system authentication was not unique only after contacting the Office of Personnel Management (OPM), the OIG concluded the FEC did not have a process to verify with the PIV card issuer and third-party providers (e.g., OPM) that identifiers used for authentication are unique. Accordingly, the OIG recommends the following actions for the Commission to consider:

1. Review all current agency systems that require PIV card login and verify the fields that are used for authentication with third-party providers.

2. Verify with the PIV card issuer that all fields used for authentication in agency systems are unique after any upgrade to the software associated with issuing PIV cards.

3. Include the Chief Information Security Officer or other technically qualified IT personnel in the procurement process to determine how the third-party providers grant FEC employees' access to their systems and determine how these systems may affect FEC operations.

Second, the OIG found that the FEC did not memorialize a change in the contract for the vendor to use its personnel to offer PIV card services offsite. The Federal Acquisition Regulations (FAR) sets forth the rules regarding government procurement. FAR 43.000 prescribes policies and procedures for preparing and processing contract modifications. Specifically, 43.104 specifies when a notification is required to a modification in the contract so the government can evaluate the changes. The FAR also requires, under 43.301, that any contract modification or changes shall be documented in Standard Form 30.

The original contract provided that FEC personnel would issue PIV cards onsite at the FEC office. Subsequently, the FEC discussed alternative options with the vendor once the FEC issued an evacuation order and required mandatory telework due to the COVID-19 pandemic; however, the decision for the vendor to issue the PIV cards to FEC employees at its location in Fairfax was not formally memorialized in an amended contract or other record.

Additionally, based on the testimony of procurement personnel, the FEC did not memorialize a modification because the procurement office believed the change in service did not require a contract modification. As such, the FEC did not draft a modification for the service because agency contracting personnel believed the service was within the scope of the original contract and the vendor was offering it at no additional cost.

Memorializing the changes may have caused the FEC to identity additional impacts and risks of allowing the vendor to offer this service offsite. Additionally, the absence of a written modification could present future risks to the agency in the event of a dispute with the contractor. Accordingly, the OIG further recommends the Commission:

4. Ensure there is a formal process to memorialize the actions taken by the FEC or its contractors when there is a change from the statement of work.

5. Evaluate the services the contractor is currently providing for the PIV cards and issue a modification to the task order detailing the change in the worksite location.