OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-21-12 January 2021

PERSONNEL SECURITY CLEARANCES AND BADGE ACCESS CONTROLS FOR SEPARATED EMPLOYEES

Department of Energy
Washington, DC 20585

January 19, 2021

MEMORANDUM FOR THE SECRETARY

FROM: Teri L. Donaldson
Inspector General

SUBJECT: INFORMATION: Audit Report on "Personnel Security Clearances and Badge Access Controls for Separated Employees"

BACKGROUND

The Department of Energy uses security clearances and badges to control access to its sites and facilities. In 2004, the Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, directed Federal agencies to adopt a common identification standard for all employees and contractors. In an effort to comply with the mandate in HSPD-12, the Department provides its Federal and contractor employees with Personal Identity Verification (PIV) cards, which serve as access authorization badges. PIV cards indicate the level of access to classified matter or Special Nuclear Material for which the holder may be eligible, hereafter referred to as a "security clearance." PIV cards also allow employees to enter, occupy, or leave Departmental sites and facilities. Between October 2015 and May 2018, more than 10,000 Federal and contractor employees separated their employment association with the Department through retirement, resignation, removal, or death. This included over 2,000 individuals with security clearances.

The Office of Inspector General has issued several reports that identified weaknesses in the Department's controls over security clearance terminations and badge retrievals for separated employees. These reports found that unauthorized individuals could gain access to Department facilities due to problems with the Department's clearance and badging controls, such as not retrieving security badges from separated employees or removing security clearances of separated employees in a timely manner. Because establishing and maintaining adequate access controls is important, we initiated this audit to determine whether the Department terminated security clearance and PIV card access for separated employees in accordance with Federal regulations and Department policies.

RESULTS OF AUDIT

We found that the Department had not always terminated security clearance and PIV card access for separated Federal and contractor employees, as required. Federal regulations, Departmental orders, and other guidance documents establish several required control procedures that are

designed to prevent access to Department sites and facilities when Federal and contractor employees separate their association with the Department. These controls include updating the Department's PIV card database in USAccess[1] to reflect employee separations; recovering and destroying access PIV cards; and, where applicable, terminating separated employees' security clearances.

We analyzed records from USAccess for 5,803 separated employees.[2] We then performed validation test work on 2,703 separated Federal and contractor employees at Headquarters and Albuquerque, New Mexico and found the following:

- 39 percent of separated employees' PIV cards or employment statuses had not been updated in USAccess to reflect that the employee had separated and no longer required access to Department facilities and systems;

- 66 percent of separated employees' PIV cards not marked as "destroyed" in USAccess were not retrieved and manually destroyed per destruction records reviewed; and

- 30 percent of separated Federal and contractor employees' security clearances were not terminated in accordance with agency requirements.

Further, there were 4,326 additional separated Federal and contractor employees that we did not evaluate because their names did not match records in USAccess.

The problems identified with updating USAccess, destroying badges, and terminating security clearances for separated employees can be attributed to the fact that current requirements do not clearly delineate responsibility and accountability for access authorization termination actions. In addition, current directives do not require a formal security out-processing procedure or outline enforcement measures. According to a Headquarters security official, the current structure of the overall process is not producing the results needed to ensure that necessary safeguards are in place for the notification, retrieval, and destruction of PIV cards for separated employees. For example, the program offices are not meeting a requirement to terminate the Department's interest in an employee's security clearance and to complete the security termination form within 4 working days of separation. While some of the data issues identified can be attributed to the deficiency in assignment of responsibility and authority, program officials also indicated that the information contained in identity management systems lacks standardization, which negatively affects access eliminations and other Department operations involving personnel information.

If clearances and PIV cards are not properly terminated, recovered, and destroyed, former employees may gain unauthorized access to Department buildings or information. Given the

[1] USAccess is a U.S. General Services Administration-managed system that provides Federal agencies with identity management and credential solutions, including managing the lifecycle of Federal and contractor employees' access authorization badges or PIV cards.

[2] We received listings showing that 10,129 Federal and contractor employees separated between October 2015 and May 2018. See Appendix 1 for the scope, methodology, and sources of the data we used for our analysis.

important role the Department plays in the Nation's security posture, we made recommendations designed to improve the Department's controls for terminating a security clearance and PIV card access for separated employees.

MANAGEMENT RESPONSE

Management generally concurred with our recommendations and identified actions it would take to address them. Management's proposed actions are responsive to our recommendations. Management's comments are included in Appendix 4.

cc: Deputy Secretary
Chief of Staff

PERSONNEL SECURITY CLEARANCES AND BADGE ACCESS CONTROLS FOR SEPARATED EMPLOYEES

TABLE OF CONTENTS

Audit Report

Appendices

PERSONNEL SECURITY CLEARANCES AND BADGE ACCESS CONTROLS FOR SEPARATED EMPLOYEES

BACKGROUND

The Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, establishes the requirement for each Government agency to issue Personal Identity Verification (PIV) compliant credentials, also referred to as PIV cards, to its Federal and contractor employees. In response, the U.S. General Services Administration (GSA) offered USAccess as an efficient way for Federal agencies to issue PIV cards to their employees and contractors. PIV cards can be used to gain access to Federal facilities and information systems within an agency and across agency borders. In an effort to comply with the HSPD-12 requirement, the Department of Energy uses the PIV card as its access authorization badge. The PIV card indicates the level of access to classified matter or Special Nuclear Material for which the holder may be eligible, hereafter referred to as a "security clearance." The PIV card also allows Federal and contractor employees to enter, occupy, or leave Departmental sites and facilities. According to employee separations records[1] provided by the Department, 10,129 Federal and contractor employees separated their employment association with the Department between October 1, 2015, and May 30, 2018, including 2,241 individuals with security clearances. Because the Department manages some of our Nation's most valuable security assets, it is important that appropriate access controls are established and maintained, especially when such access is no longer required.

Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification of Federal Employees and Contractors* (FIPS PUB 201-2), contains the minimum requirements for a Federal PIV system that meets the control and security objectives of HSPD-12. Additionally, Department Order 472.2, change 1, *Personnel Security* (Department Order 472.2, change 1); Department Order 473.3A, *Protection Program Operations* (Department Order 473.3A); Department Order 206.2, *Identity, Credential, and Access Management* (Department Order 206.2); Headquarters Facility Master Security Plan (FMSP); and GSA's USAccess course include requirements with the expectation that controls would prevent access to Department sites and facilities when Federal and contractor employees separate. These controls consist of updating relevant databases to reflect employee separation; recovering and destroying PIV cards; and, when applicable, terminating the Department's interest in separated employees' security clearances. These actions are affected through interactions between several parties, including the separated employees, program offices, Security Officers, Contracting Officer's Representatives, and contractors. For example, when Federal and contractor employees separate at Headquarters, it is the responsibility of the designated program office to inform the Badge Office of the termination. The Badge Office collects and destroys PIV cards and annotates the action in its badging system; security officials are responsible for terminating separated employees' security clearances, if applicable; and program offices are expected to update separated employees' statuses in USAccess. The Department processes updates to PIV cards in USAccess, the Department's PIV card database, and all security clearance actions through its Central Personnel Clearance Index (CPCI) system.

[1] See Appendix 1 for scope, methodology, and sources of the data used for our analysis.

The Office of Inspector General has issued several reports that identified weaknesses in the Department's controls over security clearance terminations and badge retrievals for separated employees. These reports found that unauthorized individuals could gain access to Department facilities due to problems with the Department's clearance and badging controls, such as not retrieving security badges from separated employees or removing security clearances of separated employees in a timely manner.

DETAILS OF FINDINGS

Separated Employee Access Authorizations

Our review disclosed that opportunities exist to strengthen processes for ensuring necessary USAccess status updates are made upon employee separation, PIV cards are retrieved and destroyed, and security clearances are terminated in a timely manner. These issues are similar to the ones identified in our prior reviews. We analyzed records from USAccess for 5,803 Federal and contractor employees that separated between October 2015 and May 2018. We then performed validation test work on 2,703 separated Federal and contractor employees at Headquarters and Albuquerque, New Mexico, which included Sandia National Laboratories (SNL). The following table shows exceptions for not updating USAccess, not retrieving and destroying PIV cards, and not terminating security clearances at these two locations (Headquarters and Albuquerque):

Separated Employee Access Authorizations			
Validation Procedure	**Separated Employees Reviewed**	**Exceptions Observed**	**Percent**
USAccess Status Updates	2,703	1,059	39%
PIV Cards Retrieved and Destroyed	303	199	66%
Security Clearance Terminations	235	70	30%

Further, there were 4,326 additional separated Federal and contractor employees that we did not evaluate because their names did not match records in USAccess.

USAccess Status Updates

Our analysis found that the Department and contract officials did not update USAccess for 39 percent[2] of separated Federal and contractor employees that we reviewed. FIPS PUB 201-2 requires PIV card issuers to update their systems to reflect the change in status for separated employees. The GSA's USAccess training course delineated the following two steps for updating separated employees' statuses: (1) marking separated employees' employment statuses as "terminated" in USAccess, and (2) marking separated employees' cards as "destroyed" in USAccess.

[2] See Table 1 in Appendix 2 for details on the results of our analysis at the two locations where validation procedures were performed.

However, we found that Headquarters did not mark employment statuses as "terminated" or mark PIV cards as "destroyed" in USAccess for nearly half of the separated Federal and contractor employees for which it was responsible. Although we found better results at Albuquerque, including SNL, the exception rate was still high at around 20 percent. We noticed that several Headquarters Federal and contractor employees remained active in USAccess for months and even years after separation. For example, one employee that separated in November 2015 remained active in USAccess when we reviewed the database in July 2018, over 2 years later. Further, some of these employees were identified as having been removed from their jobs and others were deceased. Subsequent to our audit work, SNL officials indicated that all individuals whose employment statuses were not updated in USAccess had since been updated.

Although we did not perform additional validation procedures, such as verifying that separated employees whose statuses were not updated in USAccess were still actively employed, we noted a similar exception rate in the 5,803 records in USAccess that we analyzed. Overall, we found that records for approximately 44 percent of the separated Federal and contractor employees in the period of review potentially had not been updated in USAccess. These exceptions show that the Department may not be terminating PIV access for separated employees, as required, thereby creating a situation where these individuals, who no longer need access to Department facilities and systems, could potentially gain access to Department resources.

Lapses in updating USAccess occurred because of several reasons. The Department had not designated a central control point responsible and accountable for ensuring that PIV card statuses are updated for separated employees. GSA's USAccess training course, for instance, indicates that the human capital offices of agencies that use the program are responsible for updating separated employees' statuses in USAccess; accordingly, within the Department, the Office of the Chief Human Capital Officer is the responsible party. However, according to Headquarters Security officials, the Department's program offices and sites are responsible for updating employment and badge destruction status in USAccess. Thus, there is no central control point responsible and accountable for ensuring that access authorization card statuses are terminated for separated employees. Although responsible for establishing expectations for the Department-wide personnel security program, the Office of Departmental Personnel Security is not responsible for oversight of the Department's security program.

Additionally, Human Capital and security officials stated that anyone that program offices designate as a "sponsor" in USAccess can make changes to any employee's record, not just employees assigned to that program office. For example, if the Office of Science assigns an individual the sponsor role in USAccess, that person can make changes to any program office's employee records across the complex. The unfettered access to employee records by anyone designated as a "sponsor" makes record accountability difficult, particularly when necessary updates are not made. Consequently, a "sponsor" cannot be specifically identified as being solely responsible for not updating USAccess upon employee separation.

Finally, at Headquarters, we found that problems with updating USAccess were compounded by a lack of interface between badging, personnel security, or human resource databases, and the fact that current procedures rely on passing paperwork between multiple offices. In contrast, we learned that SNL's internal system, the Sandia Total Access Request Tool, interfaces with its

badging and human resources systems and has read-only access to CPCI, thus limiting data entry errors. We believe that this approach contributed to the significantly lower exception rates at SNL with respect to updating separated employee information in USAccess.

PIV Card Retrieval and Destruction

Our analysis found that 66 percent[3] of the separated Federal and contractor employees whose PIV cards were not marked as "destroyed" in USAccess were not retrieved and physically destroyed, per destruction records reviewed. Department Order 473.3A requires the recovery of badges issued to employees, contractors, and other individuals before they leave the facility. Recovered security badges must be destroyed and the records annotated accordingly. Moreover, Department Order 473.3A requires that local procedures be developed to address these out-processing requirements. However, we found that a majority of the PIV cards not marked as "destroyed" in USAccess were not recovered and physically destroyed. As previously noted, many of the Headquarters employees who separated more than 12 months prior were still showing up as active in both USAccess and the local badging system, according to records provided by Headquarters security officials. For example, one employee that separated in November 2016 remained active in USAccess and the badging system when we reviewed the database in July 2018, almost 2 years later. This employee and several others potentially had access to the Department's systems and facilities until November 2020, when their PIV cards expired. Additionally, at Albuquerque, badges for two of the five separated employees we looked at had not been destroyed.

In contrast, for separated employees whose status in USAccess indicated that their badges were marked "destroyed," SNL officials had physical destruction records to support that these badges were destroyed. At SNL, an official explained that SNL's PIV card destructions are annotated in its badging application destruction log. SNL officials provided the dates that the employees' PIV cards were destroyed in SNL's system. We attributed the better outcomes at SNL for access termination to the fact that SNL's processes were more automated and had designated representatives to notify security officials of changes to contractor and employee access rights.

The exceptions with badge retrieval and destruction occurred, in part, because no Department directive required a formal out-processing procedure. While Department Order 473.3A and Headquarters FMSP prescribed access authorization controls for Federal and contractor employee security programs, they did not assign responsibility for out-processing actions, nor did they identify a process for accounting for PIV cards when employees separate. A Headquarters official explained that the Headquarters FMSP is just a guide and that each of the Department's program offices, sites, or contractors can develop its own out-processing procedure. Headquarters officials further asserted that the current structure of the overall process is not producing the results needed to ensure that the necessary safeguards are in place for the notification, retrieval, and destruction of PIV cards for separated employees. With regard to contractor separations, we also noted that Department directives did not reference Federal Acquisition Regulation 52.204-9, *Personal Identity Verification of Contractor Personnel*.

[3] See Table 2 in Appendix 2 for details on the results of our analysis at the two locations where validation procedures were performed.

This clause mandates that contractors return PIV cards or other similar badges to the agency upon completion of the contractor employee's employment when no longer needed for contract performance or upon contract completion.

Security Clearance Termination

Our review of separated Federal and contractor employees with security clearances showed that the Department did not terminate its interest in 30 percent[4] of the security clearances in accordance with agency requirements. Department Order 472.2, Change 1, describes a two-step process to administratively withdraw a security clearance. First, within 2 working days, the responsible program office or contractor is to provide written notice to their cognizant personnel security office that a separated employee no longer needs a security clearance. This written notice is either a completed Department Form 5631.29, *Security Termination*, signed by the separating employee acknowledging continuing responsibility to protect classified information and Special Nuclear Material, or if not immediately provided, an unsigned form along with a written explanation on why it was not signed. Second, the cognizant personnel security office has 2 working days to update the CPCI system with a terminated status for separated employees to show that the Department's interest in the security clearance has been terminated. However, our validation found that clearances were not always administratively withdrawn in a timely manner, or at all in some instances, when employees separated.

We reviewed whether security clearances were administratively withdrawn within 4 working days following employee separation and found that the 4-working-day timeframe was not met for 30 percent of the individuals in our sample. In fact, about 23 percent of the security clearances held by separated Headquarters Federal and contractor employees remained active for 90 days or more after their separation dates. Moreover, our review of the Office of Departmental Personnel Security's reconciliation reports revealed several instances where separated employees had active clearances in CPCI for many years after separation. Albuquerque and SNL fared much better meeting the 4-working-day timeframe for terminating separated employees' security clearances. Specifically, our analysis showed a 26 percent exception rate at Albuquerque and a 14 percent exception rate at SNL.

We attributed problems with terminating separated employees' security clearances in a timely manner to several factors. For starters, as noted in the Headquarters FMSP, no Department directive requires a formal security out-processing procedure nor identifies what office or person should be held accountable if the clearance termination action is not timely. According to Headquarters' officials, the Department's many program offices and sites are responsible for processing clearance termination actions, and as such, the process hinges on communication and the passing of paperwork between key players within the program offices. In fact, the Headquarters FMSP states that Security Officers must establish close working relationships with the human resource specialists within their elements, Contracting Officer's Representatives, and contractor project managers in order to be notified when any of their employees terminate or transfer to another element. For example, officials within the Office of Headquarters Personnel Security Operations pointed out that security officers would not know a security clearance

[4] See Table 3 in Appendix 2 for details on the results of our analysis at the two locations where validation procedures were performed.

termination is needed without written notification that an employee has separated. Officials also stated that to reduce paperwork, they sometimes held off terminating clearances for as long as 14 days when they knew the employees were transferring to a contractor, a practice that was not formalized in the order and is no longer followed. Although we were unable to verify this with our analysis, they claimed that their security officers processed 95 percent of the security clearance terminations that we reviewed within 2 working days of receiving written notification.

In contrast, Albuquerque and SNL had better delineated responsibility and accountability for termination actions. For example, there were policy documents and task instructions that identified the persons or offices responsible for completing the out-processing procedures. Additionally, SNL personnel and security systems were interfaced, allowing for automated updates to employee information once the paperwork was signed. Although Albuquerque and SNL did not always meet the 4-working-day requirement, almost all separated employees' security clearances were terminated within 90 days.

Employee Separations Data

There were 4,326 additional separated Federal and contractor employee names provided by the Department and SNL whose names did not match records in USAccess. We identified over 1,000 of these employees as having security clearances in CPCI, but we did not find their names in USAccess. Since they were not found in USAccess, we did not evaluate whether the Department and contractor officials updated employment statuses, recovered and destroyed badges, or terminated the Department's interest in their security clearances. There were a couple of possible reasons why we did not find these separated employees in USAccess. First, employee names may have been incorrectly entered into the systems used to generate the listings of separations provided to us. For example, we noted instances where middle names were inconsistently captured and aliases were used instead of legal names. Second, some employees noted as having security clearances in CPCI may not have been entered into USAccess because their employment was temporary or because they were given local badges rather than PIV cards. Temporary employees hired for 180 days or fewer may be considered an exception to the PIV card requirement. Also, contrary to the HSPD-12 requirement to issue PIV cards to all Federal and contractor employees with or without clearances and regardless of duty station, Department Order 473.3A does not mandate the issuance of PIV cards to uncleared contractor employees outside of Headquarters. At SNL, for example, we were only able to match 27 percent of its separated employees to records in USAccess. We learned that SNL issued local site badges instead of PIV cards to employees without security clearances, per a prior National Nuclear Security Administration (NNSA) policy letter. The NNSA's Supplemental Directive 206.2, *Implementation of Personal Identity Verification for Uncleared Contractors*, mandates the issuance of PIV cards to uncleared contractors who require physical or logical access to NNSA sites greater than 179 days. While the supplemental directive was issued in April 2018, NNSA clarified that it has not yet been fully implemented.

The data quality issues can be attributed to the lack of standardization of information contained in the Department's identity management systems. Specifically, Department Order 206.2 mandates, among other things, the development of an enterprise identity management system that links authoritative sources of identity information on the Department's Federal and

contractor employees and the issuance of a unique identifier for each employee. However, employee data is not linked between the Department's various systems, and not all systems include a unique identifier for each employee. An official with the Office of the Chief Information Officer noted that some identity management systems linked to the Department's Enterprise Identity Management Service System do not include unique identifiers for employees. The problem with identifying employees in the various systems was also observed in the Office of Department Personnel Security's monthly reconciliation reports. These reports identified numerous mismatches between the employee information system and the clearance database, CPCI. For example, the January and February 2018 reports showed that over 50 percent of individuals possessing clearances did not match information in the Department's employee system.

Potential for Harm to National Security Interests

If clearances and PIV cards are not properly terminated, recovered, and destroyed, former employees may gain unauthorized access to Department buildings or information. This risk has been demonstrated by incidents at the Department and other Federal agencies in which former employees have accessed facilities or systems using unrecovered badges. During our audit, we were made aware of one instance where a Department official witnessed a former Headquarters employee enter the building and access his work space in a restricted area. This former employee's PIV card had not been recovered and the employee's status in USAccess had not been updated, as required. The witness reported the incident, and Headquarters' security personnel were able to contact the individual and recover the badge without further trouble. At another Federal agency, a terminated employee repeatedly used administrator credentials to log onto Government servers and made unauthorized changes to the agency's website, including disabling the website's online tool. As a result, this former employee caused damage and loss to the agency's website. To mitigate the risk of unauthorized access, the Department needs to take actions to ensure that it terminates security clearances and PIV card access for separated Federal and contractor employees in a timely manner.

RECOMMENDATIONS

To improve controls over access authorization termination, we recommend that the Associate Under Secretary for Environment, Health, Safety and Security, and the Chief Information Officer, in coordination with the Acting Under Secretary of Energy, the Under Secretary for Science, the Acting Administrator of the National Nuclear Security Administration, and the Chief Human Capital Officer:

1. Revise Department Orders 206.2, 472.2, 473.3A, as appropriate, to:

    a. Identify/assign responsibility for updating employee status in USAccess or other PIV databases, including ensuring the completeness and accuracy of personnel information entered in identity record databases;

    b. Outline security requirements for out-processing separated employees and require local procedures, including identifying timeframes for security out-processing actions;

    c. Establish a requirement for tracking expired credentials, badges for employees transferring to other offices within the Department, and separated employees' badges;

    d. Ensure that Contracting Officers implement the requirements stipulated in Federal Acquisition Regulation 52.204-9, *Personal Identity Verification of Contractor Personnel*; and

    e. Subject all uncleared contractors to Homeland Security Presidential Directive (HSPD-12) requirements, as appropriate.

We also recommend that the Acting Under Secretary of Energy, the Under Secretary for Science, and the Acting Administrator of the National Nuclear Security Administration:

2. Take measures to ensure that appropriate databases interface with USAccess. At a minimum, require periodic reconciliations of human resources data to the local badge systems and the Department's CPCI system; and

3. Implement policy and verify that the PIV card is the common means for access to Department facilities, networks, and information systems, as required by Federal regulations.

In addition, we recommend that the Chief Information Officer, in coordination with the Director, Office of Corporate Business Systems, the Acting Under Secretary of Energy, the Under Secretary for Science, and the Acting Administrator of the National Nuclear Security Administration:

4. Ensure that the Department's human resources, identity management, and physical and logical access systems include employees' Department of Energy unique identifiers and that they interface with the Department's Enterprise Identity Management Service System.

MANAGEMENT RESPONSE

Management generally concurred with our recommendations and identified actions it would take to address them. Management plans to complete corrective actions by October 1, 2022. Management will convene a working group to determine areas within Department of Energy orders that require revision and determine a path forward for implementing the actions operationally. Additionally, Management will meet periodically with system owners to ensure that databases are on track to interface properly with USAccess and that PIV cards and security clearances are terminated in a timely manner. Management's comments are included in Appendix 4.

AUDITOR COMMENTS

Management's proposed actions are responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

We conducted this audit to determine whether the Department of Energy terminated security clearance and Personal Identity Verification (PIV) card access for separated employees in accordance with Federal regulations and Department policies.

Scope

This audit was performed from July 2018 through January 2020. We conducted the audit at the Department's Headquarters, in Washington, DC and Germantown, Maryland; and Albuquerque, New Mexico facilities, which included Sandia National Laboratories (SNL). Our scope included a review of Federal and contractor employee separations that occurred between October 1, 2015, and May 30, 2018. This audit was conducted under the Office of Inspector General project number A18CH036.

Methodology

To accomplish the objective, we:

- Reviewed applicable laws, regulations, executive orders, and other guidance.
- Interviewed Headquarters and Albuquerque personnel responsible for clearance and access authorization, and badge issuance and recovery.
- Obtained an understanding of and became familiar with the Department's use of the U.S. General Service Administration's USAccess system for PIV cards that serve as employee authorization badges, the Department's Central Personnel Clearance Index system for processing security clearance actions, and other systems that store information on employee separations.
- Tested the Department's controls over access termination using separation data provided by the Department's Office of Corporate Information Systems and SNL. We received listings showing that there were 10,129 Federal and contractor employee separations between October 1, 2015, and May 30, 2018. Department officials supplied the names for 8,151 Federal and contractor employee separations. SNL supplied the names for another 1,978 contractor employee separations. We did not request employee separation data for all the Department's sites, laboratories, or facilities. We were able to match 5,803 of the 10,129 separated employee names to information available in USAccess.
- Analyzed data on the 5,803 separated employees available in USAccess. Our analysis determined whether officials updated two key access authorization fields in USAccess for each separated employee: (1) Employment status marked as "terminated" and (2) PIV card status marked as "destroyed."

- Performed additional validation test work on 2,703 separated Federal and contractor employees at two locations, Headquarters and Albuquerque. There were a total of 1,997 employees that separated from Headquarters, comprised of 979 Federal and 1,018 contractor employee separations. We looked at a total of 706 employees that separated from Albuquerque, comprised of 179 Federal and 527 contractor employee separations from SNL. Specifically, our validation test work at these two locations:

    - Verified that the separated employees belonged to the security offices serving the locations selected and confirmed the results of our analysis on the two authorization fields.

    - Determined whether PIV cards for employees, whose cards were not marked as "destroyed" in USAccess, were recovered and physically destroyed. Along with this procedure, we observed destruction records supporting that the PIV cards marked as "destroyed" in USAccess were physically destroyed.

    - Selected a judgmental sample of 260 separated Federal and contractor employees and determined whether the Department's interests in their security clearances were terminated within the 4-working-day requirement. Our review determined that 25 employee clearances did not meet our selection criteria, leaving 235 sample items tested. Because selection was not statistically driven, the results and overall conclusions are limited to the employees reviewed and results cannot be projected to the entire population subject to audit.

- Performed limited testing on 4,326 of the 10,129 separated Federal and contractor employees whose names did not match information in USAccess. Specifically, we used Audit Command Language analysis software to identify nonmatching names and looked up separated employees with clearances in the Central Personnel Clearance Index system.

- Evaluated the results of related audits and reviews.

We conducted this performance 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit included tests of internal controls and compliance with the laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We relied on computer-processed data to satisfy the audit objective. As noted above, we could not match all the separated Federal and contractor employee names on the listings provided to information contained in USAccess. However, in cases where we used computer-processed data, we performed additional procedures to ensure that the data was sufficiently reliable for the purposes of our review.

Department officials waived an exit conference.

ANALYSIS

We found records from USAccess for 5,803 of the 10,129 Federal and contractor employees that separated between October 2015 and May 2018. We analyzed data on these 5,803 separated employees and performed validation test work on 2,703 separated Federal and contractor employees at Headquarters and Albuquerque, New Mexico, which included Sandia National Laboratories (SNL). The following three tables detail the results of our analysis on updating the Department's Personal Identity Verification (PIV) cards in U.S. General Service Administration's USAccess database to reflect employee separations; recovering and destroying access authorization badges; and, where applicable, withdrawing separated employees' security clearances.

Table 1 illustrates how often employment and card statuses were not updated in USAccess, which means that we identified separated employees whose employment statuses were not marked as "terminated" but their PIV cards were marked "destroyed" (Employment Not Marked as "Terminated"). We also identified those separated employees whose PIV cards were not marked as "destroyed" (PIV Card Not Marked "Destroyed.")

Table 1: USAccess Status Updates					
		Statuses Not Updated in USAccess			
Location of Employee Separations	**Employees Reviewed**	**Employment Not Marked "Terminated"**	**PIV Card Not Marked "Destroyed"**	**Total Not Updated**	**Percent**
Headquarters					
Federal separations	979	378	78	456	47%
Contractor separations	1,018	328	144	472	46%
Albuquerque					
Federal separations	179	32	5	37	21%
SNL Contractor separations	527	18	76	94	18%
TOTAL	**2,703**	**756**	**303**	**1,059**	**39%**

Table 2 shows Federal and contractor employees whose PIV cards were not marked as "destroyed" in USAccess compared to verified PIV destruction records.

Table 2: PIV Card Retrieval and Destruction			
		PIV Card Not Confirmed as Physically Destroyed	
Location of Employee Separations	**PIV Card Not Marked "Destroyed" in USAccess**	**No Destruction Record**	**Percent**
Headquarters			
Federal separations	78	67	86%
Contractor separations	144	130	90%
Albuquerque			
Federal separations	5	2	40%
SNL Contractor separations	76	0	0%
TOTAL	**303**	**199**	**66%**

Table 3 summarizes our analysis of security clearance terminations for a judgmental sample of 260 Federal and contractor employees that separated between October 1, 2015, and May 30, 2018, at the two locations where we performed validation procedures.

Table 3: Security Clearance Termination					
		Clearances Not Terminated			
Location of Employee Separations	**Security Clearances Reviewed**	**In 4 Working Days**	**Percent**	**Within 90 days**	**Percent**
Headquarters					
Federal separations	58	23	40%	7	12%
Contractor separations	47	21	45%	17	36%
Albuquerque					
Federal separations	65	17	26%	1	2%
SNL Contractor separations	65	9	14%	1	2%
TOTAL	**235**	**70**	**30%**	**26**	**11%**

PRIOR REPORTS

- Inspection Report on *Badge Retrieval and Security Clearance Termination at Sandia National Laboratory-New Mexico* (DOE/IG-0724, April 2006). This inspection concluded that internal controls were not adequate to ensure that security badges assigned to terminating Sandia National Laboratories (SNL) and subcontractor employees were retrieved at the time of departure or that security clearances of terminating SNL and subcontractor employees were terminated in a timely manner. The inspection also determined that subcontractor employees performing personnel security duties were not conducting adequate security debriefings or retaining all required documentation in personnel security files of departing employees.

- Inspection Report on *Security Clearance Terminations and Badge Retrieval at the Lawrence Livermore National Laboratory* (DOE/IG-0716, January 2006). This inspection concluded that Lawrence Livermore National Laboratory's (Livermore) internal control structure was not adequate to ensure that security badges were retrieved at the time of employee departure or that security clearances of departing employees were terminated in a timely manner. The report also found that Livermore did not have sufficient internal controls to adequately monitor the current employment status of over 700 cleared subcontractor employees and affiliated personnel. In addition, Livermore did not have performance metrics to measure significant aspects of personnel security activities, including timely termination of security clearances and retrieval of security badges.

- Inspection Report on *Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory* (DOE/IG-0677, February 2005). This inspection found that Los Alamos National Laboratory's out-processing procedures were not followed by more than 40 percent of the 305 terminating employees included in the inspection sample. Consequently, Property Administrators, Classified Document Custodians, and Badge Office personnel frequently did not receive timely notification that employees were terminating. The inspection also found that there was no assurance that, prior to departure, Los Alamos National Laboratory terminating employees turned in security badges, completed the required Security Termination Statement, or had their security clearances and access authorizations to classified matter and/or Special Nuclear Material terminated in a timely manner.

- Audit Report on *Personnel Security Clearances and Badge Access Controls at Selected Field Locations* (DOE/IG-0582, January 2003). This audit found a statistically significant number of badges had not been recovered from former contractor and other non-Federal workers at Oak Ridge Reservation, as well as minor discrepancies in the recovery of badges at Savannah River Site, SNL, and Los Alamos National Laboratory. Auditors also found discrepancies in the Central Personnel Clearance Index records at all four locations: a 19 percent error rate at Savannah River Site; a 13 percent error rate at SNL; a 6 percent error rate at Oak Ridge Reservation; and less than 1 percent error rate at Los Alamos. Auditors determined site-level badge recovery and clearance termination processes were inefficient and suffered from a number of control weaknesses.

- Audit Report on *Personnel Security Clearances and Badge Access Controls at Department Headquarters* (DOE/IG-0548, March 2002). This audit found that unauthorized individuals could gain access to Department of Energy Headquarters due to process problems with the Department's clearance and badging controls. The auditors reviewed a sample of selected clearance and badge records and found instances where the Department had either not terminated the employees' security clearances or had not recovered their badges, permitting potential access to Department facilities and sensitive information. The Office of Headquarters Security Operations planned to take corrective actions to improve clearance and badging controls.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

October 30, 2020

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: MATTHEW B. MOURY
ASSOCIATE UNDER SECRETARY FOR
ENVIRONMENT, HEALTH, SAFETY AND SECURITY

SUBJECT: COMMENTS FOR IG DRAFT AUDIT REPORT:
Personnel Security Clearances and Badge Access Controls for Separated Employees (A18CH036)

Thank you for the opportunity to comment on the Office of Inspector General's Draft Report "Personnel Security Clearances and Badge Access Controls for Separated Employees" (A18CH036). Following is Department of Energy's, including the National Nuclear Security Administration, consolidated response to the draft report's recommendations.

Office of Environment, Health, Safety and Security

To improve controls over access authorization termination, we recommend that the Office of Environment, Health, Safety and Security and Office of the Chief Information Officer in coordination with the Under Secretary of Energy, Under Secretary for Science, the Administrator for the National Nuclear Security Administration, and the Office of the Chief Human Capital Officer:

Recommendation 1: Revise the Department's Orders 206.2, 472.2, 473.3A, as appropriate, to:

Recommendation 1-a: Identify/assign responsibility for updating employee status in USAccess or other Personal Identity Verification in recommendation databases, including ensuring the completeness and accuracy of personnel information entered in identity record databases.

Management Response: Concur.

Action Plan: The Office of Environment, Health, Safety and Security will convene a working group with all stakeholders, including the National Nuclear Security Administration, the Office of Science, the Office of the Chief Information Officer, and the Office of Human Capital Officer, to develop a plan for addressing the recommendation. The working group will first convene within 90 days from the date of the final report and meet periodically to review the referenced Department of Energy Orders as they relate to the findings in the report. The working group will determine the areas within the Orders that require revision and determine path forward for implementing the actions operationally.

Estimated Completion Date: October 1, 2022.

Recommendation 1-b: Outline security requirements for out-processing of separated employees and require local procedures, including identifying timeframes for security out-processing actions.

Management Response: Concur.

Action Plan: The Office of Environment, Health, Safety and Security, will convene a working group with all stakeholders, including the National Nuclear Security Administration, the Office of Science, the Office of the Chief Information Officer, and the Office of Human Capital Officer, to develop a plan for addressing the recommendation. The working group will first convene within 90 days from the date of the final report and meet periodically to review the referenced Department of Energy Orders as they relate to the findings in this report. The working group will determine the areas within the Orders that require revision and determine path forward for implementing the actions operationally.

Estimated Completion Date: October 1, 2022.

Recommendation 1-c: Establish a requirement for tracking expired credentials, badges for employees transferring to other offices within the Department, and separated employees' badges.

Management Response: Concur.

Action Plan: The Office of Environment, Health, Safety and Security will convene a working group with all stakeholders, including the National Nuclear Security Administration, the Office of Science, the Office of the Chief Information Officer, and the Office of Human Capital Officer, to develop a plan for addressing the recommendation. The working group will first convene within 90 days from the date of the final report and meet periodically to review the referenced Department of Energy Orders as they relate to the findings in the report. The working group will determine the areas within the Orders that require revision and determine a path forward for implementing the actions operationally.

Estimated Completion Date: October 1, 2022.

Recommendation 1-d: Ensure that Contracting Officers implement the requirements stipulated in the Federal Acquisition Regulation 52.204-9, *Personal Identity Verification of Contractor Personnel*.

Management Response: Concur.

Action Plan: The Office of Environment, Health, Safety and Security will convene a working group with all stakeholders, including the National Nuclear Security Administration, the Office of Science, the Office of the Chief Information Officer, and the Office of Human Capital Officer, to develop a plan for addressing the recommendation. The working group will first convene within 90 days from the date of the final report and meet periodically to review the referenced Department of Energy Orders as they relate to the findings in the report. The working group will

determine the areas within the Orders that require revision and determine a path forward for implementing the actions operationally.

Estimated Completion Date: October 1, 2022.

Recommendation 1-e: Subject all uncleared contractors to Homeland Security Presidential Directive-12 (HSPD-12) requirements, as appropriate.

Management Response: Concur.

Action Plan: The Office of Environment, Health, Safety and Security will convene a working group with all stakeholders, including the National Nuclear Security Administration, the Office of Science, the Office of the Chief Information Officer, and the Office of Human Capital Officer, to develop a plan for addressing the recommendation. The working group will first convene within 90 days from the date of the final report and meet periodically to review the referenced Department of Energy Orders as they relate to the findings in the report. The working group will determine the areas within the Orders that require revision and determine a path forward for implementing the actions operationally.

Estimated Completion Date: October 1, 2022.

Office of Science

We also recommend that the Under Secretary of Energy, Under Secretary for Science, and the Administrator for the National Nuclear Security Administration:

Recommendation 2: Take measures to ensure that appropriate databases interface with USAccess. At a minimum, require periodic reconciliations of human resources data to the local badge systems and the Department's Central Personnel Clearance Index (CPCI) system.

Management Response: Concur.

Planned Action: The Office of Science (SC) will meet periodically with the Office of Environment, Health, Safety and Security and the Office of Chief Information Officer, owners of the systems/working group, and to assure databases are on track to interface properly with USAccess. This will include appropriate Office of Information Technology helpdesk and human resource personnel for badging systems and CPCI to assure Personal Identity Verification Badges and Clearances are terminated in a timely manner. SC will perform above on a minimum of an annual basis, and by performing a statistical sampling, follow up for quality control for badges and clearances.

Estimated Completion Date: October 1, 2022.

Recommendation 3. Implement policy and verify that the Personal Identity Verification card is the common means for access to Department facilities, networks, and information systems, as required by Federal regulations.

Management Response: Concur.

Planned Action: The Office of Science (SC) has already begun the process to analyze how SC Laboratories employees will utilize Personal Identity Verification badges as required by Federal regulations. SC will take steps to meet new badging requirements described in Department of Energy Order 473.1A, *Physical Protection Program*.

Estimated Completion Date: October 1, 2022.

National Nuclear Security Administration

We also recommend that the Under Secretary of Energy, Under Secretary for Science, and the Administrator for the National Nuclear Security Administration:

Recommendation 2: Take measures to ensure that appropriate databases interface with USAccess. At a minimum, require periodic reconciliations of human resources data to the local badge systems and the Department's CPCI system.

Management Response: Concur in Principle.

Action Plan: The recommendation as written is not fully actionable for NNSA. NNSA does not own USAccess or the CPCI system and, therefore, does not have the authority or responsibility to develop interfaces for those systems. NNSA will, however, provide any support requested by the system owners for development of automated interfaces.

In relation to reconciliations of human resources data to USAccess and the CPCI, during the period under review, the NNSA USAccess sponsor received daily reports from NNSA Office of Defense Nuclear Security (NA-70) showing actions taken in the CPCI for field employees and monthly separation reports from human resources that were both reconciled to badge records in USAccess. As a result of this process, NNSA's Albuquerque exception rates were much lower, as noted in the audit report. In October 2019, responsibility for NNSA Headquarters employee clearance actions was transferred from Department of Energy Personnel Security to NA-70. With this move, NNSA is now responsible for most clearance actions within the NNSA Enterprise. Consolidating responsibility for most actions has enabled organizational elements to work more collaboratively in executing processes for reconciling badging and clearance data across the complex. NNSA will continue to refine and implement these processes to ensure data integrity in the USAccess and CPCI systems. These processes will be formalized in Standard Operating Procedures by January 31, 2021.

Estimated Completion Date: January 31, 2021.

Recommendation 3. Implement policy and verify that the Personal Identity Verification card is the common means for access to Department facilities, networks, and information systems, as required by Federal regulations.

Management Response: Concur.

Action Plan: The National Nuclear Security Administration (NNSA) implements Department of Energy (DOE) Order 206.2, *Identity, Credential, and Access Management (ICAM)*, which establishes basic requirements for Homeland Security Presidential Directive 12 (HSPD-12). DOE Order 206.2 requires that HSPD-12 credentials be issued to DOE employees, cleared contractors, uncleared headquarters contractors, and other uncleared DOE contractor employees based on a risk analysis.

NNSA issued NNSA Supplemental Directive (SD) 206.2, *Implementation of Personal Identity Verification for Uncleared Contractors*, on April 14, 2018, which applies to all uncleared contractors with both logical and/or physical access to NNSA information technology systems and facilities. In keeping with the risk-based approach promulgated by the Office of Management and Budget, NNSA SD 206.2 does not mandate issuance of a Personal Identity Verification card to employees requiring only temporary, localized site access. This allows NNSA to avoid unnecessary costs associated with temporary employees such as general construction personnel. NNSA has several ongoing large-scale projects where temporary construction personnel only have access to the site and not areas containing security assets. Temporary employees are issued local site-specific badges, which allows physical access to the work area. The Supplemental Directive has been incorporated into all of the NNSA Management and Operating Contracts. NNSA considers this recommendation closed.

Estimated Completion Date: N/A

Office of the Chief Information Officer

In addition, we recommend that the Office of the Chief Information Officer in coordination with the Office of Corporate Information Systems, the Under Secretary of Energy, Under Secretary for Science, and the Administrator for National Nuclear Security Administration:

Recommendation 4: Ensure that the Department's human resources, identity management, and physical and logical access systems include employees' Department of Energy unique identifiers and that they interface with the Department's Enterprise Identity Management Service System.

Management Response: Concur.

Action Plan: The Office of the Chief Information Officer (OCIO) has engaged business owners as an integral step in the Department of Energy (DOE) Enterprise Architecture program assuring that major initiative is driven by the mission of DOE. Through this process nine opportunities have been identified of which one directly supports the underlying goal of this audit finding: Extend Enterprise Access Management. In addition, OCIO is the sponsor for three major programs: migration of systems to the ubiquitous poly-cloud environments; Identity and Access Management (ICAM) Program; and the Continuous Diagnostics and Mitigation (CDM)

program. OCIO has a strategic project to aggressively remove social security numbers from systems where there is not a compelling business driver.

OCIO, through the Enterprise Architecture Governance Board, approved the ICAM Integrated Product Team (IPT) charter at its September 2020 monthly meeting. The charter designates the ICAM Program Manager as the chair with the Office of Environment, Health, Safety, and Security (AU) serving as one co-chair and the CDM as the second co-chair. OCIO has adopted the Agile framework for accelerating the pace of service delivery taking an incremental approach to developing value. OCIO will finalize a cross functional initiative in coordination with the ICAM IPT to execute within the agile framework to create an Epic "Identity and Access Management for the DOE Polycloud Modernization." This special project will be led by elements of the Office of Architecture Engineering, Technology, & Innovation (IM-50), Office of Cybersecurity (IM-30), Office of Enterprise Records Management, Privacy, and Compliance (IM-40), and AU's Office of Information Management, guided by the ICAM IPT. Stakeholders will include supporting elements in the Office of Budget and Contracts (IM-10), the Office of Policy and Investments (IM-20), Lawrence Livermore National Laboratory (OneID,) and AU (physical access control systems.)

The outcome will be a coordinated and integrated approach to assure accountability and access validation for physical and logical systems.

Estimated Completion Date: September 1, 2021.

If you have any questions, please contact me at (202) 586-1285 or have a member of your staff contact Mr. James Hutton, Director, Office of Headquarters Security Operations, at (202) 586-0975.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 586-1818. For media-related inquiries, please call (202) 586-7406.