INVESTIGATIVE REPORT

David Cook, Inspector General

OFFICE: INDIANA FAMILY AND SOCIAL SERVICES ADMINISTRATION (FSSA) & INDIANA OFFICE OF TECHNOLOGY (IOT)
TITLE: MISSING STATE LAPTOPS[1]
CASE ID: 2022-01-0013
DATE: January 3, 2023

Indiana Office of Inspector General Chief Legal Counsel, Tiffany Mulligan, after an investigation by Inspector General Special Agent Sam Stearley reports as follows:

The Indiana General Assembly charged the Office of the Indiana Inspector General (OIG) with addressing fraud, waste, abuse and wrongdoing in the executive branch agencies of state government. Ind. Code §4-2-7-2(b). The OIG also investigates allegations of criminal activity and Code of Ethics violations within state government. Ind. Code §4-2-7-3. The OIG may recommend policies and carry out other activities designed to deter, detect and eradicate fraud, waste, abuse, mismanagement and misconduct in state government. Ind. Code §4-2-7-3(2).

I. Complaint

In January of 2022, the OIG received a complaint alleging that fifty-three state laptops assigned to the Indiana Family and Social Services Administration (FSSA) had been lost or stolen. Shortly after receiving the complaint, the OIG learned that FSSA's IN211 team reported the theft of thirty-three laptops. The OIG confirmed that the thirty-three laptops were included in the original fifty-three that had been reported to the OIG as lost or stolen and the remaining twenty

[1] The Inspector General has determined that publishing this report is in the public's interest.

laptops had been returned to the State. FSSA staff reported that the IN211 team filed police reports with the Indiana State Police (ISP) for the thirty-three missing laptops. They also reported that the laptops were encrypted so FSSA had no concerns regarding data leakage.

II. OIG Investigation

OIG Special Agent Sam Stearley investigated the complaint. As part of the investigation, Special Agent Stearley interviewed multiple individuals, including several employees of FSSA and the Indiana Office of Technology (IOT) who were involved in either the distribution or attempts to recover the missing laptops. He also interviewed the ISP Detective who investigated the missing laptops. Special Agent Stearley obtained and reviewed multiple documents from FSSA, IOT and ISP, including state contracts, purchase orders, policies, emails and the ISP report on the missing laptops.

According to Special Agent Stearley's investigation, the thirty-three missing computers were valued at approximately six hundred and sixty-two dollars ($662) each, for a total value of twenty-one thousand eight hundred and forty-six dollars ($21,846).

A. Purchase and Assignment of Laptops

Special Agent Stearley learned that IOT purchased approximately five hundred laptops at the request of FSSA in 2020. The thirty-three missing laptops were part of this purchase. FSSA requested the laptops to support the State's IN211 Vaccination Call Center (VCC) during the COVID-19 pandemic. As COVID-19 vaccinations became available in Indiana, the State developed the VCC to help Hoosiers schedule vaccination appointments. The State placed the VCC under the IN211 program, which is managed by FSSA. FSSA funded the VCC using Federal Emergency Management Agency funds.

FSSA utilized Knowledge Services to hire staff to support the VCC. Knowledge Services is a private company that provides government and commercial workforce management programs. During the initial development of the VCC, Knowledge Services had a Quantity Purchase Agreement (QPA) with the State of Indiana to provide Managed Service Provider (MSP) services to the State.[2] FSSA purchased MSP services under the QPA using a Purchase Order supported by a Statement of Work. This allowed FSSA to utilize Knowledge Services to supply staff for the VCC. A FSSA employee stated that VCC staff worked remotely.

Special Agent Stearley interviewed several IOT employees who are, in various ways, involved with the management of equipment that IOT provides to state agencies. He learned that IOT owns all state laptops and charges a monthly rate to state agencies for the use of the laptops. According to one IOT employee, IOT owns the laptops, but they are not the "keepers" of the laptops. She explained that IOT refreshes state laptops every four years, and state agencies sign a "PC Refresh Project Charter" at the time of the refresh. The PC Refresh Project Charter specifies that the agencies are the "custodians" of the laptops. Special Agent Stearley obtained a copy of the "IOT FSSA PC Refresh Project Charter" (Charter) that IOT and FSSA representatives signed on October 13, 2017. It reads that FSSA will be "the custodian of all IOT-owned assets provided to the agency."

IOT employees explained the process a state agency uses to obtain new equipment from IOT. IOT receives a job order request from the agency, which includes the details of the agency's request, and IOT keeps a copy of the job order request for its records. IOT also maintains documentation when it purchases equipment from a vendor, including: IOT's purchase orders for the equipment and the packing slips or bills of lading when IOT receives the equipment. When a

[2] The State of Indiana entered into a QPA for MSP services with a new vendor, Computer Aid, Inc. (CAI), in December of 2021.

state agency needs additional equipment from IOT, it submits a ticket to IOT through IOT's ticketing system. IOT then distributes the equipment to the requesting state agency, and the agency distributes the equipment to its employees or contractors. Special Agent Stearley obtained a copy of the job orders and purchase order that IOT maintained for the purchase of the laptops for the VCC.

Special Agent Stearley learned that after IOT purchased the approximately five hundred laptops for the VCC, FSSA did not take delivery of all the laptops at once. At various times, FSSA arranged for groups of approximately twenty-five to fifty employees to start work with the VCC and receive their laptops[3]. A FSSA employee picked up the laptops from IOT periodically as new VCC staff began work. An IOT employee stated that IOT and FSSA maintained a spreadsheet to track the laptops that FSSA picked up. Special Agent Stearley obtained a copy of the spreadsheet. The spreadsheet included how many computers FSSA staff picked up from IOT each day, along with the serial numbers of the laptops.

A FSSA employee explained that after he picked up laptops from IOT for use by the Knowledge Services' employees who would be working for the VCC, he would provide the laptops to the employees and provide them with training. He said that at the start of the VCC, FSSA did not require a signature from the employees or otherwise track which employee received which laptop.

The FSSA employee explained that when FSSA first set up the VCC, FSSA did not have a standard process for ordering the large volume of laptops it needed for the VCC. In the past, when FSSA needed staff from Knowledge Services, FSSA would work with Knowledge Services to identify which Knowledge Services' employees would be performing FSSA work, and then

[3] Along with the state-issued laptop, each employee also received a headset and a charging cord for the laptop.

FSSA would work with SPD and IOT to get the specific employees the assets they needed to perform their work, such as a FSSA identification card and a laptop. With the VCC, FSSA ordered the laptops first, picked them up from IOT and then assigned them to Knowledge Services' employees after FSSA picked up the laptops from IOT. The FSSA employee explained that FSSA does not generally order laptops in bulk for a contractor's employees; however, FSSA handled the request for laptops for the VCC differently due to the speed of which the State needed the VCC to be operational.

An IOT employee explained that IOT usually performs an electronic install form, or "e-install", on a laptop. The employee stated that IOT does not require a signature when an individual receives a computer from IOT because the e-install usually includes information on the end user or the person who received the computer. IOT did not have the names of the end users when FSSA staff picked up the laptops because Knowledge Services had not yet hired staff to work at the VCC. IOT used the FSSA employee's name who picked up most of the computers for purposes of the e-install.

A FSSA employee explained that when he became aware of missing laptops from the VCC, he began writing down the names of VCC workers to whom he assigned specific laptops. The employee explained that this was not the practice when the VCC first started and still is not the standard practice in some instances because of the number of people involved in the process. He cited two reasons that FSSA believed it was unnecessary to track the names of Knowledge Services' employees who received state laptops: (1) FSSA believed Knowledge Services had an agreement with the State that held Knowledge Services responsible for returning any state equipment back to the State in the same condition in which they received the equipment; and (2)

FSSA believed IOT was able to track computers and where they are located when a laptop goes missing.

B. Discovery of and Attempts to Recover Missing Laptops

Special Agent Stearley learned that Knowledge Services' employees who were working for the VCC left work with the VCC at various times and for various reasons. In at least two instances, FSSA engaged in bulk layoffs because of the reduced need for VCC workers as the pandemic-related calls slowed down. In other instances, VCC workers left employment voluntarily or FSSA terminated their employment for poor performance. In some instances, VCC workers simply stopped working with no formal notice of resignation or termination. Special Agent Stearley learned that FSSA employees discovered that some of the terminated VCC workers failed to return their laptops to the State after leaving the VCC. The thirty-three laptops that were reported to the OIG as missing had been assigned to VCC workers who failed to return the laptops when they left employment.

An IOT employee explained that when the pandemic-related calls first started to slow down, FSSA returned several hundred laptops to IOT. She stated that after that point, the return of the laptops by VCC workers ebbed and flowed. She stated that when Knowledge Services employees ended their work for the VCC, they were supposed to turn in their laptops to FSSA. FSSA then was responsible for turning the laptops back to IOT. She explained that the proper procedure is to have an IOT ticket with a returned laptop, so IOT would have an audit trail. IOT wants this record to ensure that the laptop is returned, and IOT takes the use of the laptop off the agency's bill once the laptop is returned.

IOT employees explained that when a laptop is lost or stolen, an agency should submit a ticket to IOT and obtain a police report. The IOT ticket and police report prompts IOT to take the

laptop off the agency's monthly bill. IOT determines depreciation on the laptop and remotely freezes, or locks, the laptop so that it cannot be used by another user. The laptop must be turned on and connected to the internet for IOT to freeze it and ping its location. IOT submits a "ping report" to law enforcement. IOT then reports the loss to the OIG pursuant to Section 8.4.3 of the Indiana State Board of Account's Accounting and Uniform Compliance Guidelines Manual for State and Quasi Agencies (Manual)[4]. One IOT employee explained that it is difficult for IOT to know how many computers are missing on any given day because the number constantly changes as laptops are returned or go missing.

Some of the IOT employees who Special Agent Stearley interviewed stated that they were unaware of any written policies that IOT has in place to handle missing laptops. One IOT employee stated that IOT has a task sequence in the software for lost and stolen property. Special Agent Stearley obtained a copy of a written workflow overview that describes the steps IOT takes when an agency reports IOT equipment as lost or stolen. It confirmed some of the steps described by the IOT employees whom Special Agent Stearley interviewed. Some of the IOT employees stated that they believed that IOT's standard procedures were followed for the missing laptops assigned to the VCC.

The Charter provided that FSSA was responsible for notifying IOT when FSSA determined that IOT equipment had gone missing or stolen. The Charter further reads that FSSA "assumes fiscal responsibility for damage or loss of all IOT-owned assets under their control." A FSSA employee stated that FSSA did not report the thirty-three missing laptops to ISP or the OIG immediately. He claimed this was primarily due to the large number of initiatives that were going

[4] Chapter 8 of the Manual can be located at: CH08-Capital-Asset-Accounting.pdf. Section 8.4.3 of the Manual provides that "Stolen (or suspected stolen) assets should be reported to the Capitol Police and the [OIG] prior to processing retirement."

on at the same time. He also stated that there was an assumption that Knowledge Services would be responsible for collecting the missing laptops.

The FSSA employee stated that once FSSA discovered the missing laptops, FSSA staff brought it to Knowledge Services' attention. FSSA staff worked with Knowledge Services staff to try to identify which former employees had received which laptops. Knowledge Services then sent letters to some of the employees demanding return of the laptops. Special Agent Stearley asked several FSSA employees for copies of these letters; however, he never received copies or saw the letters. The IOT employee stated that although VCC workers were supposed to return the laptops to FSSA, many of them dropped off the laptops to an IOT employee after receiving a letter from Knowledge Services.

Special Agent Stearley learned that Knowledge Services employees who ended their employment with the VCC had several options to return their state laptops. For example, they could return the laptops to the local FSSA office or to the Indiana Government Center in Indianapolis. They also had the option to return the laptops via FedEx. An IOT employee stated that they have had some problems with FedEx losing state equipment, and IOT has had to file claims with FedEx for the lost property. With the various methods employees could use to return the laptops to the State, there was no clear policy for tracking the laptops once the State received them.

FSSA staff stated that once FSSA discovered the missing laptops, FSSA and Knowledge Services began using a shared tracking list, which they could both use to help track the computers and compare notes on a weekly basis. FSSA and Knowledge Services' staff would update the spreadsheet every time an employee was hired or terminated. The FSSA employee stated that it is still not the cleanest or most comprehensive process; however, it was much better than what

occurred at the start of the VCC. He stated that previously FSSA would go several weeks or months after an employee had been terminated before realizing the employee still had a state laptop, but with the spreadsheet, they identified the missing laptop much quicker.

Special Agent Stearley learned that starting in January of 2021, Knowledge Services sent an email to all its staff asking them to sign an agreement acknowledging that they must return equipment upon termination of their assignment. The agreement requires an employee to "immediately return" equipment upon termination of an assignment. In January of 2022, Knowledge Services revised the language. The revised language prohibited employees from using equipment for any personal use and made the employee personally responsible and liable for the security and safety of the equipment. The revised language further required the employee to promptly return the equipment to Knowledge Services upon termination. It reads, "Failure to return the Equipment or pay for damages to such Equipment may result in legal action."

Under FSSA's original Statement of Work with Knowledge Services, Knowledge Services had sixty days to coordinate return of state equipment to the State. After discovery of the missing laptops, FSSA revised the Statement of Work to provide Knowledge Services thirty days to coordinate the return of state equipment.

According to the interviews Special Agent Stearley conducted, the State has made limited efforts to recover the missing laptops from Knowledge Services and has made no efforts to recover funds for the missing laptops from Knowledge Services. One FSSA employee stated that she spoke with Knowledge Services and told them they were responsible for returning the equipment. She stated that she asked if Knowledge Services could withhold the last paycheck for employees who failed to return laptops and was told no. Another FSSA employee stated that he asked if the State could bill Knowledge Services for the missing laptops and was told it could not. None of the

employees that Special Agent Stearley interviewed said they were aware of any efforts by IOT or FSSA to hold Knowledge Services accountable for the missing laptops.

C. ISP Investigation

Special Agent Stearley contacted the ISP Detective who investigated the missing laptops for ISP. The ISP Detective stated that ISP's investigation was long and tedious, both because of FSSA's delay in reporting the missing laptops to ISP and because of Knowledge Service's delay in providing documents in response to the ISP Detective's inquiries. The ISP Detective also stated that Knowledge Services was unable to provide him with certain information. For example, he stated that Knowledge Services could not tell him when and how Knowledge Services staff contacted former employees who failed to return the state laptops because Knowledge Services did not document the contact. He also stated that Knowledge Services never produced written policies on how they managed state-owned equipment and did not have dedicated personnel responsible for documenting or tracking the equipment or the personnel to whom they assigned equipment.

The ISP Detective informed Special Agent Stearley that he submitted the investigation to the Marion County Prosecutor's Office for consideration of criminal charges. The Marion County Prosecutor's Office declined to prosecute the case and cited a list of reasons for this decision. The reasons included: poor business practices associated with State's deployment of the laptops, such as issuing the laptops without adequate documentation and the lack of an agreement signed by the user documenting which laptop the State assigned to which individual; poor business practices associated with accountability of the laptops; lack of a uniform method for employees to return the laptops to the State upon termination by the State; and a lack of documentation to prove recovery efforts by Knowledge Services.

III. Conclusion and Recommendations

The OIG understands that the urgency of the pandemic and the need to have a large volume of employees hired to staff the VCC in a very short timeframe was unprecedented and extremely challenging. In this case, the lack of clear policies and procedures, as well as the assumptions that another agency or the contractor would be responsible for missing assets, contributed to the loss of over $20,000 of state equipment. Such loss is not acceptable, and the State must make efforts to reduce and remedy such loss in the future.

Although the State hopefully will not face another urgent crisis in the near future, it is possible that a state executive branch agency will need to hire a large number of contract employees and assign them state equipment. As such, state agencies should prepare now for such a possibility. Furthermore, state agencies who are responsible for assigning and distributing state equipment to any state employee or contract worker must find ways to better manage and protect these resources so that taxpayer funds are not wasted on state equipment that is never returned to the State.

The OIG also recognizes that FSSA and IOT made some improvements in their processes after discovery of the missing laptops that the OIG investigated in this case. For example, FSSA and Knowledge Services began tracking which laptops they assigned to which individual workers and began tracking whether the workers returned the laptops after their assignment with the VCC ended. Nonetheless, more must be done to reduce future waste of state resources. To this end, the OIG asks all state executive branch agencies to consider how best to protect state assets assigned

to contract workers and makes the following recommendations to help ensure the responsible management of state assets in the future.

Recommendation 1

FSSA eventually reported the missing laptops to both ISP and the OIG pursuant to the SBOA Manual; however, FSSA did not report the missing laptops immediately upon discovery. The delay in reporting the missing laptops complicated both ISP's and the OIG's investigations. The OIG recommends that FSSA, and any other executive branch agency that suspects state equipment has been stolen, report the suspected theft to ISP Capitol Police and the OIG as soon as practical after the agency discovers it.

Recommendation 2

Although IOT and FSSA signed a charter in 2017 that held FSSA responsible for the damage or loss of IOT equipment, some FSSA staff appeared unclear on who was responsible for the state laptops that went missing. The OIG recommends that IOT provide clear, written guidance to state agencies *at the time they receive IOT equipment* that the agency is responsible for damage to or loss of the equipment until they return the equipment to IOT. The OIG also recommends that IOT ensure agencies are aware of the process for an agency to report missing equipment, so that IOT can remove the monthly charges for use of missing equipment from an agency's bill.

Recommendation 3

FSSA staff assigned state laptops to Knowledge Services' employees without tracking which employee received which laptop on a regular basis. The OIG recommends that any executive branch agency that assigns state laptops to state employees or contract employees should have a clear, written policy for tracking the assignment of specific state laptops to the individual employees. For example, employees receiving a state laptop could receive a receipt and/or have to

sign for their laptops, so both the state agency and the employee have a clear record of which laptops have been assigned to which employees.

Recommendation 4

Although the OIG's investigation was limited to the missing laptops assigned to VCC workers, the OIG recommends that state agencies utilizing contract staff also enact policies to track other assets provided to contract employees, including state equipment with serial numbers, state identification badges, access to state government buildings and access to state information. Along with ensuring state assets are returned to the State when a contract worker leaves, state agencies must ensure that the former contract employee no longer has unrestricted access to state government buildings or to confidential information.

Recommendation 5

The OIG recognizes the advantage of allowing state employees and contract employees various methods for returning equipment to the State; however, the multiple methods for returning state equipment made it difficult for all parties involved to know whether state equipment was returned. For example, an employee may have returned a laptop directly to one division of IOT without FSSA, Knowledge Services or even other divisions of IOT knowing of its return. The Marion County Prosecutor's Office cited this as a major reason they declined to prosecute the employees who failed to return the laptops. The OIG recommends that IOT and executive branch agencies clarify how employees must return state equipment and have a consistent method for

tracking its return, regardless of the methods used. Agencies also should consider providing employees some type of receipt for return of state property.

Recommendation 6

State executive branch agencies who assign state equipment to state employees and/or contract employees should advise the employees of the potential consequences, including criminal prosecution for theft, of failing to return the equipment upon termination of their employment. Clear notice to employees of the potential consequences will help encourage former employees to return state equipment and provide better evidence for prosecution when a former employee fails to do so. The OIG recommends that the state agencies require employees to sign a statement acknowledging receipt of state equipment and advising state employees that failure to return state equipment may be considered theft under Ind. Code §35-43-4-2.

Recommendation 7

Although FSSA worked with Knowledge Services to get some of the laptops returned, the State failed to hold Knowledge Services fully accountable for their employees' failure to return state equipment. The OIG recommends that the State incorporate stronger provisions into its contracts with vendors specifying that the vendors will be held responsible for any lost or stolen state equipment that was assigned to the vendor or its workers. Furthermore, the OIG recommends that the State take all appropriate measures to hold the vendors accountable for loss of state equipment.

Dated: January 3, 2023

APPROVED BY:

David Cook, Inspector General