STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL

RANDALL J. MEYER, INSPECTOR GENERAL

REPORT OF INVESTIGATION

AGENCY: OHIO DEPARTMENT OF REHABILITATION AND CORRECTION
FILE ID NO.: 2014-CA00056
DATE OF REPORT: DECEMBER 13, 2016

The Office of the Ohio Inspector General ...
The State Watchdog

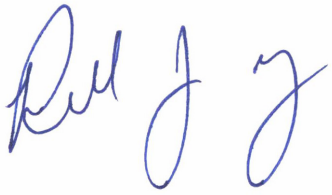
"Safeguarding integrity in state government"

The Ohio Office of the Inspector General is authorized by state law to investigate alleged wrongful acts or omissions committed by state officers or state employees involved in the management and operation of state agencies. We at the Inspector General's Office recognize that the majority of state employees and public officials are hardworking, honest, and trustworthy individuals. However, we also believe that the responsibilities of this Office are critical in ensuring that state government and those doing or seeking to do business with the State of Ohio act with the highest of standards. It is the commitment of the Inspector General's Office to fulfill its mission of safeguarding integrity in state government. We strive to restore trust in government by conducting impartial investigations in matters referred for investigation and offering objective conclusions based upon those investigations.

Statutory authority for conducting such investigations is defined in *Ohio Revised Code §121.41* through *121.50*. A *Report of Investigation* is issued based on the findings of the Office, and copies are delivered to the Governor of Ohio and the director of the agency subject to the investigation. At the discretion of the Inspector General, copies of the report may also be forwarded to law enforcement agencies or other state agencies responsible for investigating, auditing, reviewing, or evaluating the management and operation of state agencies. The *Report of Investigation* by the Ohio Inspector General is a public record under *Ohio Revised Code §149.43* and related sections of *Chapter 149*. It is available to the public for a fee that does not exceed the cost of reproducing and delivering the report.

The Office of the Inspector General does not serve as an advocate for either the complainant or the agency involved in a particular case. The role of the Office is to ensure that the process of investigating state agencies is conducted completely, fairly, and impartially. The Inspector General's Office may or may not find wrongdoing associated with a particular investigation. However, the Office always reserves the right to make administrative recommendations for improving the operation of state government or referring a matter to the appropriate agency for review.

The Inspector General's Office remains dedicated to the principle that no public servant, regardless of rank or position, is above the law, and the strength of our government is built on the solid character of the individuals who hold the public trust.



Randall J. Meyer
Ohio Inspector General

STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL
RANDALL J. MEYER, INSPECTOR GENERAL

REPORT OF INVESTIGATION

FILE ID NUMBER:	2014-CA00056
SUBJECT NAME:	Ohio Department of Rehabilitation and Correction
POSITION:	State Agency
AGENCY:	Ohio Department of Rehabilitation and Correction
BASIS FOR INVESTIGATION:	Inspector General Initiative
ALLEGATIONS:	Theft of Records and/or Information
INITIATED:	August 21, 2014
DATE OF REPORT:	December 13, 2016

INITIAL ALLEGATION AND COMPLAINT SUMMARY

On August 19, 2014, the Office of the Ohio Inspector General was contacted with a request for assistance in an on-going investigation by the U.S. Department of Education Office of Inspector General (USDOE-OIG). The USDOE-OIG identified particular applications for federal student aid using identities of individuals incarcerated by the Ohio Department of Rehabilitation and Correction (ODRC). USDOE-OIG requested assistance from the Office of the Ohio Inspector General in determining how the identities of the inmates could have been used to submit a Free Application for Federal Student Aid (FAFSA) and if any ODRC employees were involved in the scheme. An investigation was opened on August 21, 2014.

BACKGROUND

Ohio Department of Rehabilitation and Correction

The Ohio Department of Rehabilitation and Correction is charged with the supervision of felony offenders in the custody of the state, including providing housing, following their release from incarceration, and monitoring the individuals through the parole authority. The department also oversees the community control sanction system that provides judges with sentencing options to reduce the inmate population. There are currently 27 correctional institutions throughout the state of Ohio. The director of ODRC is appointed by the governor and confirmed by the Ohio Senate. ODRC is funded through general revenue funds, federal funding, and revenue earned through sales from the Ohio Penal Industries.[1]

Federal Student Aid

Federal Student Aid (FSA), a part of the U.S. Department of Education, provides federal grants, loans, and work-study funds to students throughout the country. To apply for student aid, individuals complete the Free Application for Federal Student Aid (FAFSA) and submit the application to FSA for processing. This form is available online and can be submitted electronically or via a hardcopy by mail.[2]

[1] Source: Biennial budget documents.
[2] Source: Federal Student Aid website.

Relevant Statutes and Policies

Ohio's Confidential Personal Information Protection Statute

Ohio Revised Code (ORC) §1347.15 states that state agencies must develop and adopt agency rules regarding the access of confidential personal information (CPI) that is maintained by the state agency. Confidential personal information is defined as any personal information that is not considered a public record, with common examples being Social Security numbers, driver's license numbers, medical records, or other records whose release is prohibited by state or federal law. ORC §1347.15 specifies several requirements that agencies must incorporate into their rules concerning the handling of CPI, including but not limited to: a defined criteria used to determine an employee's level of access to CPI and a list of valid reasons as to when employees are permitted to access CPI; a procedure for logging and recording employee access to CPI and the requirement that a password or other authentication must be used to access CPI stored electronically; that agencies designate an employee to serve as the data privacy point-of-contact who ensures that CPI is properly protected; the requirement that agencies must provide, on demand to an individual, a detailed listing of all CPI maintained by that agency concerning that individual, unless the CPI relates to an investigation; and a policy that requires agencies to notify individuals whose CPI has been accessed for an invalid reason.

However, ORC §1347.04 exempts ODRC from the requirements of tracking and logging access to confidential personal information. Specifically, ORC §1347.04(A)(1)(d) states "… any agency or local agency that is a correction, probation, pardon or parole authority" is not required to follow the provisions of the CPI statute.

State of Ohio Policies and Procedures

On April 18, 2011, the Ohio Department of Administrative Services (ODAS) Office of Information Security and Privacy issued State of Ohio IT Standard ITS-SEC-02, *Enterprise Security Controls Framework*. This policy sets the statewide minimum standard for information security in all state agencies. ITS-SEC-02 incorporates the National Institute of Standards and

Technology 800-53 (NIST 800-53) recommendations[3] as the framework for information security controls.

In addition, ODAS Policy ITS-SEC-02 4.1.7 *Maintenance, Monitoring and Analysis of Security Audit Logs* adopts NIST 800-53 audit and accountability (AU family) protocols. This policy requires state agencies to determine specific "auditable events" based upon risk assessment and business needs. The content of these auditable events are determined by the nature and type of the event. In the case of user access, an auditable event should include user or process identifiers (i.e., user name), time stamp of the event, files or information access involved, and the access control rule invoked. Per this policy, these audit event records should be automatically retained for future inspection. The AU family of protocols also states that a mechanism for a "session audit" be put into place, that is a mechanism to capture and log all content related to a specific user session.

ODAS Policy ITS-SEC-02 4.1.10 *Controlled Access* states that state agencies must implement user access controls based on the principles of "need-to-know" and "least privilege" articulated in the NIST 800-53 Access Control (AC family) protocols. The principle of "need-to-know" is a data restriction classification for material considered sensitive. It states that for any sensitive information, access to the information should only be given to those individuals who require the information for necessary functions. The principle of "least privilege," also called "minimal privilege" or "least authority," states that in a particular computing environment, users should have access privileges only for the information or resources which are necessary for that user's legitimate purposes. Stated another way, the principle of "least privilege" states that system users should not have access to information or resources which are not necessary for the user's legitimate purposes. Together, these principles entail creating user access controls which restrict users from accessing any information except the least amount of information necessary to accomplish specific assigned tasks. The policy also states that information systems should

[3] ITS-SEC-02 specifically adopts National Institute of Standards and Technology Special Publication 800-53, Revision 3 (NIST 800-53); however, since the creation of ITS-SEC-02, NIST 800-53 has been updated to Revision 4. For purposes of this report, there are no significant changes between Revision 3 and Revision 4.

include an access enforcement mechanism which controls user access to approved authorized information.

INVESTIGATIVE SUMMARY

The USDOE-OIG presented the Office of the Ohio Inspector General with 713 FAFSA applications for federal student aid suspected of being fraudulent. Investigators cross-referenced the data supplied by the USDOE-OIG with a database of Ohio inmates and identified 145 applications from inmates or parolees under supervision by the State of Ohio during the time period the inmate identities were used to fraudulently apply for student aid from February 1, 2012, to July 9, 2014. Of those 145 applications, 62 inmate identities were used to enroll in qualifying academic institutions around the United States, and were able to successfully apply for and receive disbursements from the USDOE totaling $422,523.50. After the USDOE FSA program paid the tuition balance to the academic institutions, the remaining funds were disbursed to financial institutions provided by the applicants.

While investigating how these inmates' identities were acquired and used in USDOE FAFSA applications, the Office of the Ohio Inspector General discovered that the ODRC Departmental Offender Tracking System (DOTS) displayed the inmate's Social Security number and date of birth on the initial screen, called the Offender Summary Screen (OSMRY). Investigators determined that this was the probable source of the confidential personal information used in the fraudulent FAFSA applications. On September 19, 2014, investigators contacted the Ohio Department of Administrative Services Chief Security Officer David Brown, and notified him of the probable source for the breach of the inmates' identities while in the custody of the state.

On October 7, 2014, Office of the Ohio Inspector General investigators met with ODRC Chief Information Officer Vinko Kucinic, ODRC IT Manager Bob Johnson, and ODRC IT Specialist Katie Harriston, who oversees the management and administration of DOTS. At this meeting, the ODRC officials stated that any employee with a valid account within DOTS could access any inmate record, including an inmate's Social Security number, date of birth, and other personal identifying information. In addition, another computer application portal, ODRC Gateway, also contains this confidential inmate information, and can be accessed by any system user. ODRC

Gateway is provided to and used by numerous social services organizations, halfway houses, work release programs, parole and probation agencies throughout the State of Ohio. ODRC estimated that approximately 15,000 individuals employed or contracted throughout the state would have access to the Social Security numbers, dates of birth, and other personal information of any inmate or parolee.

In order to determine which of the potentially 15,000 system users had accessed the specific inmate identities used to apply for student aid, the Office of the Ohio Inspector General requested access control logs required by ORC §1347.04, and the ODAS IT policies. ODRC officials stated that, since they are exempt from the requirements of ORC §1347.04, they do not electronically track user access, or require system users to manually log access information.

Without the ability to track user accesses through access logs, either electronically or manually, it is impossible for investigators to determine who accessed the 62 individual inmate records illicitly used in the FAFSA scheme. This lack of ability to review user accesses to the DOTS and ODRC Gateway systems prevented the Office of the Ohio Inspector General from further investigating, and consequently, determining a suspect list related to possible inappropriate record accesses.

Despite being exempted from the statutory requirements of ORC §1347.04, ODRC is required to follow the statewide policies of ODAS in maintaining IT security. The Office of the Ohio Inspector General determined that the controls recommended in NIST 800-53, and incorporated into State of Ohio policies, were not implemented by ODRC during the time period the inmate identities were used to fraudulently apply for student aid.

On July 1, 2015, while this investigation was ongoing, ODAS developed and instituted new information security policies, IT-13 and IT-14. ODAS Policy IT-13 *Data Classification* requires all state agencies, including ODRC, to classify all data it maintains into a data classification methodology regarding the level of confidentiality of stored information. This policy requires all state agencies to create three security classifications, and to sort all information they maintain into one of the three classifications: Confidentiality Low (Public), Confidentiality Moderate, and

Confidentiality High. IT-13 also requires state agencies to adopt data access guidelines for each of the confidentiality classifications requiring more stringent access qualifications for higher classifications of confidentiality, and implement proper access controls.

ODAS Policy IT-14 *Data Encryption and Securing Sensitive Data*[4] requires all state agencies to utilize state-approved encryption systems and to ensure the security and integrity of each information system. This policy also requires each state agency to develop a response procedure in the event of a security breach. ODRC is working with ODAS to develop the required policies and procedures under these new state policies.

CONCLUSION

The U.S. Department of Education Office of the Inspector General requested the assistance of the Office of the Ohio Inspector General in an ongoing federal investigation involving alleged fraudulent payments of federal financial student aid to inmates housed within Ohio. The Office of the Ohio Inspector General attempted to determine how the confidential data of 62 inmates was obtained in order to perpetrate financial fraud against the USDOE totaling $422,523.50. Investigators determined that ODRC employees, contractors, and third-party social service providers did have unaudited access to the confidential personal information of the entire inmate population. Investigators also determined that numerous individuals outside of ODRC employment had access to the confidential personal information of Ohio inmates. However, the legal requirements for handling confidential personal information found in Ohio Revised Code §1347.15, specifically exempts ODRC from maintaining a system log which would have provided an audit trail showing who had accessed specific confidential personal information. The lack of this auditable access log prohibited investigators from determining the nature of the breach of inmates' confidential personal information.

Accordingly, the Office of the Ohio Inspector General finds no reasonable cause to believe a wrongful act or omission occurred in this instance.

[4] ODAS Policy IT-14 was first published as Ohio IT Bulletin ITB-2007.02 on July 25, 2007. This bulletin was a notice to state agencies of recommended information security measures, but was not adopted as official state policy until July 1, 2015, with the creation of IT-14.

Though ODRC is exempt from the requirements of ORC §1347.15, it is not exempt from the requirements of ODAS Policy ITS-SEC-02. This policy details the minimum requirements for information security for state agencies to follow, in order to protect confidential personal information. ITS-SEC-02 incorporates National Institute of Standards and Technology Special Publication 800-53 guidelines into state policy, in part requiring state agencies to maintain systems with event auditing capabilities and restrict user access based on need-to-know and least privilege principles.

The Office of the Ohio Inspector General determined that ODRC did not have the ability to maintain audit logs which would have provided key information regarding which system users had accessed inmate confidential personal information, and ODRC allowed all system users the same level of full access, without implementing principles that would have restricted access on a need-to-know basis.

Accordingly, the Office of the Ohio Inspector General finds reasonable cause to believe a wrongful act or omission occurred in this instance.

Presently, ODRC is working with ODAS to develop adequate protections based on the new ODAS IT policies IT-13 and IT-14.

RECOMMENDATION(S)

The Office of the Ohio Inspector General makes the following recommendations and asks the director of the Ohio Department of Rehabilitation and Correction to respond within 60 days with a plan detailing how the recommendations will be implemented. The Ohio Department of Rehabilitation and Correction should:

1) Fully comply with state policies for data classification (IT-13) and data encryption (IT-14) in order to provide adequate protections to confidential personal information of inmates and parolees under the supervision and care of ODRC.
2) Implement the 21 security controls identified by the Enterprise Security Controls Framework (ITS-SEC-02).

3) Work with the Ohio Department of Administrative Services, Office of Information Security and Privacy, to further develop and improve the technical governance for facilities, applications, and information necessary for the fulfillment of the ODRC mission.

REFERRALS

The Office of the Ohio Inspector General has determined that no referrals are warranted for this report of investigation.

STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL
RANDALL J. MEYER, INSPECTOR GENERAL

NAME OF REPORT: Ohio Department of Rehabilitation and Correction

FILE ID #: 2014-CA00056

KEEPER OF RECORDS CERTIFICATION

This is a true and correct copy of the report which is required to be prepared by the Office of the Ohio Inspector General pursuant to Section 121.42 of the Ohio Revised Code.

Jill Jones
KEEPER OF RECORDS

CERTIFIED
December 13, 2016

Rhodes State Office Tower ◇ 30 East Broad Street – Suite 2940 ◇ Columbus, Ohio 43215-3414
Phone: 614-644-9110 ◇ FAX: 614-644-9504 ◇ Toll Free: 800-686-1525 ◇ Email: oig_watchdog@oig.ohio.gov
The Ohio Inspector General is on the World Wide Web at www.watchdog.ohio.gov

MAILING ADDRESS

OFFICE OF THE INSPECTOR GENERAL
JAMES A. RHODES STATE OFFICE TOWER
30 EAST BROAD STREET – SUITE 2940
COLUMBUS, OH 43215-3414

TELEPHONE

(614) 644-9110

IN STATE TOLL- FREE

(800) 686-1525

FAX

(614) 644-9504

EMAIL

OIG_WATCHDOG@OIG.OHIO.GOV

INTERNET

WATCHDOG.OHIO.GOV