

February 10, 2017

Randall J. Meyer  
Ohio Inspector General  
30 East Broad Street, Suite 2940  
Columbus, Ohio 43215-3414

RE: IG File ID Number 2014-CA00056

Dear Inspector General Meyer:

This letter is in response to investigative file # 2014-CA00056 submitted to the Department of Rehabilitation and Correction by your office on December 13, 2016 with a finding of “no reasonable cause to believe that a wrongful act or omission occurred in this instance”. The following details the response by this agency regarding recommendations made by your office.

**Recommendation #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.**

**Recommendation #2:**

**Implement the 21 security controls identified by the Enterprise Security Controls Framework (ITS-SEC-02).**

**Response:**

As noted in the Ohio Department of Rehabilitation and Correction (ODRC) Report, FILE ID # 2014-CA00056, ORC §1347.04 exempts ODRC from the requirements of tracking and logging access to confidential personal information (CPI). Nonetheless, ODRC is committed to protecting all State of Ohio data, including CPI, by adhering to the best standards and best practices promulgated by the Ohio Department of Administrative Services, Office of Information Technology, Ohio Department of Administrative Services, Office of Information Security and Privacy and the Ohio Office of Budget and Management, Office of Internal Audits.

ODRC’s commitment to protecting State of Ohio data, including CPI, is illustrated by the following proactive actions taken by ODRC over the last three years:

Enterprise Governance: ODRC utilizes a systematic, organizational approach to govern its information technology enterprise. All information technology user policies emulate the directives, standards and best practices of the Ohio Department of Administrative Services, Office of Information Technology, Ohio Department of Administrative Services, Office of Information Security and Privacy and Ohio Office of Budget and Management, Office of Internal Audits. Formal governance oversight groups, representing data owners and stakeholders, technical personnel and the DRC leadership, meet regularly to review, assess and approve information technology projects that impact ODRC users and ODRC inmates. Information technology controls are reviewed annually as part of ODRC's internal management audits. In addition, in 2015, the Ohio Department of Administrative Services assigned a fulltime Chief Information Security Officer (CISO) to ODRC to serve as a direct link between the Ohio Department of Administrative Services, Office of Information Security and Privacy and ODRC for purposes of providing technical governance of ODRC's facilities, data and information systems. The CISO has been invaluable in protecting ODRC information technology infrastructure and ODRC data and information systems to facilitate the mission of ODRC by providing guidance and direction to ODRC in the areas of enterprise security and control policy and procedure development and implementation, ODRC technical staff awareness training, incident response and remediation and security solution identification and implementation.

Staff Training and Awareness: ODRC technology users are required to successfully complete mandatory training that focuses on their role in securing information systems and applications. In addition, the users are notified at every logon to the ODRC network that all ODRC computers and information systems and applications must be used only for official state business. ODRC technology users are also required to report data security threats and are notified when a security threat has been detected and remediated.

Infrastructure and Network: ODRC has deployed significant security enhancements to its information technology infrastructure and network. Privilege access management, Internet monitoring and vulnerability scans have been strengthened. Critical control assessments have been conducted and are ongoing. Penetration testing of DRC's network was also conducted.

Information Systems and Applications: On the application and information system level, ODRC has made security improvements in the encryption of data, the management of user passwords and logon procedures, the masking of CPI and the logging of user transactions. As part of the implementation of new application modules and the production of new features for existing applications, ODRC reviews user access and user privileges using a "need to know" methodology. In addition, user accounts are reviewed on a monthly basis and are disabled for non-use.

Inmate Use of Information Technology: ODRC has allocated considerable resources to enhance the security of information technology hardware and software used by inmates in furtherance of ODRC's Mission to, "Reduce Recidivism Among Those We Touch." An enterprise governance group, comprised of ODRC's leadership, technical personnel and internal subject matter experts, delivers guidance and facilitates a standardized framework for identifying the appropriate access to information technology by inmates. In addition, under the direction of the Chief Information Security Officer, ODRC has taken a more systematic approach for identifying inmate information technology security vulnerabilities and interdicting, investigating and remediating data security

incidents caused by inmates. More importantly, in partnership with the Office of Information Technology at the Ohio Department of Administrative Services, ODRC has initiated a major effort to design, build and implement a highly secure, centralized inmate-specific information technology network that will deliver education, skill building, programming and other online applications to inmates. To enhance the security of the new network, inmate computers will be replaced with dedicated thin client devices that can only access the new inmate network.

National Correctional Leadership: ODRC is proud of its long and fruitful relationship with the American Correctional Association, a national organization that, for 146 years, has championed the cause of corrections and the effectiveness of correctional practices. In recognition of ODRC's information technology efforts, the American Correctional Association, recently adopted information technology auditing standards, proposed by ODRC, that will be used during American Correctional Association audits of correctional facilities and operations throughout the United States.

Thank you for the opportunity to respond to your recommendations.

Sincerely,

A handwritten signature in black ink, appearing to read "Gary C. Mohr". The signature is fluid and cursive, with the first name "Gary" being the most prominent.

Gary C. Mohr  
Director