Ohio | Department of Rehabilitation & Correction

John R. Kasich, Governor
Gary C. Mohr, Director

2017 JUN 16 PM 2:37

June 16, 2017

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

RE: IG File ID Number 2015-CA00043

Dear Inspector General Meyer:

This letter is in response to investigative file #2015-CA00043 submitted to the Department of Rehabilitation and Correction by your office on April 11, 2017, with findings of "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:

ODRC should review the actions of all employees involved to determine if administrative action or training is needed. Specifically, to improve the supervision of the inmates and security of computers and computer parts and eliminate the voluminous hours of unsupervised time of the inmates and their freedom of travel throughout the institution, which is a threat to institutional security and the general public.

Response: ODRC has implemented institution information technology (IT) internal management audit standards, based on ODRC policies, that focus on ensuring that inmate access to IT hardware and software is strictly limited to only ODRC-approved, pro-social, treatment, educational, career technology, law library and industrial programming purposes. The audit results will be used to remediate security gaps in inmate access to computers and computer parts.

ODRC has contracted with an experienced vendor for the disposal of ODRC staff and inmate computers and computer parts. The vendor will collect institution computers and computer parts that have reached the end of their life cycle, document and process the computers and parts pursuant to Ohio Department of Administrative Services (ODAS) and ODRC asset management policies and dispose of the computers and computer parts in a secure manner. This will ensure that ODRC inmates have very limited opportunities to access end of life computers and computer parts.

ODRC has allocated considerable resources to enhance the security of IT hardware and software used by inmates. 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 BITS Chief Information Security Officer (CISO), ODRC has taken a more systematic approach in identifying inmate information technology security vulnerabilities and interdicting, investigating and remediating data security incidents caused by inmates. More importantly, in partnership with the ODAS OIT, 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 this new network, inmate computers will be replaced with dedicated thin client devices that can only access the new inmate network. Deployment of the new inmate-specific network and new thin clients will significantly reduce inmate-related ODRC IT security vulnerabilities.

Recommendation #2:

ODRC's current table of organization has the institution investigator reporting directly to the warden. ODRC should consider having the institution investigator report to the Chief Inspector's Office instead of the warden to prevent any perceived conflict of interest or influence.

Response: An ODRC IT operational assessment completed by the Ohio Office of Budget and Management (OBM) independently reached a similar conclusion, noting in their observations that ODRC's IT operations are structured such that remote site information technology staff do not report through the central ODRC Bureau of Information Technology Services (BITS) management operational structure. The OBM assessment team noted that, "[h]aving a de-centralized operational structure for remote IT support staff increases the risk of misalignment between the remote site IT priorities and the BITS IT priorities and initiatives for DRC." The OBM assessment team further noted that ODAS's Office of Information Technology (OIT) is migrating shared services to a centralized model, as are other state agencies. The team emphasized that, "[i]mplementing a more centralized IT organizational structure, while at the same time retaining remote support staff, would reduce the risk that remote sites IT resources are misaligned with BITS IT initiatives and priorities." Like the Officer of the Inspector General, the OBM assessment team recommended that ODRC, "consider reassessing the appropriateness of the current IT operational structure for IT staff who do not report up through DRC BITS management. DRC BITS may consider evaluating the current IT Operational structure for possible enhancements to ensure alignment of remote IT staff priorities and initiatives with DRC BITS IT priority and initiatives." The OBM assessment team further recommended that ODRC consider, "centralizing the IT reporting structure for IT Support staff," which will ensure that remote site IT priorities and initiatives align with ODRC BITS IT priorities and initiatives."

ODRC is cognizant of the organizational and budgetary complexity of centralizing remote IT staff that have traditionally reported to institution managers. Nonetheless, ODRC is working to aligns remote site ODRC IT staff with ODRC BITS IT priorities and initiatives.

While ODRC appreciates the recommendation and its intended outcome, centralization is not deemed to be practical with institution investigators. However, we are confident our current table of organization can achieve the desired goal with enhancements to policy designed to foster more transparency and increased oversight by the Chief Inspector's office over institutional investigators and investigations initiated at the institutional level.

Additional oversight will be achieved by the Chief Inspector's Office, Regional Directors and Managing Directors with the implementation of an electronic case management system currently under development by our vendor, GTL. The system is expected to roll out and be fully implemented by the end of the year. Policy and procedure will require all institution investigations not related to minor time and attendance issues to be managed through this electronic system.

Recommendation #3:

ODRC should review with all employees the Governor's Policy and Procedure for Notification of Suspected Illegal or Improper Activity within State Departments and Agencies and incorporate it in ODRC policy.

Response: The Governor's Policy and Procedure for Notification of Suspected Illegal or Improper Activity within State Departments or Agencies was reissued to ODRC staff on July 24, 2015. Applicable ODRC policies have been updated with this directive. Going forward, the policy will be reissued annually as a reminder to ODRC staff.

Recommendation #4:

ODRC should provide and make available, or notify the Ohio State Highway Patrol of all incidents to eliminate failure to identify criminal violations.

Response: ODRC has updated and clarified language in applicable policies reinforcing the requirement to notify the Ohio State Highway Patrol of potential criminal violations. This notification requirement has been and will continue to be reinforced at executive staff meetings/trainings throughout the agency. ODRC is considering establishing a protocol to provide for the review of incident reports by the Troopers assigned to each institution.

Recommendation #5: ODRC should review with all employees and assure compliance with ODRC policy Information Technology Systems Password and Account Security 05-OIT-17 so that all employees have proper passwords and those passwords are changed, at a minimum, every 90 days.

Response: All ODRC online system users, including staff, contractors and volunteers, are required by ODRC policy, to complete IT security awareness training prior to receiving access to DRC online systems. In addition, ODRC online system users are required by ODRC policy, to complete supplemental IT security awareness training required by the ODRC BITS chief. The training ensures that ODRC online system users understand their IT security role and responsibility.

All ODRC online system users must acknowledge receipt of a standardized written admonition every single time they attempt to log into their ODRC domain user account. That admonition states in part:

> "[b]y using (including access and attempts to access) this State of Ohio government system, you acknowledge use of this system is governed by statute and policy, may be monitored, and that such use is for authorized purposes only. Any unauthorized or improper use of this system is strictly prohibited and may result in criminal or civil liability or disciplinary action. You have no expectation of privacy in any material placed or viewed on this system."

Importantly, a failure to mouse click and acknowledge the admonition automatically terminates the user's session access.

ODRC has centralized the issuance of user passwords for all systems and has automated user password resets for the agency's two primary online offender documentation and tracking systems. One system requires users to change their password in 60 days and the other system requires users to change the password in 90 days. In addition, all ODRC domain user passwords must be changed by system users every 90 days. ODRC's IT password reset standards facilitate basic security for ODRC's online systems.

Recommendation #6: ODRC should assure that inmates are not used in installing, operating, maintaining or servicing any information technology hardware, software or system assets. ODRC should assure that inmates no longer have access to computer hardware or wiping and imaging software.

Response: In furtherance of ODRC's Mission to, "reduce recidivism among those we touch," Ohio Revised Code and current ODRC policy limit inmate access to IT hardware and software to pro-social, treatment, educational, career technical, law library and industrial program purposes. Inmate access to IT hardware, software and system assets capable of accessing inmate, employee, victim, security, operational or any other sensitive or confidential ODRC information, data or records, including installing IT hardware and software, is strictly prohibited. When discovered, violations of this policy are investigated, staff and inmate violators receive appropriate sanctions and additional remediation actions are taken to address gaps in IT security. This policy will be reviewed with ODRC wardens at an upcoming managing officer meeting to ensure that all ODRC managing officers understand the policy requirements.

In addition, in 2015, at the request of ODRC, ODAS assigned a fulltime Chief Information Security Officer (CISO) to ODRC to serve as a direct link between the ODAS OIT and ODRC for purposes of providing technical governance of ODRC's facilities, data and information systems. The CISO has been invaluable in protecting ODRC IT assets 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.

Recommendation #7:

ODRC should review with all employees the Protection of a Crime Scene policy to assure compliance, reporting, and prevention of valuable evidence loss.

Response: ODRC, in consultation with the forensics unit of the Ohio State Highway Patrol has developed a policy governing the management of computer forensics. The Chief Inspector's Office will partner with the ODRC Office of Information Technology to provide training to computer techs on crime scene preservation at their annual meeting in June 2017.

The Chief Inspector's Office, in partnership with the Ohio State Highway Patrol has trained all institutional investigators in crime scene preservation. In addition, institution investigators will be tasked with conducting in-service trainings at their respective institutions on the DRC policy on crime scene preservation.

ODRC is reviewing policy requirements for crime scene preservation in consideration of developing internal management audit standards to help assess any vulnerabilities and ensure compliance.

Recommendation #8: ODRC should secure network cables, devices and servers to prevent access by inmates. ODRC should audit existing cable installations for vulnerabilities resulting from installation or configuration. Cable management documentation should be maintained and updated to identify any illicit cabling.

Response: ODRC will assess the IT remediation effort completed jointly by ODRC and ODAS OIT at the Marion Correctional Institution to determine, from an operational and resource standpoint, how the remediation effort can be duplicated, in whole or in part, at other ODRC institutions. While the remediation progresses, ODRC is moving forward, in partnership with ODAS OIT, with several hardware and software initiatives to strengthen the IT security posture of the ODRC staff network and, as noted previously above in response to Recommendation 1., reduce vulnerabilities arising from inmate access to IT assets by implementing a secure, inmate-specific network.

Recommendation #9: ODRC should conduct an inventory of all IT equipment at the Marion Correctional Institution to assure compliance with the State of Ohio Asset Management policy.

Response: ODRC will complete a comprehensive inventory of all IT equipment at the Marion Correctional Institution, to include all new networking infrastructure, when the ODAS OIT remediation effort is concluded.

Thank you for the opportunity to respond to your recommendations.

Sincerely,

Gary C. Mohr
Director