Ohio | Department of Rehabilitation & Correction

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

November 28, 2017

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

RE: IG File ID Number 2016-CA00005

Dear Inspector General Meyer:
This letter is in response to investigative file #2016-CA00005 submitted to the Department of Rehabilitation and Correction by your office on October 31, 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:

Disable the USB ports and CD drives on all computers accessed by inmates.

Response: Pursuant to *DRC Policy 05-OIT-11*, Inmate Access to Information Technology, DRC inmate access to information (IT) hardware and software is limited to pro-social treatment, educational, career technical, law library and industrial program purposes. The policy permits inmates to have limited access and use of storage media, such as CDs, CD-R discs, flash memory cards and USB jump drives in specific areas of the institution designated by Managing Officer or designee, provided the storage media is strictly controlled by the appropriate supervisor, the use of the storage media is documented by the appropriate supervisor via dedicated DRC Form *DRC1750, Sign-Out/Sign-In Log* and the log is reviewed at regular intervals by the managing officer or designee. As noted in the investigation, DRC currently utilizes a variety of automated software tools, such as *Websense*, to monitor compliance with IT security policies and procedures. As further noted in the investigation, when suspected violations of the IT security policies and procedures are detected, the suspected violations are appropriately reported and investigated and inmate and staff violators are held accountable for their actions.

Moving forward, DRC will strengthen the monitoring of *DRC Policy 05-OIT-11* through the Internal Management Audits conducted on an annual basis at all DRC institutions. A dedicated 2018 IT audit standard will require auditors to physically check and observe the areas in and around inmate computers for any storage media and, if discovered, the auditors must determine if the storage media is approved by the Managing Officer or designee, contains data required for the specific pro-social program being conducted by the institution in the area where the storage media was discovered, and is properly documented by DRC1750.

In partnership with the Department of Administrative Service, Office of Information Technology (DAS OIT) DRC has also invested significant resources to build a dedicated centralized and secure IT inmate data network

and purchase secure, thin client computing devices to replace existing DRC inmate computers. The existing inmate computers will be inventoried, removed from service and disposed of pursuant to DAS and DRC asset management policies and procedures.

The new network and their associated thin clients will be used exclusively by DRC inmates for pro-social treatment, educational, law library and industrial programming purposes. On November 13, 2017, DRC began to deploy the new network and the new thin clients at a test site institution. Once the testing is completed, deployment of the new network and thin clients will be initiated throughout the DRC enterprise.

Recommendation #2:

Review computer use policy with all employees.

Response: At the next quarterly Managing Officer Meeting, the DRC Chief Information Officer and DRC Managing Director of the Office of Prisons will present the findings of Investigation 2016-CA00005 and review *DRC Policy 05-OIT-11, Inmate Access to Information Technology*, and DRC *Policy 05-OIT-10, Internet, Electronic Mail and On-Line Services Use*, with all DRC Managing Officers in attendance. In addition, new language stating that DRC inmates / offenders are prohibited from using DRC staff computers will be added to the current written admonition that must be acknowledged by all DRC staff computer users in order to log on to DRC computers.

Recommendation #3:

Require staff members to change passwords regularly and never leave unlocked PCs unattended.

Response: DRC has taken specific steps to protect DRC data and DRC information systems. For example, DRC has automated a standardized 90-day password change process for user access to mission critical DRC online information systems. DRC also employs a standardized group IT policy that automatically terminates a user's computer session and, thus, logs the user off of their computer if the computer is inactive for 15 minutes. In addition, DRC utilizes a standardized, group IT policy that reboots all DRC computers on a designated day and time every week. Finally, in order to maximize the security of mobile DRC computing devices, such as laptops and PC tablets, DRC employs a group policy that disables mobile computing devices that do not register on the DRC data network at designated timeframes to download the required security software updates.

In addition to using automated IT tools, processes and procedures to protect DRC data, information systems and computing devices, DRC is in the process of updating DRC Policy 05-OIT-10, Internet, Electronic Mail and Online Services Use, in order to incorporate the security requirements mandated by DAS OIT in DAS OIT Policy 700-01, Information Technology Resource Usage.

Thank you for the opportunity to respond to your recommendations.

Sincerely,

Gary C. Mohr
Director