



Department of
Rehabilitation & Correction

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

2018 JUL 23 AM 10:10

July 20, 2018

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

RE: IG File ID Number 2016-CA00032

Dear Inspector, General Meyer:

This letter is in response to investigative file #2016-CA00032 submitted to the Department of Rehabilitation and Correction by your office on May 22, 2018, 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: Conduct a complete inventory of all IT equipment to bring MCI into compliance with ODAS Asset Management policy. All computers and computer components improperly acquired should be salvaged through ODAS State Surplus and documentation of such provided to the Office of the Ohio Inspector General.

Response: An inventory of all IT equipment at MCI was completed by Operation Support Center and MCI staff by February 20, 2018. In order to monitor ongoing compliance with the ODAS Asset Management inventory policy, an IT equipment inventory quality assurance process was initiated at MCI. Institution IT staff are working closely with fiscal and warehouse staff to ensure all assets are being captured. Improperly acquired computer components and surplus equipment will be salvaged pursuant to the applicable ODAS State Surplus policies and procedures.

In addition, in December 2017, ODRC removed personal computers in the MCI library, used by inmates to conduct legal research, and replaced them with new, secure thin client computing devices attached to the centralized, highly secure inmate network. In May 2018, ODRC installed the new, secure thin clients, which are also attached to the secure centralized network, in inmate educational / vocational areas at MCI. These devices also replaced inmate personal computers in these areas.

Lastly, ODRC is in the process of completing a security-specific policy that focuses on the control of inmate computers and storage media.

Recommendation #2: Assure that inmates are not used in installing, operating, maintaining, or servicing any information technology hardware, software or systems assets. ODRC should assure that inmates no longer have access to computer hardware or wiping and imaging software.

Response: ODRC Policy 05-OIT-11, Inmate Access to Information Technology, will be revised, as necessary, to emphasize that inmates are prohibited from accessing, installing or using any wiping or imaging software and are prohibited from installing, operating, maintaining, or servicing any ODRC or inmate information technology hardware, software or system assets. In addition, the policy will be revised to emphasize that inmates are permitted to have access to computer hardware only for pro-social, treatment, educational, career technical, law library and/or industrial program purposes and only when under the *direct supervision* of ODRC staff members or other authorized individuals. For the purposes of the policy, *direct supervision* is defined as, “the frequent, nonscheduled, direct and unimpeded personal observation and contact between one or more ODRC staff members or other authorized individuals and inmates using authorized computing devices.”

In July 2016, the DRC leadership was notified by DRC’s Chief Information Officer that DRC would no longer accept donated computers, tablets, iPads, etc. for inmate use. In addition, the DRC leadership was advised that new DRC computers, as well as DRC computers identified for disposal and salvage, would no longer be assigned to inmates. These prohibitions will also be inserted into ODRC Policy 05-OIT-11.

In addition to making these policy revisions, ODRC will continue to audit ODRC institutions for compliance with ODRC Policy 05-OIT-11. The policy and the internal management audit results that focus on assessing compliance with the policy will be reviewed with all ODRC Managing Officers and all IT staff members. This will ensure that the ODRC leadership and the ODRC IT staff members that support and maintain ODRC staff and inmate IT system assets in the institutions understand the importance of adhering to ODRC Policy 05-OIT-11.

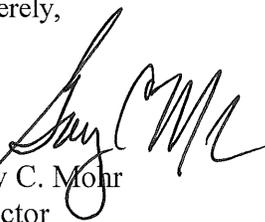
ODRC is proud of its long and fruitful relationship with the American Correctional Association, a national organization that, for 147 years, has championed the cause of corrections and the effectiveness of correctional practices. In recognition of ODRC’s information technology efforts, the American Correctional 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.

Recommendation #3: Assure that all ODRC employees involved in the acquisition of IT equipment comply with the statewide ODAS IT Policy Office requirements.

Response: ODRC Policy 22-BUS-11, Internal Control of Fiscal Activity, establishes training requirements for, “...specific ODRC employees who process and/or approve Business/Cashiers’ Office transactions through the agency’s appropriated and/or non-appropriated funds...”. Those employees who work in a business or cashier role are required to complete “Overview of Business” within six months of hire date or and every training cycle. This course includes information on the ODAS IT and procurement requirements. The material will be updated to directly cover this issue.

Thank you for the opportunity to respond to your recommendations.

Sincerely,


Gary C. Mohr
Director