

STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL

RANDALL J. MEYER, INSPECTOR GENERAL

REPORT OF
INVESTIGATION



AGENCY: OHIO DEPARTMENT OF REHABILITATION & CORRECTION
FILE ID NO.: 2016-CA00005
DATE OF REPORT: OCTOBER 31, 2017

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: 2016-CA00005

SUBJECT NAME: Chad Hider
Robert Rumack

POSITION: ODRC Teacher 1
Inmate

AGENCY: Ohio Department of Rehabilitation and Correction

BASIS FOR INVESTIGATION: Agency Referral

ALLEGATIONS: Failure to Exercise Adequate Oversight of Agency/
Departmental Functions/Activities

INITIATED: January 28, 2016

DATE OF REPORT: October 31, 2017

INITIAL ALLEGATION AND COMPLAINT SUMMARY

On January 28, 2016, the Office of the Ohio Inspector General initiated an investigation after receiving information from the Ohio Department of Administrative Services (ODAS), Office of Information Technology (OIT) about possible wrongdoing at the Richland Correctional Institution (RiCI). On January 4, 2016, the Ohio Department of Rehabilitation and Correction (ODRC) had received a Websense¹ alert notifying officials that RiCI employee Chad Hider's user identification had been used to attempt to log into a proxy avoidance website².

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. 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.³

Ohio Central School System

In April 1973, under Ohio Revised Code §3313.61, the Ohio Department of Education formally chartered the Ohio Central School System (OCSS). This charter and the school system it established enables ODRC to provide comprehensive educational programs that address the needs of under-educated and under-skilled inmates. These services include: Adult Basic Literacy Education (ABLE), high school equivalency (GED[®]), high school options, apprenticeship training, library services, release preparation, special education, Career-Technical Education (CTE), Transitional Education Program (TEP), Youth Transition Program (YTP),

¹ Websense is a computer security software.

² Proxy avoidance websites allow users to bypass the browsing restrictions that are placed on a network.

³ Biennial budget documents.

Education Intensive Program Prison (EIPP), and other educational programs. Additionally, OCSS has the authority to seek additional funding from the federal government.

Websense

Websense is a computer security software used by businesses and government institutions to protect their networks from cybercrime, malware, and data theft. The software also prevents users from viewing sexual or other inappropriate content, and discourages employees from browsing non-business-related websites. Websense uses a combination of classification engines, filtering categories, data fingerprints, and word filters designed by the individual customer's network policy.

ODRC Inmate Access to Information Technology policy 05-OIT-11 states, in part;

Inmates are strictly prohibited from; accessing any hardware, software or system assets that are part of a LAN or WAN system used in the administrative operations of the Department or to access the internet or Department intranet.

ODRC Internet, Electronic Mail, and Online Services Use policy 05-OIT-10 VI.G 2 states, in part;

Employees and other individuals with DRC system asset accounts, such as the internet, electronic mail, online services, and the VPN, shall not:

- g. Use their DRC accounts for recreational purposes such as downloading or playing computer games, gambling, or to send, distribute or solicit sexually oriented messages, materials or images.
- i. Use their DRC accounts to download or order non-DRC software, software service packs, or software updates to any State of Ohio owned or leased computer, peripheral device, communication line or network.

Ohio Department of Administrative Services Office of Information Technology

The Office of Information Technology (OIT), a division of the Ohio Department of Administrative Services, is responsible for establishing policies and procedures regarding the purchase, use, and security of computer hardware and software in use by state agencies. The office is overseen by a

state chief information officer appointed by the director of the Ohio Department of Administrative Services. All state agencies, excluding the elected officials, are subject to the rules and standards issued by OIT.

INVESTIGATIVE SUMMARY

On January 4, 2016, the ODRC Bureau of Information Technology and Security (BITS) received a Websense alert indicating that an attempt had been made to log into a website categorized as a proxy avoidance, and the attempt had been blocked. A proxy or proxy server operates as a hub through which internet requests are processed. Network administrators can apply proxy filters to impose browsing restrictions, which limit a user's ability to access predefined websites. Proxy avoidance websites simply allow users to bypass the browsing restrictions that are set onto a network. ODRC BITS determined that the user identification of the individual who was logged onto the computer from where the attempt was made was Chad Hider, a teacher in the basic education area at Richland Correctional Institution (RiCI). ODRC BITS forwarded this information to the ODRC Chief Inspector's Office for review.

The ODRC Chief Inspector's Office then notified the warden at RiCI and ODRC Infrastructure Specialist 2 Derek Green of the Websense alert. The chief inspector's notification included the following information:

Hacking sites are viewed as potential threats against DRC's network and technology assets. There are many web sites on "how to hack." BITS blocks all web sites that relate to Hacking. Websense Alerts are sent directly to our Network Security Team for each "attempt" to view a Hacking web site. One attempt will trigger an alert, and BITS will contact the Chief Inspector's office to let the institution know. Proxy Avoidance sites are simply sites that advise users how to avoid proxy servers. The proxy is what blocks inappropriate or malicious web sites so some users try to find a way around it. Both of these types of sites can have "false positives." As such, BITS staff does a cursory review of the site(s) before sending the alerts.

ODRC Infrastructure Specialist Green told investigators that Hider had repeatedly denied visiting the website that caused the Websense alert. Green also said he knew that Hider's

teaching assistant, inmate Robert Rumack, had been previously investigated for possible computer security breaches. Subsequently, Green inspected the ODRC computer assigned to Rumack, and discovered a second hard drive had been installed in the device. Green removed both hard drives from Rumack's computer and the hard drive from the computer assigned to Hider, and forwarded the drives to the Ohio Department of Administrative Services (ODAS), Office of Information Technology (OIT). On January 28, 2016, the Office of the Ohio Inspector General initiated an investigation after receiving this information from ODAS OIT. The Office of the Inspector General obtained, for analysis, images of the two hard drives installed in Rumack's ODRC-assigned computer and the hard drive installed in Hider's ODRC-assigned computer.

On February 2, 2016, ODRC BITS provided to the Office of the Ohio Inspector General additional Websense alerts from Hider's computer. The Websense protocol was established on October 15, 2015. The Websense alerts history for Hider's computer indicated three alerts categorized as "Hacking." Each of these alerts were reviewed by investigators to determine if the sites that were being accessed were either incorrectly categorized or actual "Hacking" sites. Investigators later determined that these three alerts did not involve hacking sites. There were 15 alerts from Hider's computer for "Custom-encrypted Uploads" (YouTube), and one alert for sexual content. Each of these sites had been blocked.

Prior to the Websense alert for a proxy avoidance site, Hider's ODRC-assigned computer was also used to access numerous "YouTube" sites. On January 4, 2016, at 1:21:23 p.m., someone on Hider's computer attempted to access the website www.chris-pc.com/download.html. However, Websense identified the website as a proxy avoidance site. The "chris-pc" is a software application created for fast downloading of files and software, and is used to convert YouTube videos to high quality MP3 audio files. The "chris-pc" website claims that it secures the user's privacy while connected to the internet by anonymizing all TCP/IP⁴ traffic. Websense blocked access to this site from Hider's computer. Eleven seconds later, at 1:21:34 p.m., there was an attempt from Hider's computer to access www.vevodownloader.html, a YouTube video

⁴ TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the internet.

downloading site. Access to the site was initially blocked; however, it was not identified as a proxy avoidance site, and Websense permitted a second access attempt at www.vevdownloader.html.

Hard Drive Analysis

The Office of the Ohio Inspector General conducted a forensic analysis of the hard drive found in Hider's ODRC-assigned computer, which revealed numerous internet accesses to sports-related sites, including ESPN and fantasy football sites. Also, attempts to access Facebook and Twitter sites were blocked by Websense. The forensic analysis determined that Hider's computer contained software that had been downloaded and installed for copying and producing videos from the internet, and software designed to remove trace evidence of software and files from the computer's operating system history. Additionally, the forensic analysis found trace evidence indicating that approximately 15 software programs were downloaded and installed from January 1, 2015, until January 28, 2016. One of these programs was designed to obscure the network address identification and enabled secure tunneling, to prevent detection when using downloaders and torrents.⁵

Investigators also conducted a forensic analysis on the hard drives from Rumack's ODRC-assigned computer. Rumack's computer contained two hard drives: one hard drive (HD1) that enabled his assigned computer for use when executing his duties as Hider's assistant, and a second hard drive (HD2) concealed inside the computer, which was discovered by ODRC Infrastructure Specialist Green. Forensic analysis determined that from time to time, the computer had been reconfigured to work alternately between the HD1 drive and the HD2 drive.

Software that was downloaded and installed on Hider's computer was also installed on both the HD1 and HD2 hard drives of Rumack's ODRC-assigned computer. The software that was

⁵ A torrent is a file sent via the BitTorrent protocol. It can be just about any type of file, such as a movie, song, game, or application. During the transmission, the file is incomplete and therefore is referred to as a torrent. Torrent downloads that have been paused or stopped cannot be opened as regular files, since they do not contain all the necessary data. However, they can often be resumed using a BitTorrent client, as long as the file is available from another server.

installed on both HD1 and HD2 enabled Rumack's computer to be used to produce video and music files in various file formats for distribution. Additionally, pornographic video files, television programs, and thousands of music files were identified on the HD2 hard drive on Rumack's computer; and trace internet history connected to softcore pornography websites and television programs were identified on Hider's computer.

The analysis of the two hard drives from Rumack's computer revealed the HD1 hard drive showed 253 logins as "voc," between June 17, 2015, and January 13, 2016. This hard drive also contained 4,614 music files and various football-related files, including one titled "Mr. Hiders Fantasy Football." The analysis of the HD2 hard drive indicated 163 logins as "Administrator" and 593 logins as "Student" between July 22, 2015, and January 21, 2016. This hard drive also contained 4,670 music files and 33 pornographic movies.

The analysis also revealed evidence of USB storage device activity on the hard drives obtained from both Hider's and Rumack's ODRC-assigned computers. In particular, investigators discovered that a single USB storage device had been used on all three hard drives. *ODRC Inmate Access to Information Technology* policy 05-OIT-11 states, in part, that inmates are prohibited from, "... receiving, possessing or using any storage media, which is contraband, outside of the specific areas designated by the managing officer/designee." ODRC officials indicated that the department neither authorized nor issued Hider the use of a USB storage device.

Interviews

On November 10, 2016, investigators conducted separate interviews with inmate Robert Rumack and ODRC Teacher 1 Chad Hider. During Rumack's interview, he denied to investigators either accessing Hider's computer or transferring any material from Hider's computer to his computer. Rumack stated that he created the "fantasy football stuff" on his computer with the statistics provided to him from Hider, and that the information was not transferred from Hider's computer. Rumack explained that Hider would obtain the statistics of football players on his (Hider's) computer, and he (Rumack) would write the information on paper and then enter these statistics

onto his computer. Rumack noted the football statistics were used during math classes to create math problems for students.

Rumack admitted to investigators that he knew there were two hard drives in the ODRC-assigned computer he used. Rumack said that the original hard drive (HD1) contained a program that was not compatible with the program used by Hider in a class, so the second hard drive (HD2) was installed by RiCI Information Technology personnel. Rumack also admitted transferring music from compact discs onto the computer assigned for his use, but denied knowing about or downloading pornography onto his computer. Rumack noted that although the ODRC computer was assigned to him, other inmates could access the device. Rumack denied accessing Hider's computer.

During his November 10, 2016, interview, Chad Hider informed investigators that he taught general education courses and had limited computer skills. Regarding his computer, Hider said, I don't know how to use them, other than for my job. Looking up DOTS stuff or as uh --- and stuff for my job... I know Rumack's a lot more knowledgeable on computers than me. Whether he did something or not, like I said, I was not privy to it.

Hider said his internet access is used for research for class material and noted that he used football statistics to create math problems for the classes he teaches. Hider also admitted to investigators that he used YouTube videos in his class, saying,

Yeah, I show YouTube videos for uh my class, like history stuff. I mean science, health, weather. I mean ... --- and that's the one that says that continue, you got 180 minutes a day to use and stuff like that. Like I said, I got three hours to kill time and there's not a lot of work in the, the, the time we have to give them without them going nuts. So I try to use whatever I can as far as --- I mean videos are --- some people learn from that stuff. Whether it's World War II or a tornado hitting Alabama or something like that.

Hider stated he was unaware that Rumack's computer had two hard drives, and contained music and pornography files.

During discussions with ODRC Network Services Supervisor Linda Diroll, she told investigators that Hider was permitted to access YouTube sites for 180 minutes per day. Diroll said Websense allows this access when an authorized user opens YouTube.com and clicks on the “Use Quota Time” to start a 60-minute session for viewing the site and other sites in quota-limited categories. Diroll explained that the 60-minute “clock” continues to elapse whether the user chooses to play a video or not. Should a user close the YouTube.com browser within that 60-minute session, the 60-minute time period continues to elapse. Diroll added that a user can reopen the YouTube.com browser within that 60-minute session and watch videos without being re-prompted to use an additional “quota time.” However, after 60 minutes has elapsed, “Use Quota Time” will prompt the user to approve the use of another 60 minutes of quota time to continue. Diroll noted that Hider would not be permitted to access social networking sites like Facebook or Twitter, and that Hider’s profile listed his access to the USB port as “disabled.”

On March 28, 2017, investigators conducted a second interview with Chad Hider. Hider again denied that he had attempted to access a proxy avoidance site or downloaded any software programs. Hider also denied giving his computer password to Rumack but speculated that because their desks were close together, Rumack could have observed his password being entered when Hider was signing on to his ODRC-assigned computer. Hider admitted to investigators that he had left the classroom unattended while inmates were in the room. Hider said Rumack did have access to compact disks, and that both their computers had functioning USB ports and CD drives.

CONCLUSION

On January 4, 2016, the ODRC Bureau of Information Technology and Security (BITS) received a Websense alert indicating that an attempt had been made to log into a website categorized as a proxy avoidance, and the attempt had been blocked. ODRC BITS determined that the user identification for the individual logged onto the computer where the attempt was made was Chad Hider, a teacher in the basic education area at Richland Correctional Institution (RiCI). The blocked website provided users access to a software application used to anonymously and quickly download files and software, and convert YouTube videos. ODRC permits authorized

employees access to YouTube sites for three hours-a-day, and Hider used videos from YouTube as part of the general education courses he provided to inmates. Hider repeatedly denied to ODRC that he had accessed the blocked proxy avoidance website. Inmate Robert Rumack, who assisted Hider, had a history of computer misuse at ODRC. As part of ODRC protocol, the RiCI administration was advised of the Websense alert and the matter was referred to the ODRC Chief Inspector's Office. On January 28, 2016, the Office of the Ohio Inspector General initiated an investigation into the matter.

ODRC IT inspected both Hider's and Rumack's ODRC-assigned computers. ODRC IT discovered that a second hard drive (HD2) had been installed within Rumack's computer. The Office of the Ohio Inspector General conducted a forensic analysis on all three hard drives obtained from both Hider's and Rumack's computers. Investigators discovered software had been downloaded on numerous occasions onto both Hider and Rumack's computers. One of the programs that was downloaded and installed was designed to obscure the network address identification and enable secure tunneling to prevent detection when using downloaders and torrents. Additionally, investigators found pornographic video files, television programs, and thousands of music files on Rumack's HD2 hard drive; and trace internet history indicating downloads of softcore pornography and television programs on Hider's computer.

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

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) Disable the USB ports and CD drives on all computers accessed by inmates.
- 2) Review computer use policy with all employees.

- 3) Require staff members to change passwords regularly and never leave unlocked computers unattended.

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 & Correction

FILE ID #: 2016-CA00005

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
October 31, 2017

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