STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL

RANDALL J. MEYER, INSPECTOR GENERAL

REPORT OF INVESTIGATION

AGENCY: OHIO DEPARTMENT OF REHABILITATION AND CORRECTION
FILE ID NO.: 2015-CA00043
DATE OF REPORT: APRIL 11, 2017

The Office of the Ohio Inspector General ...
The State Watchdog

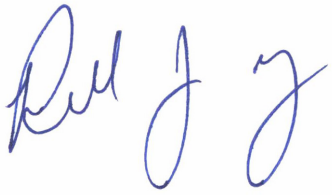
"Safeguarding integrity in state government"

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:	2015-CA00043
SUBJECT NAME(S):	Adam Johnston; Karen Gallienne; Jason Bunting; Carl Brady; Randall Canterbury.
POSITION(S):	Inmate, Marion Correctional Institution (MCI); Inmate Johnston's Mother; Former Warden, MCI; Infrastructure Specialist 2, MCI; Former Training Officer, MCI.
AGENCY:	Ohio Department of Rehabilitation and Correction
BASIS FOR INVESTIGATION:	Complaint
ALLEGATIONS:	Failure to Comply with State Law and/or Regulations
INITIATED:	August 19, 2015
DATE OF REPORT:	April 11, 2017

INITIAL ALLEGATION AND COMPLAINT SUMMARY

On August 7, 2015, the Ohio Department of Rehabilitation and Correction (ODRC) notified the Office of the Ohio Inspector General that on July 27, 2015, Marion Correctional Institution (MCI) staff had discovered two unauthorized personal computers hidden on a plywood board in the ceiling above a closet in a training room. The two computers were connected to ODRC's computer network and were not owned by the State of Ohio.

BACKGROUND

Ohio Department of Rehabilitation and Correction

The Ohio Department of Rehabilitation and Correction (ODRC) 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.[1]

Marion Correctional Institution (MCI) is located in Marion County and houses approximately 2,500 primarily medium security inmates. MCI operates several programs to educate or provide service to the community. One of those programs is the MCI Green Initiative which is an offender group that was created to foster conservation and green practices throughout MCI. The group formed approximately five years ago to revamp the institution's trash and recycling processes. From those initial efforts, other projects were added, including: a community garden which donates 90 percent of its produce to local food pantries; an aquatics program that breeds ornamental fish for sale to the community and feeder fish to local pet stores; RET3 which employs offenders to disassemble out-of-date computer hard drives and other obsolete technology items (such as VCRs, analog phones, etc.); and education programs, such as Roots

[1] Source: Biennial budget documents.

for Success, which teach conservation and green practices. The organization has worked with or partnered with local recyclers, specifically: Delaware/Knox/Marion/Morrow Solid Waste Authority, The Ohio State University Marion/Marion Technical College, Ohio Department of Natural Resources, and The Wilds. The Green Initiative employs approximately 120 offenders, most of whom perform work in recycling, trash management, food service, and RET3.

Green Initiative

The Green Initiative is operated under the administration of inmates known as the Executive Committee. During the investigation, the Executive Committee was comprised of five inmates: Stanislov Transkiy, executive committee chairman of recycling; Leeshan McCullough, chairman of aquaculture; Robert Cooper, chairman of horticulture; Matthew Brown, chairman of environmental education; and Adam Johnston, executive committee treasurer. The responsibilities of the Executive Committee include the hiring and firing of inmates who work in one of the programs, and the authorization to purchase items for the Green Initiative. **(Exhibit 1)**

RET3

RET3 is a non-profit agency located in Cleveland, Ohio dedicated to the environmentally responsible disposal of end-of-life electronic equipment. RET3 utilizes a combination of remanufacturing, reuse, and recycling techniques to provide an efficient means for the disposal of electronic waste. In August 2014, MCI entered a contract with RET3 to provide inmate labor to disassemble old computers. Specifically, RET3 collects unwanted computers, delivers the computers to MCI for the inmates to disassemble into basic parts, and returns the separated parts to RET3 for processing.

Randy Canterbury was a contract employee who had oversight of all Green Initiative operations, including RET3. Previously, Canterbury was a long-time ODRC employee. At ODRC, Canterbury held the position of training officer/Green Initiative advisor and his office was located on the third floor of the administration building in the training room. On May 30, 2015, Canterbury retired from ODRC and on June 1, 2015, Canterbury was hired by RET3.

Lifeline

According to former MCI Warden Jason Bunting, the Lifeline program is a space for healing and learning, through programs provided by Healing Broken Circles. Five areas of service address the needs and aspirations of the whole person:

- Turning Professional provides workforce development and job readiness.
- True Potential attends to personal growth in people and interconnections in the community.
- Thinking People creates opportunities for advanced and continuing education.
- In Thriving Path, men learn to care for minds, bodies and spirits.
- Talented Performers makes arts and creativity part of growth and development. All programming is strength-based and focused on belonging, mastery, independence and generosity, four characteristics of a healthy person. Trained and experienced resident aides and volunteers, supervised by HBC contractors, facilitate learning in subjects from Spanish to philosophy, digital arts to mediation, improv to java, and music theory to Microsoft office applications.

Lifeline participants also have many opportunities to develop appropriate social skills and confidence as they interact with the outside community through events such as TEDxMarionCorrectional and Generation Why. Outside professional and collegiate volunteers bring perspectives on education, business, and current issues. Programming provided in Lifeline is open to any offender who desires to participate, to be accountable for himself and his learning, and to focus on his growth and potential.

ODRC Policies

The following policies and Ohio Revised Code sections were reviewed as part of the investigation:

ODRC policy *Information Technology Systems Password and Account Security 05-OIT-17* states, in part:

> User passwords for DRC information technology systems shall meet or exceed the following security standards:

- Minimum of eight (08) characters in length;
- Contain at least one upper case letter;
- Contain at least one special character (e.g. !,@, #, $, %, ^, &, *);
- Not contain personal user identifiers (e.g., SSN, DOB, telephone number, part of a user name).
- DRC information technology systems that can automatically compel employee or contractor users to change their individual passwords shall be configured to compel password changes every 90 days.
- In addition, they [employees] are prohibited from displaying their unique, individual usernames and passwords where others may view them.

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

Inmates are strictly prohibited from:

1. Specifying, designing, purchasing, installing, operating, maintaining or servicing any information technology hardware, software or system assets that are used in the administrative operations of the Department (e.g., count sheets, pass lists, bed rosters, any confidential or sensitive data, any security related information, etc.).
2. Receiving or possessing any technical documentation, in any format, that describes the handling, functionality and/or architecture of information technology hardware, software or system assets pertaining to the administrative operations of the Department.
3. Receiving or possessing any technical documentation, in any format, that provides information or instructions on exploiting weaknesses in a computer system or network.
4. Receiving, possessing or using any hardware or software NOT specifically designated for pro-social, treatment, educational, career technical, law library or industrial program purposes approved by the Managing Officer.
5. 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 policy *Protection of a Crime Scene 310-SEC-13* states, in part:

> It shall be the policy of the Ohio Department of Rehabilitation and Correction to preserve all suspected crime scenes and notify the Ohio State Highway Patrol of any suspected crime occurring on institutional property or other Department of Rehabilitation and Correction facilities. The investigator and/or shift supervisor shall promptly notify the local Ohio State Highway Patrol Post and communicate the following:
>
> 1. Detailed description of the incident and time of occurrence;
> 2. Names of employees, visitors and/or inmate(s) involved;
> 3. Any injuries or property damage; and
> 4. Action taken to preserve the crime scene.

ODRC policy *Special Investigations 09-INV-03* states, in part:

> Investigations of incidents that are already known or suspected to be criminal in nature shall not be initiated by the Department's officials unless the Ohio State Highway Patrol is aware of the nature of the incident and has granted the Department consent to conduct an administrative investigation. Investigations that uncover suspected criminal activity shall be halted pending notification and consent of OSHP to continue.

Policy and Procedures for Notification of Suspected Illegal or Improper Activity within State Departments and Agencies

The Governor's Office issued a policy and procedure, titled *Policy and Procedures for Notification of Suspected Illegal or Improper Activity within State Departments and Agencies*, to be followed when illegal or improper activity by any state employee or official is observed, suspected, or reported:

> The Chief Legal Counsel for the Department and/or the Department Director shall promptly provide the information to (a) the Chief Legal Counsel for the Governor (or his designee), (b) the State Highway Patrol Office of Investigative Services and (c) the Ohio Inspector General (or his designee). **(Exhibit 2)**

Office of Information Technology

The Office of Information Technology (OIT), a division of the Ohio Department of Administrative Services (ODAS) 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 ODAS. All state agencies, excluding the elected officials, are subject to the rules and standards issued by OIT.[2]

Section 125.16 of the Ohio Revised Code requires ODAS to maintain current inventory records as submitted and certified by state agencies consisting of owned tangible personal property and real property (including land, land improvements, buildings, and infrastructure). The State of Ohio Asset Management Handbook directs that:

> Agencies shall maintain current and accurate inventory records and related activity for all the following Computing and Information Technology (IT) Equipment, including but not limited to desktop computers, laptops, notebooks, servers, and personal digital assistants (PDAs); including but not limited to palm pilots, blackberries and smartphones; received March 1, 2008 and after regardless of acquisition cost or donated market value at time of donation.[3]

Websense

Websense, now renamed Forcepoint, is a company specializing in computer security software. Businesses and government institutions use its security solutions to protect their networks from cybercrime, malware and data theft, as well as to prevent users from viewing sexual or other inappropriate content. It is also used to discourage employees from browsing non-business-related websites.

---

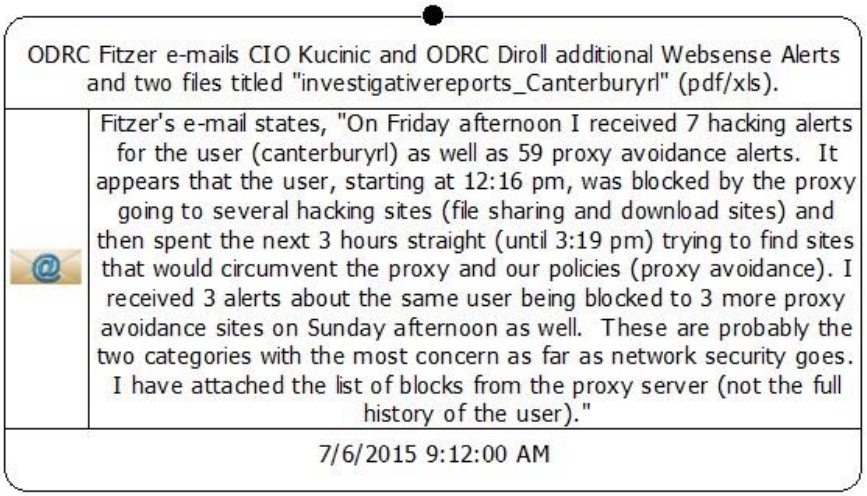
[2] Source: Ohio Revised Code §125.18 - The elected officials include the Ohio Attorney General, Auditor of State, Secretary of State and Treasurer of State.

[3] State of Ohio Administrative Policy, *Asset Management AM-01.* (Page 15)

Sometime between June 22, 2015, and July 3, 2015, ODRC IT began migrating MCI from the Microsoft proxy servers[4] to the Websense proxy server to improve performance and reporting and gain greater control over internet traffic.

INVESTIGATIVE SUMMARY

On Friday July 3, 2015, ODRC Operation Support Center (OSC) employees received a Websense e-mail alert reporting that a computer operating through the ODRC computer network had exceeded a daily internet usage threshold. This alert reported that Randy Canterbury's ODRC log-in credentials were being used on the computer in question. Canterbury is a retired ODRC employee[5] and a current contract employee for RET3 working at MCI. There were additional alerts indicating attempts to avoid ODRC network controls on Saturday July 4 and July 6. The following email is from ODRC IT employees to the ODRC Chief Information Officer (CIO) Vinko Kucinic:

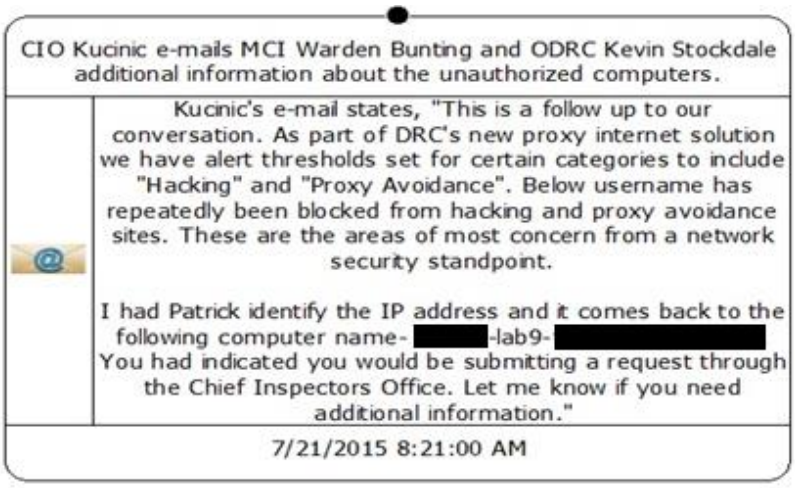


Canterbury's work week is Monday through Thursday which led ODRC to believe that Canterbury was not the individual making the attempts to avoid network controls (proxy avoidance) and that another person was using Canterbury's log-in credentials. The next email between ODRC IT employees regarding Websense alerts occurred on Friday July 17, 2015, again identifying Canterbury's log-in credentials being used from an ODRC IP address attempting to access proxy avoidance sites. ODRC IT employees identified both the computer's

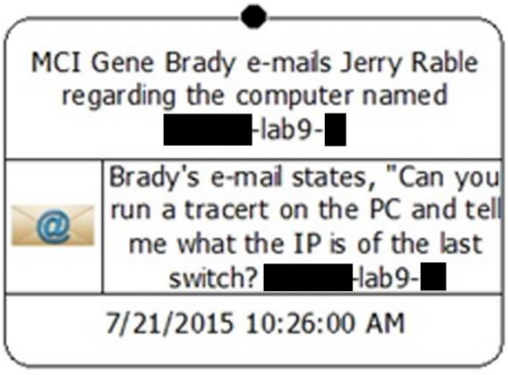
[4] Proxy server - A computer system that facilitates the exchange of data between users on a network.
[5] Effective May 30, 2015.

name (lab9)[6] and IP address. ODRC IT employees determined this computer was unauthorized because part of its computer name, "-lab9-," fell outside of the numbers assigned to the six known computers used in the PC training area. According to a forensic analysis performed by Ohio Department of Administrative Service (ODAS), Office of Security and Privacy, the computer's operating system was installed on April 1, 2015.

On July 21, 2015, Kucinic sent an email to MCI Warden Jason Bunting[7] updating him about the unauthorized computer being used at MCI.

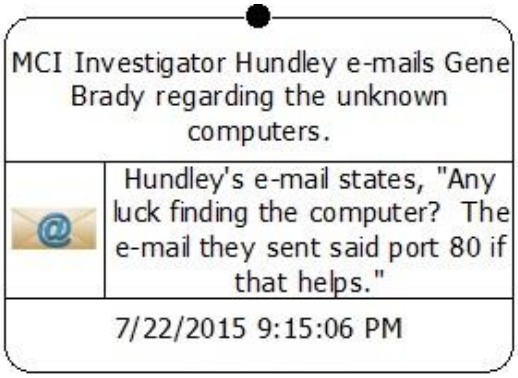


An email from MCI Infrastructure Specialist 2 Carl (Gene) Brady to ODRC IT employees indicated that he was aware of the unauthorized computer and was attempting to locate the network switch that the unauthorized computer was connected into. Brady has worked for ODRC since November 1994, and is responsible for IT support at MCI.

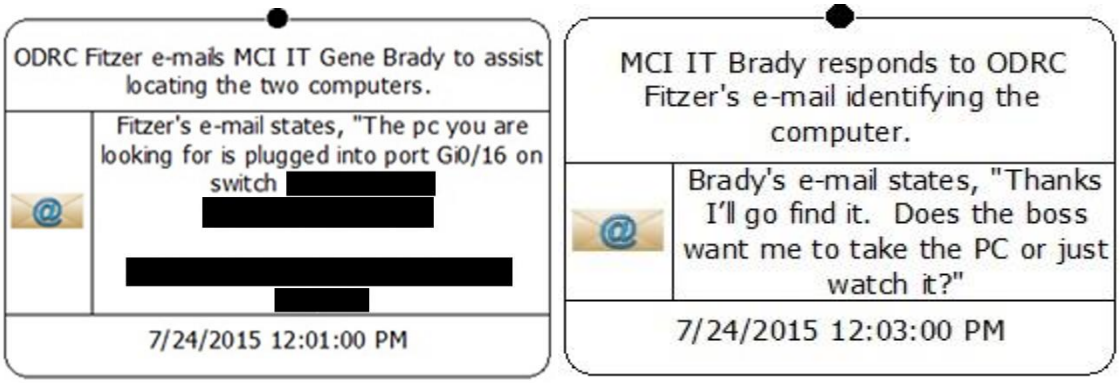


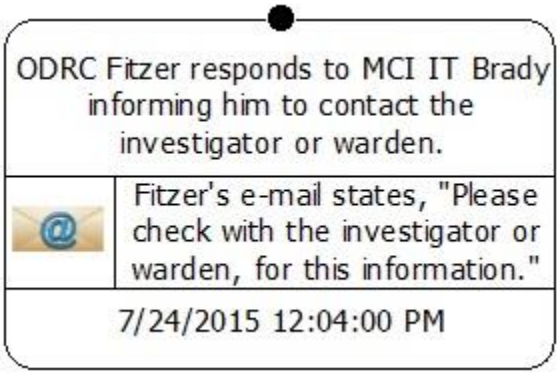
[6] Due to security concerns, the computer's name will be referred to as "lab9" in this report of investigation.
[7] Jason Bunting resigned his position as warden at MCI and is currently the superintendent of the Northwest Ohio Development Center.

On July 22, 2015, MCI Investigator Michael Hundley emailed Brady concerning the unauthorized computer, indicating he was aware of its existence.



On Friday July 24, 2015, ODRC IT employee Patrick Fitzer emailed Brady, identifying that the switch the unauthorized computer was plugged into was located in the P3 training room. The P3 training room was the same room that had been used as an office for Randy Canterbury when he had worked as a training officer for ODRC.





On Monday July 27, 2015, Brady created an incident report informing that he had located two unauthorized computers. Brady stated,

> On the above date and time I was following up on information received from OSC IT department. I had been told there was a PC on our network that was being used to try and hack through the proxy servers. They narrowed the search area down to the switch in P3 and the PC was connected to port 16. I was able to follow the cable from the switch to a closet in the small training room. When I removed the ceiling tiles I found 2 PC's hidden in the ceiling on 2 pieces of plywood.

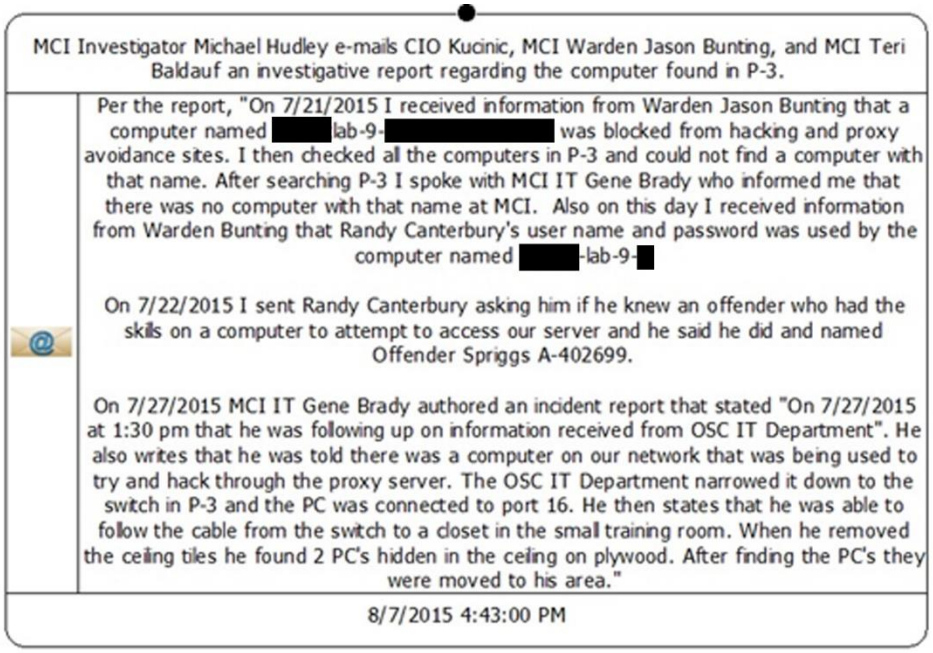
Brady had the two unauthorized computers removed from the ceiling.

On Wednesday July 29, 2015, Brady emailed Bunting, Kucinic, and Hundley and asked, "What do you want me to do with the PC's?" Kucinic replied and directed Brady to call him the next day to discuss the matter and make arrangements.

On Thursday July 30, 2015, Brady emailed Kucinic, telling him that he was coming to ODRC headquarters that day and that he could bring the computers with him. Kucinic emailed back and replied, "Yes please." Brady delivered the computers on July 30, 2015.

On Friday July 31, 2015, ODAS OIT Chief Information Security Officer Nathan Norris[8] emailed Kucinic and informed him that the two computers had identification placards: one computer indicated as being the property of Shaker Heights City Schools and the other computer indicated a business named Parker Hannifin Corporation, Wheel & Brake Division located in Avon, Ohio. On Friday August 7, 2015, Hundley created an incident report and emailed it to Bunting describing his investigation of the two non-State of Ohio computers found hidden in the ceiling of the P3 training room.

[8] Norris is an ODAS OIT employee assigned to monitor the ODRC IT network.



On August 7, 2015, ODRC Chief Counsel Stephen Gray issued a Notification of Employee Suspected Illegal Activity to the Office of the Ohio Inspector General and the Ohio State Highway Patrol (OSHP).

On August 10, 2015, the OSHP Computer Crimes Unit (CCU) took possession of the two computers from ODRC and began imaging the hard drives. The Office of the Ohio Inspector General acquired copies of the two imaged hard drives from CCU to analyze the data on the two drives. The Office of the Ohio Inspector General was tasked with locating evidence of criminal conduct and ODAS OIT was tasked with identifying hacking tools and software installed on the computers.

Forensic Analysis Completed by the Office of the Ohio Inspector General

From its forensic analysis of the two hard drives, the Office of the Ohio Inspector General determined that the computers had been used for the following activity:

- Searches of inmate information through the ODRC Departmental Offender Tracking System (DOTS), including a search conducted on Kyle Patrick, an inmate housed at the Mansfield Correctional Institution (ManCI) since June 26, 2014. Prior to his incarceration, Patrick resided in Youngstown, Ohio.

- The submissions of five credit card applications in the name of "Kyle Patrick." These applications specified Patrick's Social Security number (SSN) and a mailing address of 1484 Willamet Road, Dayton, Ohio.
- A Bloomberg Business article on tax refund fraud describing how a criminal with valid Social Security numbers, dates of birth, bank account information, addresses, and an internet connection can illicitly obtain tax refunds loaded onto prepaid cards.
- A textport[9] conversation on May 28, 2015, between inmate Adam Johnston to a cell phone belonging to his mother, Karen Gallienne. During this conversation, Gallienne texted Johnston an address: 1484 Willamet Road in Kettering, Ohio, and stated that this was where "Steve" lives. Johnston sent a text message back to his mother, stating: "Wow that sounds really close to your house." Johnston later texted, "I would've texted yesterday, but I wasn't able to get online."
- The issuance of passes for inmates to gain access to multiple areas within MCI.
- Accessing unauthorized inmate records including disciplinary records, sentencing data, and inmate locations.

Forensic Analysis Completed by ODAS OIT

ODAS OIT also conducted a forensic analysis on the two computers' hard drives. From its analysis, ODAS OIT reported "… a large hacker's toolkit with numerous malicious tools for possible attacks. These malicious tools included password-cracking tools, virtual private network tools (VPN), network enumeration tools, hand-crafted software, numerous proxy tools, and other software used for various types of malicious activity."

The malicious tools found on the two drives reported by ODAS OIT included, but were not limited to the following:

- **CC Proxy** – proxy server for Windows, an internet access proxy software
- **Cain** – hacking tool for recovering password
- **Zed Attack Proxy (ZAP)** – provides scanners and tools to find security vulnerabilities
- **CC Cleaner** – freeware tool for system optimization, privacy, and cleaning

[9] Textport - A free online text messaging service that allows text messages to be sent from online computers to mobile phones.

- **Wireshark** – free and open-source packet analyzer
- **NMap** – utility for network discovery and security auditing
- **ZenMap** – security scanner and the official cross-platform GUI for Nmap
- **Hand-Crafted Software**
- **SoftEther VPN Server** – free and open-source multi-protocol VPN software
- **OpenVPN** – free and open-source VPN software
- **Jana Server** – multi-platform web proxy
- **Yoshi –** email spamming tool
- **VideoLan** – VLC is a free and open source cross-platform multimedia player.
- **Clamwin** – anti-virus software
- **phpBB** – free and open source forum software
- **AdvOr Tor Browser** – free software for enabling anonymous communication and is better than TOR for anonymity and speed
- **Paros** – Java-based proxy that helps in assessing the vulnerability of web applications hacking tool used for Man-In-The-Middle Attacks (MITM) and client certificates.
- **3CXVoip Phone –** free VOIP/SIP softphone for Windows.
- **Webslayer** – hacker tool designed to Brute Force web application
- **Cavin** – small portable editor to encrypt and decrypt text
- **Virtual Box** – Kali installed
- **TrueCrypt** – open-source encryption tool which can encrypt a partition in Windows
- **THC Hydra** – a very fast hacking/network cracker tool for cracking logins
- **Kali Linux** – is regarded as the most versatile and advanced penetration testing distribution

ODAS also reported finding "… self-signed certificates, Pidgin chat accounts, Tor sites, Tor geo exit nodes, ether soft, virtual phone, pornography, videos, VideoLan, and other various software." Additionally, articles about making home-made drugs, plastics, explosives, and credit cards were discovered.

The ODAS OIT analysis also revealed that malicious activity had been occurring within the ODRC inmate network. ODAS OIT reported, "…inmates appeared to have been conducting attacks against the ODRC network using proxy machines that were connected to the inmate and department networks." Additionally, ODAS OIT reported, "It appears the Departmental Offender Tracking System (DOTS) portal was attacked and inmate passes were created. Findings of bitcoin wallets, stripe accounts, bank accounts, and credit card accounts point toward possible identity fraud, along with other possible cyber-crimes."

Based on information discovered during the forensic analysis, the Office of the Ohio Inspector General issued subpoenas to five banks that had received credit/debit card applications in the name of "Kyle Patrick."

On October 19, 2015, the Office of the Ohio Inspector General reviewed 17 telephone calls made between April 26, 2015, through August 9, 2015, from Inmate Johnston to his mother Karen Gallienne. From its review of these telephone calls, the Office of the Ohio Inspector General discovered the following:

- Gallienne verbally confirmed that she resided at 1497 Willamet Road, Kettering, Ohio.
- Gallienne informed Johnston that she had received a notice from Chase that the credit card for Kyle Patrick was declined.
- Gallienne informed Johnston that she had received a Visa debit card for Kyle Patrick and read the card number, expiration date, and activation code to Johnston.
- While talking to Johnston, Gallienne told Johnston that she was researching information for him on the internet.

On October 20, 2015, the Ohio State Highway Patrol interviewed ManCI inmate, Kyle Patrick. Patrick stated that he did not know Johnston and was never incarcerated with him.

On November 3, 2015, investigators met with Bunting to discuss the movement of inmates Transkiy, Cooper, Spriggs, Johnston, and Watkins to other ODRC institutions. Johnston was transferred to Grafton Correctional Institution (GCI). Bunting was told that these inmates should not be permitted access to any telephone, because of a pending search warrant slated to be executed. This was to prevent the destruction of any evidence and for the safety of investigators. Bunting sent an email to the wardens of the institutions involved instructing them that these inmates were to be housed in restricted housing units and not permitted access to telephones.

On November 5, 2015, the Ohio State Highway Patrol executed a search warrant of Karen Gallienne's residence at 1497 Willamet Road, Kettering, Ohio. During this search, the Ohio

State Highway Patrol found and obtained the Visa debit card from MetaBank issued to Kyle Patrick and mailed to the address of 1484 Willamet Road, Dayton, Ohio.

The Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed Karen Gallienne to determine her involvement in the issuance of credit/debit cards. Gallienne admitted to investigators that she had provided the address "1484 Willamet Road, Dayton, Ohio" to her son, inmate Johnston, through a text message. Gallienne added that the address was the residence of Steve Seifert, an acquaintance of hers who lives across the street from her and who agreed to allow mail to be sent to his address in the name of Kyle Patrick. Gallienne noted that she would either pick up the mail addressed to Kyle Patrick from Seifert or he would bring his mail to her. When asked by investigators why Johnston did not put the debit card in her name, Gallienne said, "Because he didn't want to put my name on anything."

Gallienne acknowledged to investigators that she knew Johnston submitted credit/debit card applications using Kyle Patrick's name and Seifert's address. Gallienne said Johnston told her, "He was gonna try to put some money on it so he could… give me money, help me out." Gallienne admitted that she, during a telephone conversation with Johnston, gave him the approved debit card number she had received through the mail "… so he could activate it." When Gallienne was asked by investigators what Johnston was going to do with the debit card, she said, "He won't tell me anything 'cause he doesn't want me to get in trouble." Gallienne also revealed that Johnston continued to call her from Grafton Correctional Institution while he was in a segregation unit. Further investigation revealed that Johnston made five calls to Gallienne from GCI.

On November 17, 2015, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed inmate Adam Johnston at the Grafton Correctional Institution. During this interview Johnston admitted that he placed the two computers in the ceiling. Johnston said the unauthorized computers came from the RET3 area and were built by inmate Scott Spriggs. Johnston said the computers were fully functioning when he took them from the RET3 area to the P3 training room. Johnston denied naming the computer with a specific computer

identification number. However, Johnston stated, "I imaged the drive ... with Acronis ... all you gotta do is take that drive, plug it into any computer and it will boot up." Johnston said he obtained the hard drive from another inmate computer, stating "… [I] took a network card out of another computer and put it in that." Johnston said, "Put it in there, plugged it in. Plugged it in that one into the inmate switch. The other one into the other ones. Remote desk top into the computer. And then… bam. I'm on the network." Johnston could not remember the date when he placed the two computers in the ceiling, but said it was prior to June 1, 2015, when he was still working in the P3 training room with Canterbury. Johnston also admitted to investigators that he ran computer wire from the two computers to the switch in Canterbury's office.

Network hub located in MCI Training Room P3.

Johnston admitted to investigators that he used the computer to text message his mother on May 28, 2015, and that Gallienne provided Johnston with Stephen Seifert's address. Johnston told investigators that he did not know "Steve" but "… knew that his address was there and I told her just to go over there and get it," meaning the debit card applications or any mail sent to Kyle Patrick.

Johnston admitted to investigators that he submitted the online credit/debit card applications using the computers hidden in the ceiling of the P3 training room. Investigators asked Johnston how and why he chose inmate Kyle Patrick's name to use for the applications. Johnston said he reviewed the directory of inmates in the ODRC system for a young inmate who was serving a lengthy sentence and eventually chose Patrick. Johnston said he obtained Patrick's Social Security number and date of birth through the Departmental Offender Tracking System (DOTS). Johnston said he accessed DOTS by signing onto the system using Canterbury's password which he had obtained by "shoulder surfing" Canterbury when he logged into DOTS. When confronted with the fact that the Social Security number is obscured on the inmate information sheet, Johnston explained how he got the Social Security number.

Johnston admitted to investigators that he accessed an article online from the Bloomberg.com site detailing how to submit fraudulent tax returns and have the refunds wired to debit cards. Johnston noted that this tax fraud plan was one of the several plans he had intended to try in order to obtain debit cards. Johnston also admitted to using the internet to run Kyle Patrick's name and Social Security number through TINCheck to verify the Social Security number belonging to Kyle Patrick.

In addition to his actions related to Kyle Patrick, Johnston also confirmed to investigators that he had downloaded the pornography that was found on a thumb drive in the possession of inmate Robert Cooper. Johnston told investigators that he had called his mother several times from Grafton Correctional Institution (GCI) while in segregation by using another inmate's pin number. While GCI blocked Johnston's pin number from being able to complete calls, they did not block Gallienne's phone number or prevent Johnston's access to a telephone.
On November 17, 2015, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed Ken Kovatch, owner of RET3. Kovatch explained his company collects outdated or non-functioning computers from businesses, schools, and organizations to be recycled. In 2014, Kovatch entered into a contract with MCI to use inmates to dissemble computers. Kovatch explained the process to investigators. Kovatch delivered the computers on skids to MCI. The inmates disassembled the computers and placed the various parts into

separate boxes. Later, Kovatch picked up the boxes of computer parts for salvage. Kovatch noted that his company is R2/RIOS[10] certified, which requires certain training and procedures, and because of this certification, the refurbishment of computers could not be performed at MCI. Kovatch told investigators that he believed he donated 93 computers to MCI in 2013 to be used in the Lifeline program and that the computers had a RET3 sticker affixed to them. Kovatch noted that he had recently looked for the computers in the Lifeline area and found only six of the 93 computers he had donated.

Investigators asked Kovatch about his interactions with Canterbury and Brady. Kovatch stated Canterbury was MCI's designated contact person who oversaw the disassembly of the computers. Kovatch said about a month after this recycling program started at MCI, he had a meeting with Rebecca Shafer, business administrator at MCI. Kovatch said Shafer told him that,

> Canterbury's gonna be retiring, and when he retired he could work for you --- I don't know what the particular --- I don't know, I don't understand what was said in the meeting. He could work for you for a period of time on your payroll and then we could put him back on the medical uh plan. Uh that I, I did not understand. It wasn't any of my business anyway, but if he would --- he, he had so many months to work after and then he could get back onto uh the state's uh retirement or whatever.

Kovatch then received a transition plan explaining how Canterbury would retire from ODRC and later become a RET3 employee overseeing the program at MCI.

Kovatch told investigators that Brady had brought scrap from MCI to his company to be salvaged. Kovatch added that Brady had taken computer parts, memory, hard drives, and switches from his company. Kovatch said that he did not keep an inventory of items taken by Brady from his warehouse.

[10] The R2/RIOS™ certification is solely for electronics recyclers to demonstrate to customers that electronics are being recycled with the highest standards for data privacy, environmental controls, employee health and safety and corporate responsibility.

On November 24, 2015, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed inmate Robert Cooper. On September 16, 2015, Cooper was found to be in the possession of a thumb drive that contained pornography and movies. Cooper did not want to provide investigators with any information regarding other people, but was willing to tell of his direct involvement with the thumb drive. Cooper said he would receive the thumb drive loaded with movies, "… it was not just pornographic movies. It was like the new releases, TV series. That's all I would get." Cooper said he also would get music on the thumb drive which he would then sell to other inmates, and his payment was usually in the form of commissary items. Cooper would not identify who loaded the thumb drive for him, but said, "I was a beneficiary of what another individual done."

On November 24, 2015, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed inmate David Aldridge. Aldridge assisted Brady with IT matters and was the inmate network administrator. Aldridge denied any participation or knowledge of the two computers found in the ceiling. Aldridge said he and inmate Ben Watkins were with Brady in the P3 training room the day the two computers were found. Aldridge explained that it was he and Watkins who found the computers and removed them from the ceiling, adding, "No one knew and I don't think anybody knows to this day that we were the ones that were actually there and found them." Aldridge said after the computers in the ceiling were discovered, inmates began wiping the computers located at the institution. Aldridge said Brady authorized him to refurbish computers that came into MCI through the RET3 program. Aldridge said Brady had told him that there was an agreement allowing Brady to refurbish 100 computers that came from RET3 and place them for use in MCI. The replaced computers would be scraped out so the incoming weight would match the outgoing weight. Aldridge acknowledged that he received incentive pay for other Green Initiative jobs he performed and was paid in hygiene items. Aldridge confirmed that the hygiene cart was usually pushed by Johnston or Spriggs.

On November 30, 2015, the Office of the Ohio Inspector General received a response from MetaBank to a request for information of all credit/debit card applications received for Kyle Patrick at 1484 Willamet Road, Dayton, Ohio. MetaBank's response confirmed that a debit card

application was received on June 21, 2015, at 5:38 p.m. from an ODRC IP address, and that the debit card was activated on July 16, 2015, at 11:01 a.m. again from an ODRC IP address. The applications for credit/debit cards to four other banks were declined.

On December 8, 2015, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed inmate Scott Spriggs. Spriggs denied having any involvement with the two computers found in the ceiling, but was willing to discuss the security lapse at MCI. Investigators asked Spriggs how it was possible to move two computers from the RET3 area, across the institution, past a crash gate with metal detector and a corrections officer, to an elevator, and up to the third-floor P3 training room in the administration building. Spriggs responded, "… the regulars [corrections officers] are less likely to even stop you. So if it's their post they're less likely to even say a word to you." Spriggs acknowledged to investigators that it would require a great deal of unsupervised time to place two computers in the ceiling of the P3 training room and then run cables from the computers to the network switch.

Since he worked in the RET3 area, investigators asked Spriggs about his views on Brady's supervision. Spriggs said,

> I would say his supervision's pretty lax, too. Not to mention that if you take the deal he had with RET3 about coming and taking any computer he wanted … I know that he came and told me that I should be looking for high-end dual cores and any quad cores. And whenever just send a message to him or when he came down to pick up hard drives have them set aside and he would reallocate them throughout the system.

Spriggs estimated that Brady took approximately 30 quad core computers from the RET3 area that were supposed to be dismantled, to replace computers in the institution. Spriggs said when Canterbury became an RET3 employee, RET3 sent him a dual core HP computer. "When it came in Brady had said that they were phasing those out of the network or something like that 'cause they're, you know, a few years old. So he gave him a different computer." Spriggs admitted that Canterbury allowed him and other inmates access to Canterbury's computer under his (Canterbury's) direct supervision. Regarding the issue of access to software, Spriggs said

inmate David Aldridge "… had tons of software and a lot would be put up on the network." Spriggs told investigators that software was available to everyone including wiping and recovery software that was not password protected.

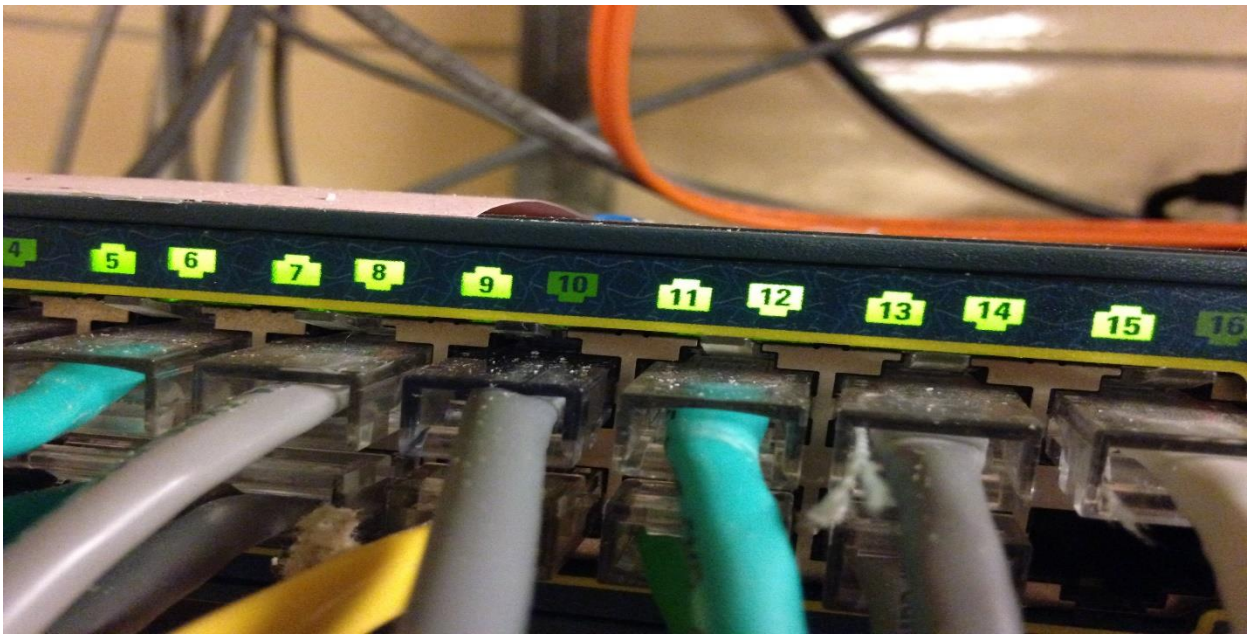
On January 5, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed Randall Canterbury. Canterbury explained to investigators that prior to his retirement from ODRC on May 31, 2015, he served as the training officer, conservation coordinator, and recycling coordinator for MCI. His office was located on P3, the third floor of the administration building. On June 1, 2015, he became an employee for RET3, continuing his responsibilities overseeing the recycling of computers and the conservation programs of the Green Initiative. MCI moved Canterbury's office space to the RET3 area. Canterbury said the function of the RET3 program at MCI was for inmates to break down computers shipped in from RET3 into parts. Canterbury said the inmates "… kept the inventory of stuff coming in and the stuff going out." Canterbury said refurbishing was not a function of his area and, "… we refurbished nothing for nobody." Canterbury said, "I just know Gene refurbished computers. I don't know if Gene got them from RET3 … but I, I'm not sure." When asked by investigators whether he had instructed Spriggs to set aside functioning computers for Gene Brady to pick-up; Canterbury said, "I … don't recall telling him to do that, but that could have happened."

Canterbury denied knowing anything about the two computers hidden in the ceiling. Canterbury told investigators his computer password and noted that he had probably last changed his password several years ago. Canterbury confirmed to investigators that inmate Johnston helped select items from online vendors to be purchased for the Green Initiative. Canterbury later admitted that, "There might have been an --- a chance where a guy says hey, can I look at that and he clicked on it. Yeah." When investigators informed Canterbury that Transkiy admitted using his computer while he was present, Canterbury said, "But I don't recall him using the keyboard."

Canterbury acknowledged to investigators that when his office was located in the P3 training room, he had left inmates unsupervised for long periods of time, adding, "Well, they could be

back there all afternoon." Canterbury also admitted that he left inmates unsupervised in the RET3 area. Concerning Canterbury's transition from a state employee to a RET3 contract employee, Canterbury said he believed Transkiy wrote the contract. Canterbury noted he submitted a letter to the Ethics Commission for an opinion regarding his move from a state employee to a MCI contract employee. Canterbury said he received a letter from the "… Ohio Ethics Commission that it wasn't an issue with me working as a contractor as long as the State of Ohio wasn't paying me." At this point, Canterbury ended his interview with investigators.

On January 14, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed MCI Infrastructure Specialist 2 Carl (Gene) Brady. Brady told investigators that he first became aware of the unauthorized computer operating in MCI around July 17, 2015, after an email from the ODRC Operation Support Center in Columbus was sent to Warden Bunting, who then notified MCI Investigator Hundley, who then informed him (Brady). Brady stated that when he was provided with the identification name of the computer (lab9), Brady knew the computer was not an MCI-authorized computer. Brady explained that he assigns an identification name to all computers located at MCI. From the name of this unauthorized computer, Brady said he was able to determine the computer was located in the P3 training room. Brady stated that there were only six computers in the training room and are numbered sequentially "1" through "6." However, Brady noted, the unauthorized computer was numbered "9." Brady said he received the email on July 24, 2015, informing him the unauthorized computers were plugged into port 16 on the network switch. However, when he went to search for the cable, he mistakenly checked port 10. However, Brady re-read the email again on Monday July 27, 2015, and discovered his mistake. Brady said, "At that point, yes. I was, I was --- at this point I'm pretty sure it's inmates."



Network switch port numbers 10 and 16.

On Monday July 27, 2015, Brady, along with inmates Aldridge and Watson, went to the P3 training room to evaluate the situation. They followed a cable from port 16 up into the ceiling over into the closet area, lifted the ceiling tiles and discovered two computers sitting on plywood boards. Brady told investigators that after the discovery, he called MCI Lieutenant Tim Rayburn who came to the room and took pictures of the computers and that he (Brady) then removed the computers from the ceiling. When Brady was questioned by investigators whether he personally removed the computers from the ceiling, Brady acknowledged that the two inmates removed the computers from the ceiling. Brady told investigators he was aware of the protection of a crime scene policy but noted that he did not realize it was a crime scene until the computers were removed from the ceiling. However, Brady said he tagged them as contraband. Brady said because he did not receive any instructions on what to do with the computers, he delivered them to the ODRC Operation Support Center in Columbus on July 30, 2015.

Brady confirmed to investigators that he directed inmate Spriggs, who worked in the RET3 area, to set aside newer computers to be repaired or refurbished, for use at MCI. Brady also admitted that he authorized the availability of wiping software on the inmate computer network to allow inmates to wipe or clean hard drives. Brady claimed to investigators that he was against permitting inmates access to wiping software, but noted Warden Bunting, through Business

Administrator Rebecca Shafer, authorized the use of the software. Brady added, "I've had Jason personally tell me a couple times just --- as long as they're not getting outside the institution, I don't care."

On January 21, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed MCI Warden Jason Bunting. Investigators asked Bunting how and when he became aware of the unauthorized computers operating in MCI. Bunting said he received a telephone call in early July from either Business Operation Manager Kevin Stockdale or CIO Vinko Kucinic. Bunting was informed that a computer operating from MCI was attempting to circumvent ODRC network controls and was accessing the internet for long periods of time. Bunting said he was also informed of the computer's identification and the computer's assigned user name, Randy Canterbury. Bunting stated he forwarded the computer information to Brady and instructed Brady to locate the computer. Bunting said,

> … so then that was about uh identifying and isolating to what area it was coming from. And that's part of what took him --- according to him, if I recall, took him so long to find the computer because it wasn't anything he set up. And then he had to find --- narrow it down to what area it was. And I remember him saying, I think I got it narrowed down. I got it narrowed down. And then finding it. But it was a --- we initiated a search trying to find it and that's what I told Mr. Bobby.

Bunting also noted that he informed MCI Investigator Michael Hundley[11] and then called his supervisor, ODRC Northwest Regional Director David Bobby. Bunting was asked about an email he had received on July 21, 2015, from Kucinic, who wrote, "You had indicated you would be submitting a request through the Chief Inspectors Office." Investigators asked Bunting whether he had contacted the Chief Inspectors Office to inform them of the situation regarding the two computers. Bunting said, "So it would have been Roger Wilson and his shop. Gosh, I have a great memory, but I don't know what it is, I can't link --- I don't recall talking to Roger."

[11] MCI Investigator Michael Hundley passed away on January 2, 2016.

Bunting told investigators that he recalled being told that it was not an MCI computer because of the computer's identification. Bunting was also aware that the unauthorized computer was being used during times when Canterbury was not at the institution. When investigators asked Bunting what he deducted from this information, Bunting said, "… you lean towards an inmate has access to it. Absolutely." Moreover, Bunting was aware that the unauthorized computer had accessed DOTS and "… attempts to get into our network and some of our secured area which is a no-no." Bunting added,

> I remember a conversation about applying for a credit card. I don't know when that --- I don't know if that was this initial conversation or it was some of the group conversations, but I remember credit card fraud being a thought and that they actually submitted a request for a credit card. It came back denied.

Bunting admitted knowing all of this before the two unauthorized computers were found. Bunting agreed that he knew at that time a crime was occurring, saying, "I knew obviously illegal activity was going on." Investigators asked Bunting why he did not notify the Ohio State Highway Patrol of this illegal activity and Bunting responded, "… and I don't have that answer for you." Bunting agreed that he was aware of the Governor's directive to report suspected illegal activity to the Ohio State Highway Patrol and the Office of the Ohio Inspector General. Bunting agreed that he was aware of the ODRC protection of a crime scene policy, but was not aware that inmates were being used to retrieve the two computers hidden in the ceiling or where the computers went after being removed from the ceiling.

Bunting acknowledged receiving from Brady an incident report written on July 27, 2015, informing him that the computers were located, but Bunting did not recall forwarding the incident report to anyone or to the ODRC Central Office. Bunting claimed the incident report written by MCI Investigator Hundley on August 7, 2015, was completed at Bunting's request for his (Bunting's) own records. **(Exhibit 3)**

Bunting was asked if he authorized anyone to open or enter any of the secured areas involved in this investigation. Bunting said he believed that after speaking to Hundley,

> I interpreted what he had told me as OSHP had --- was done with what they needed to do and that place was able to be accessed… P2 had inmate organization leaders and computers in there, our offender organization computers. There was materials in there that the staff liaisons were asking for to maintain fundraisers and documentation and those kind of things because they knew they weren't getting computers, but they needed their files --- their hard files and those kind of things. And so based on how I interpreted what Mike had told me, uh my understanding was with Mike it would be okay to let him escort a staff member in there; get the materials they needed and get out. But after couple of dialogues with Mike it was clear that we weren't on the same page regarding that area.

On February 9, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed MCI Lieutenant Tim Rayburn. Rayburn acknowledged that he was aware of the search for the unauthorized computers in MCI prior to them being found. He was also aware that the computers were being used to access sites outside of the institution. Rayburn stated that MCI Major Sam Grisham informed him that the computers were found, and directed him (Rayburn) to travel to the site and take photographs of the computers. Rayburn stated that when he arrived at the P3 training room, Brady and two inmates were present and a ceiling tile was removed and the computers were visible. After taking the photographs, Rayburn left the area, downloaded the photographs, and forwarded them to Hundley. When asked by investigators why the scene was not secured and OSHP was not notified as the policy requires, Rayburn said, "I don't have an answer for that." Rayburn acknowledged that he was aware of the Protection of Crime Scene policy, but his only direction was to take the photographs of the scene. Rayburn acknowledged that it is common at MCI to allow inmates unsupervised access to areas of the institution and use the elevator. Rayburn noted that he had previously witnessed unsupervised inmates in the P3 training room where Canterbury's office was once located.

On February 9, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed MCI Business Administrator Rebecca Shafer regarding the removal of items from the secured areas; specifically, from Transkiy's, Johnston's, and Spriggs' offices located on

P2. Shafer stated she had not entered those areas nor removed any items. Shafer said that inmates,

> … may have had a copy of our um trash contract to see what dumpsters we had here and how often we pick up because as part of um the energy conservation policy we have to review um like our, our --- all our utilities and our uh waste. Um so we do audits of those and that group provided a lot of that analysis … they may have had contracts for uh … something that we purchase. Um maybe it's um supplies for, you know, like whose, whose on contract for supplies they may need on the back dock like gloves and um, you know, different materials they use.

Shafer continued,

> Any time I've needed information I've gone --- I went through the investigator and/or the warden and said this is what I need. You mean --- are --- so we're talking about while this investigation's been active? Yes. All my in --- all my requests have gone --- went through the investigator. I would say this is what I need. You know, can I get --- can I get this? And no one from the Business Office, I can assure you, would have gone up. I, I have--- nobody here has removed anything. We always went through the investigator and/or the warden.

On February 11, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed MCI Major Sam Grisham. Grisham said he was never informed of the search for an unauthorized computer on the state network. Grisham said Brady called him on July 27, 2015, to inform him that, "... they found a computer that had the capability to connect outside and was on our server." Grisham stated he had directed Rayburn to go to the training room and take photographs of the computers, "… because it's not an area where they should be." Grisham was asked by investigators who he believed used the two computers, knowing that the computers had access to the state network and the internet; that the computers did not belong to MCI; and that one of the computer's identified users, "Canterbury," was used during times when Canterbury was not at the institution. Grisham answered, "inmates." Grisham noted to investigators that when the two unauthorized computers were found, the P3 training room should have been handled by MCI as a crime scene and OSHP should have been notified.

Grisham said, "Randy would leave the floor and leave the offenders up there," referring to the P3 training room. Grisham stated that he had directed Canterbury to not leave inmates in the area unsupervised. Grisham also complained to Bunting about the inmates having the ability to text or instant message each other through the computers. Grisham said,

> … the problem I have with it is I lose security. If I'm gonna do a surprise walk-in and try to catch somebody doing something, inmates are texting each other, hey, Grisham's here; Grisham's there … they should not have any means of communications such as that.

On February 16, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed ODRC Chief Information Officer Vinko Kucinic. Kucinic stated that ODRC received a Websense alert on Friday July 3, 2015, indicating that Canterbury's log-in credentials were used in an attempt to avoid ODRC security controls for three hours. Kucinic noted that he was not informed that Canterbury does not work on Fridays or weekends and that the unauthorized computers were hidden. Kucinic said,

> … and then I think on a weekend, too, there was some uh --- I believe on a Saturday, so it, it didn't seem right … in situations like this we normally will reach out to the --- you know, the warden and/or the regional administrator … this is suspicious.

Kucinic noted he had a discussion with Bunting about possibly installing a camera to determine who was using the computer. Kucinic stated after a week or two had passed, he recalled receiving an email from Warden Bunting saying, "… thanks for the information, we found two computers in the ceiling." Kucinic said that he did not have any contact with Brady regarding these unauthorized computers until two days after they had been found when Brady asked him for direction as what to do with the computers.

On February 23, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed ODRC Northwest Regional Director David Bobby. Bobby told investigators that he was aware of the search for a computer saying, "I knew we were searching for something that was hooked into our system that wasn't supposed to be there." Bobby added that he had received an email from Bunting that stated, "Did I tell you about the two computers that we

found uh in the ceiling?" Bobby then said, "And, and my response was, no; were they operational? And then I believe we talked on the phone at that point." Bobby did not recall any other details or conversations regarding the computers. Bobby agreed that "… normally if they --- if the institution has uh --- they suspect that a crime is committed on the grounds they notify the local folks ... ," meaning the Ohio State Highway Patrol. Bobby denied telling Bunting to not report the operation or search for the unauthorized computers and he denied anyone telling him to not report the operation or search for the unauthorized computers.

On February 25, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed ODRC Chief Counsel Stephen Gray to discuss the reason for the delay in notifying the incident to the Office of the Ohio Inspector General and the Ohio State Highway Patrol. Gray stated,

> I prepared a notification on August 7th and that was the same day that I became aware of this uh --- the incident … I received a call from Vinko Kucinic, my Chief I.T., uh who --- I think he asked me up to his office and I forget who was there. I don't know if um Nathan Norris was working for us at the time or not, but … I recall there was someone in the office, or maybe somebody on the phone and they were explaining to me kind of what happened at, at Marion. And then, you know, kind of gave me a little bit details that we --- they, they were able to --- you know, and talking I.T. speak where I don't understand. They got some ping on this and they were able to locate something. Um and I, and I believe Vinko said he'd been in touch in with DAS I.T. and maybe the Patrol knew about this. And then when I found out about it I said, well, I --- you know, there could have been some illegal activity associated with this 'cause we don't know what the inmates were doing. So that's when I um drafted the uh notification that went out on that day.

On March 3, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed ODRC Office of Administration Deputy Director Kevin Stockdale. Stockdale stated that in early July 2015, he was made aware of the Websense alerts involving MCI. Stockdale said, "… the first assumption was that it was likely an instance of an inmate getting access to a

computer potentially and doing something inappropriate." Stockdale said he had a conversation with Bunting on July 9, 2015, regarding the Websense alerts. Stockdale stated,

> … the course that the institution wanted to take at that point was to investigate it as potentially we have an inmate who's out of place and um, you know, let's get some cameras up and see what's going on … we probably let the institution work through their process um to a greater extent than we should have.

Stockdale noted that he knew some of the Websense alerts occurred on weekends which caused him to believe that Canterbury was not involved. Stockdale added,

> … the appropriate course of action was for the institution to notify the Chief Inspector's Office and that was --- that would signal our involvement as, as far as the technologists. I mean … they get pulled into investigations, but they're not investigators. They're just … I.T. people.

On March 3, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed ODRC Managing Director Stuart Hudson. Hudson said that on August 7, 2015, Kucinic briefed him on the MCI incident. Hudson explained,

> … when it came to me I heard that we found this computer. Uh there was all kinds of things tied into it. We don't know what we have yet and I think notifications started being at the OIT and, and that type of thing. But it wasn't 'til later --- I know it was late in the day. I don't know if it was that day or the day before, but it was late in this day where we convened a small group of leadership just to start talking about and figure out what we actually had here. And this was much more serious and we need to get up there be --- and at that point we didn't call the warden in yet. Um but shortly after that call we did call the warden and had him on a conference call with myself, Vinko, um Dave Bobby and Chief Counsel. … there was concern at first that the institution may not be taking this as serious as they should. Um and that's --- that was with the warden and, and how they were dealing with it locally.

When the incident was reported to Hudson, he believed inmates were involved. Hudson stated,

> Um so we knew it was inmate related, but … there was some talk about how this was tied into the N.A.'s [network administrator] stuff, too. You know the, the perception was you go in there and you see how he was using inmates to do some of the work, too. So it --- tended to believe that we had a more serious issue here than, than what we really thought. So that's, that's why we started making all notifications.

On March 3, 2016, the Office of the Ohio Inspector General and the Ohio State Highway Patrol interviewed ODRC Chief Inspector Roger Wilson and Assistant Chief Inspector Paul Shoemaker. The Office of the Chief Inspector provides assistance to institutional investigators and inspectors as well as conducts internal administrative investigations for the department. However, institutional investigators report directly to the warden. Both Wilson and Shoemaker confirmed that they were never contacted or informed of the two unauthorized computers at MCI, or the search for the computers, or that the computers were found. It was not until the computers were delivered to ODRC Central Office on July 30, 2015, that the Chief Inspectors Office became aware of the incident.

Other Issues Discovered

Slow and Improper Response

On Friday July 3, 2015, ODRC IT employees received a Websense email alert regarding Randy Canterbury[12] attempting to avoid ODRC security controls. The next day, ODRC CIO Vinko Kucinic was informed of the Websense alerts. On Monday July 6, 2015, an ODRC IT employee emailed numerous Websense alerts to Kucinic, stating "… this guy spent 3 hours searching the internet and trying different methods to avoid the proxy server." On Friday July 17, 2015, and Monday July 20, 2015, ODRC IT employees received additional Websense alerts regarding the user Randy Canterbury attempting to avoid ODRC security controls. ODRC IT employees identified the activity was coming from the same IP address and the computer's identification is "lab9." On July 21, 2015, Kucinic emailed the computer's identification to MCI Warden Jason Bunting. In this email, it was inferred that Kucinic and Bunting had a previous conversation and

[12] Canterbury did not work on Fridays.

Bunting indicated that he would be contacting the Chief Inspectors Office. Also on July 21, 2015, from email evidence evaluated, investigators determined that MCI Infrastructure Specialist Carl (Gene) Brady was aware of the unauthorized computer, the computer's name, and its general location. Additionally, on July 21, 2015, investigators found email evidence indicating that the MCI Investigator Michael Hundley was aware of the unauthorized computer, possible location, and was searching for the unauthorized computer. On Friday, July 24, 2015, ODRC IT emailed Brady informing him the computer's location and the port it was plugged into. Brady told investigators that he had misread the email and mistakenly looked at port 10 instead of port 16, as specified in the email. Brady stated that on Monday, July 27, 2015, Brady read the email again and discovered his mistake. He went to the P3 training room, discovered a cable plugged into port 16, followed the cable into the ceiling, and discovered the two unauthorized computers.

When Brady found the two computers hidden in the ceiling, he said he knew they were not State of Ohio computers or computers that should be operating in MCI. Brady said he knew these computers were not MCI-authorized computers because the computer names were outside of his naming convention. When alerted that the computers had been found hidden in the ceiling, MCI Major Sam Grisham instructed MCI Lieutenant Tim Rayburn to photograph the scene. Rayburn photographed the computers then returned to his office to download the photos for Investigator Hundley. Brady then directed two inmates to remove the computers from the ceiling and move them to his office.

Bunting, Hundley, and Brady were aware that the computer they were searching for was not an MCI computer. Bunting and Hundley knew some of these Websense alerts occurred on days when Canterbury was not in the institution. Bunting, Hundley, and Brady knew the computer was not visibly in the training room. With knowledge of these facts, Bunting and Brady concluded that an inmate was involved, but never notified the OSHP trooper assigned to MCI or the Office of the Ohio Inspector General to handle the criminal investigation occurring at MCI.

Hundley and Bunting knew the two computers had been found on July 27, 2015, but did not notify the OSHP trooper assigned to MCI to handle criminal investigation occurring at MCI or

the Office of the Ohio Inspector General. The OSHP trooper assigned to MCI shares an office with Hundley. No one from the ODRC IT Operation Support Center reported to the Ohio State Highway Patrol or the Office of the Ohio Inspector General that they had discovered unauthorized computers operating inside MCI. When OSC delivered the computers to the ODAS IT Chief Information Security Officer Nathan Norris on August 7, 2015, he informed ODRC that they must report this illegal activity, as specified in the Policy and Procedures for Notification of Suspected Illegal or Improper Activity within State Departments and Agencies. On August 10, 2015, the Ohio State Highway Patrol Computer Crimes Unit took possession of the computers. Additionally, when the computers were found hidden in the ceiling, the scene was not secured and OSHP was not notified as specified in ODRC Protection of a Crime Scene policy.

ODRC-DOTS

In October 2014,[13] the Office of the Ohio Inspector General discovered and alerted ODRC that the Departmental Offender Tracking System (DOTS) displayed the Social Security numbers of inmates and that all ODRC DOTS users had access to this confidential personal information. ODRC's solution to this problem was to create a filter or block on the offender information screen that would cover Social Security numbers with zeros. However, as inmate Johnston explained during the investigation, once a user has accessed DOTS, the user could easily adjust the browser view settings and display an inmate's Social Security number. Based on information provided by Johnston, the Office of the Ohio Inspector General promptly reported to ODRC that previous efforts to conceal Social Security numbers were inadequate. As of the date of this report, ODRC has fixed the problem.

Password Security

ODRC policy *Information Technology Systems Password and Account Security 05-OIT-17* requires that information technology systems automatically compel employee or contractor users to change their individual passwords every 90 days. During the period of time under review, ODRC employees were not compelled to change their passwords.

[13] Report of Investigation 2014-CA00056.

Failure to Maintain Inventory Records

The Ohio State Highway Patrol seized the hard drives from 308 computers found in the Lifeline, One Stop, RET3, and P2 areas. Of these 308 computers, 291 did not possess a State of Ohio ODRC MCI fixed asset tag or an assigned inventory number.

MCI Infrastructure Specialist 2 Carl Brady acknowledged to investigators that he had obtained computers from the RET3 area that were slated to be salvaged and used them to replace outdated computers in the Lifeline and other program areas. Brady said he would then return the outdated computers to the RET3 area to be salvaged. Brady admitted that, "We probably didn't put any tags on them. Other than a Lifeline sticker." Investigators determined Brady's actions were in violation of ODRC policy *Inventory, Donation, Transfer, and Disposal of DRC IT Hardware & Software 05-OIT-21*.

Brady also admitted that he permitted inmates to remove the hard drives from RET3 computers slated for salvage and allowed the inmates to wipe the hard drives. Brady agreed with investigators that it would be possible for those inmates to take a hard drive, access the information stored on the hard drive, copy the information or transfer the information to another hard drive, and possibly use the confidential personal information of the previous owner. Investigators determined Brady's actions were in violation of ODRC policy *Inmate Access to Information Technology 05-OIT-11*.

Security Lapse/Unprotected IT Wiring and Network Switches

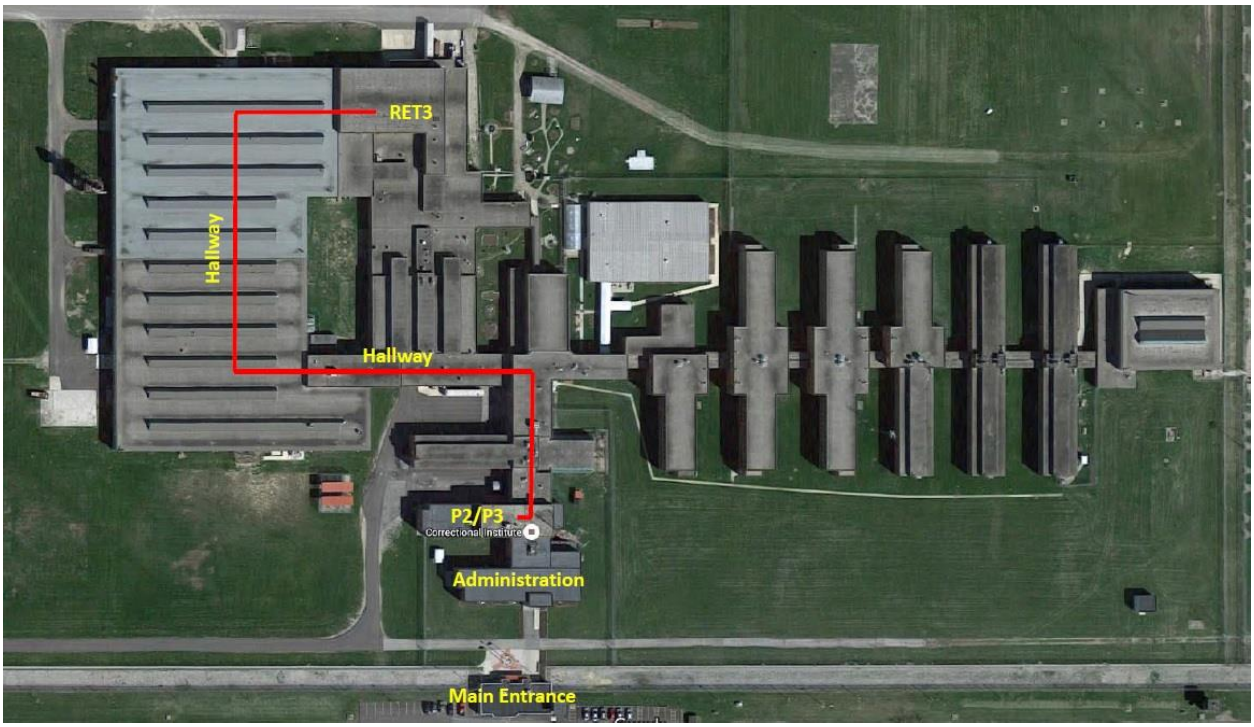
Inmates had access to computers, computer parts, network cables, ODRC-secured network switches, and ODRC operating systems. Johnston explained to investigators that he found computer cable laying in the ceiling, and he believed he found the power cord in the RET3 area. Johnston discovered the plywood boards that the computers were placed on in a closet in the P3 training room.

Location in ceiling where the computers were found.

In explaining to investigators how he moved the computers from the RET3 area to the P3 training room located on the third floor, Johnston said he used a cart. Johnston said,

> … with my job, I would transport like uh we passed out hygiene items to a few guys in the recycling program. And I stuck the uh computers in a box with all the hygiene and just --- and then went up there.

The distance that Johnston travelled from the RET3 area to the P3 training room was 1,100 feet. Johnston had to pass a corrections officer and a crash gate equipped with a metal detector. After he arrived in the front area of the administration building, Johnston used the elevator to go to the third floor. Johnston admitted that there were times when he was left unsupervised in the training room for up to an hour. Johnston also said he could go to the training room unsupervised to make modifications to the two hidden computers during late afternoons or evenings.



Releasing of Secured Areas and Other Security Issues

When the investigation was initiated, the doors to the Lifeline area, One Stop area, RET3 area, P2 and P3 areas were re-keyed so that only one key would access all the areas. The key was held in the control center and only a limited number of people were permitted to use the key. On September 2, 2015, representatives from the Office of the Ohio Inspector General, Ohio State Highway Patrol, and the Ohio Department of Administrative Services met with Warden Bunting. At this meeting, Bunting was advised that the Lifeline area, One Stop area, RET3 area, and the P2 area were to be considered as "secured" areas as part of this investigation and should any questions or issues involving these areas arise, Bunting was directed to contact either the Office of the Ohio Inspector General or the Ohio State Highway Patrol. On August 25, 2015, the Ohio State Highway Patrol began seizing the hard drives from every computer in these areas. Also in these areas, investigators mapped and seized hard copy documents in an effort to match physical evidence to forensic evidence recovered from the hard drives. On October 19, 2015, the Office of the Ohio Inspector General discovered that documents and books were missing from the One Stop Area and the inmate office used by Spriggs, Johnston, and Transkiy located on P2.

Before (photo dated August 26, 2015)

After (photo dated October 19, 2015)

Bunting was contacted to find out who authorized entry into these areas and the removal of documents and other property from these areas. Bunting said Hundley took staff members into these areas to obtain files needed for the Green Iniative programs.

On August 2, 2016, investigators initiated forensic processing of five hard drives collected by the Ohio State Highway Patrol from one personal computer located in MCI's P2 Reentry office, Room A178 (PC-1). A placard identifying that Spriggs and Johnston were approved to access computers in this area was also located in the vicinity of PC-1. On August 6, 2016, the forensic processing was completed and an initial review of PC-1 was initiated on August 8, 2016. Investigators were specifically looking to identify what, if any, "anti-forensic" software and tools were utilized by the inmates to remove or destroy potential evidence related to their illegal activities.

Investigators determined that PC cleaning software (CCleaner) found on PC-1 was executed on at least 10 occasions between August 17 and August 18, 2015. The use of this cleaning software

occurred well after ODRC discovered the two computers in the ceiling of the P3 training room and just prior to the area being secured for evidence collection. PC-1 was accessible to a number of unsupervised inmates who were both granted access to the P2 reentry office and who knew the generic login credentials for the machine.

CCleaner is downloadable software that enables a user to remove trace evidence of user activity and remove user files. The following are examples of what CCleaner removes from a computer operating system:

- Temporary internet files
- Internet History
- Internet Cache
- Download History
- Cookies
- Recently typed URLs
- Last download location
- Autocomplete form history
- Saved Passwords
- Recent Documents
- Thumbnail cache
- Network passwords
- Recycle Bin
- Temporary files
- Clipboard
- Memory dumps
- Windows log files
- Windows event logs
- Custom files and folders
- RegEdit
- Wipes free space

Because inmates were identified as possibly being connected to the two computers found in the ceiling, four inmates were placed in the segregation unit at MCI. However, it became apparent to investigators that the inmates were not separated to the point that they could not exchange information among themselves about what was discussed during their respective interviews or polygraphs. Because of this, Transkiy was transferred to the Mansfield Correctional Institution, Spriggs was transferred to Allen Correctional Institution, Johnston was transferred to Grafton

Correctional Institution, and Watkins was transferred to Lorain Correctional Institution. The four inmates were housed in their respective segregation units and were prohibited access to a telephone or kiosk, or electronic devices associated with a kiosk.

The primary reason investigators requested that these inmates be segregated and prohibited from making telephone calls was, in part, to prevent Johnston from being able to contact his mother to ask her to destroy evidence. During the interviews of Gallienne and Johnston, it was revealed that Johnston made five calls to his mother from October 27, 2015, to November 6, 2015, while he was being housed in the segregation unit at Grafton Correctional Institution. Investigators learned that although Johnston's pin number was blocked, his mother's phone number was not blocked. Johnston said he just used another inmate's pin number to make the calls to his mother.

Canterbury's Transition from ODRC Employee to RET3 Employee

During the course of the investigation, the Office of the Ohio Inspector General discovered that when Canterbury was still an ODRC employee, he had submitted a "Transition Plan" which specified that he would retire from ODRC to become an RET3 employee to continue his oversight of all Green Initiative programs. Canterbury emailed this "Transition Plan" to Deputy Warden Kristen Faine, Business Office Administrator Rebecca Shafer, and RET3 owner Ken Kovatch on March 4, 2015. **(Exhibit 4)** Canterbury wrote, "Please take a moment to review and once the administration makes any changes, I will begin collecting signatures." At the bottom of the transition plan were signature lines for the five inmates who served on the MCI Green Initiative Executive Committee. Canterbury requested an opinion from the Ohio Ethics Commission regarding his permissibility to except the contract position with RET3 after his retirement from ODRC. The Ohio Ethics Commission responded in a letter dated January 22, 2015, stating,

> Yes, provided that: (1) While you are an employee of the MCI, you do not participate, in any way, in the authorization of the contract between you and MCI; and (2) MCI determines it is in its best interest to hire you to manage the program.

Canterbury retired from ODRC on May 31, 2015.

CONCLUSION

The Marion Correctional Institution (MCI) allows inmates to operate several programs under the Green Initiative title. Some of those programs include a community garden program, aquatics program, recycling program, and the RET3 Corp., Inc. (RET3) program which disassembles out-of-date computers.

Investigators determined that inmates Spriggs and Johnston were unsupervised for extensive periods of time at MCI. For example, Spriggs and Johnston took two computers that should have been disassembled, placed hard drives into the computers, installed a network card, transported the computers across the institution for approximately 1,100 feet, through the security check point without being searched or challenged by staff, accessed an elevator to the third floor, and placed the two computers in the ceiling of the P3 training room. Additionally, Spriggs and Johnston not only placed the two computers in the ceiling, they also ran wire, cable, and power cords to connect the devices undetected onto the ODRC network. Johnston also told investigators that he would return periodically to the P3 training room unsupervised to make modifications to the hidden computers. Johnston connected the computers to the staff network allowing them access to the internet, which they could remotely access through any inmate computer.

With these computers, Johnston used the password of former MCI employee and contractor Canterbury to access DOTS. Johnston circumvented the security measures implemented by ODRC to conceal offenders' Social Security numbers in DOTS. Johnston obtained inmate Kyle Patrick's date of birth and Social Security number and created an email account for Patrick. Johnston then applied for five credit/debit cards via the internet using Patrick's name and the home address of an acquaintance who lived across the street from Johnston's mother. Any mail sent to Patrick would then be picked up by his (Johnston's) mother. Johnston was also planning to file false tax returns and have the refunds wired to the debit cards. Additionally, Johnston used DOTS to create passes for inmates to access unauthorized areas in MCI, creating a security risk.

Investigators determined prisoners took advantage of the freedoms, programs, and lax security standards at MCI. Inmates were allowed unsupervised access to computers and computer parts. Inmates were allowed unsupervised access to vast areas of the institution, and unsupervised time to build, transport, run computer cables, and hide the computers in the ceiling. Those computers were then used to access DOTS to obtain confidential personal information to attain a fraudulent debit card account to file fraudulent tax returns. Additionally, through DOTS, inmates had unauthorized access to inmate records including disciplinary records, sentencing data, and inmate locations.

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

Failure to Report Suspected Illegal Activity

On July 3, 2015, ODRC became aware of a computer user with the log-in identity of Randy Canterbury at MCI, attempting to bypass ODRC network security controls. The computer identified in this activity was not a computer listed as one that should be operating inside MCI. MCI Warden Jason Bunting knew some of the activity on the unauthorized computer occurred on days and times when Canterbury was not on the grounds of the institution. Bunting also knew the websites being accessed and that the computer was hidden, leading him to suspect an inmate was involved and he admitted knowing illegal activity was going on. Neither Bunting nor MCI Investigator Michael Hundley advised the Ohio State Highway Patrol trooper assigned to MCI to investigate criminal activity, or MCI Major Sam Grisham, who is responsible for the security of the institution, of the operation or search for the unauthorized computers. Bunting did not forward to his supervisors or ODRC Central Office the incident report dated July 27, 2015, documenting that the illegal computers were found. Bunting had no explanation as to why he did not report this suspected illegal activity to the Ohio State Highway Patrol and the Office of the Ohio Inspector General as required by policy. This failure to report criminal and illegal activity violates the Governor's Office Policy and Procedures for Notification of Suspected Illegal or Improper Activity within State Departments and Agencies and ODRC policies.

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

Failure to Follow Crime Scene Protection Policy

ODRC policy *Protection of a Crime Scene 310-SEC-13* advises all employees "… to preserve all suspected crime scenes and notify the Ohio State Highway Patrol of any suspected crime occurring on institutional property … and the crime scene shall remain secured until released by the Ohio State Highway Patrol."

Before finding the two computers on July 27, 2015, MCI Infrastructure Specialist Brady knew that these unauthorized computers were accessing the state network and internet and told investigators: "… at this point I'm pretty sure it's inmates." When he discovered the switch that the computers were plugged into and the cable in the ceiling, Brady had inmates remove the two hidden computers instead of securing the scene and notifying the Ohio State Highway Patrol.

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

Failure to Supervise Inmates and Protect Information Technology Resources

MCI inmates were allowed unsupervised access to computers, computer wiping and imaging software, and computer hardware parts. Moreover, MCI inmates had access to computer cables, power cords, and plywood boards all of which were used to place the two computers in the ceiling. Inmates had numerous unsupervised hours to collect, transport, covertly install, and connect the computers to an unprotected network switch. Inmates routinely used computers in offices without windows or windows that were covered and doors that could be closed.

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

Failure to Follow Password Security Policy

ODRC Information Technology failed to automatically compel employee or contractor users to change their individual passwords every 90 days. During the period of time under review, investigators found ODRC employees were not compelled to change their passwords, in violation of ODRC policy *Information Technology Systems Password and Account Security 05-OIT-17.*

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

Failure to Follow State of Ohio Asset Management Policy

MCI Infrastructure Specialist 2 Carl Brady failed to follow inventory policies and procedures to provide the necessary accountability to comply with state auditing, financial reporting, risk management, and homeland security requirements. Investigators determined Brady's actions were in violation of ODRC policy *Inventory, Donation, Transfer, and Disposal of DRC IT Hardware & Software 05-OIT-21.*

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. 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.

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 Inspectors Office instead of the warden to prevent any perceived conflict of interest or influence. Also since the security of information technology is paramount, institution IT personnel should report to the ODRC CIO to centralize all IT administration, instead of the business administrator.

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

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

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.

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.

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

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.

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

REFERRALS

The findings from this investigation have been forwarded to the Marion County Prosecutor's Office and the Ohio Ethics Commission for consideration.

STATE OF OHIO
OFFICE OF THE INSPECTOR GENERAL
RANDALL J. MEYER, INSPECTOR GENERAL

NAME OF REPORT: Ohio Department of Rehabilitation and Correction

FILE ID #: 2015-CA00043

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
April 11, 2017

Rhodes State Office Tower ◇ 30 East Broad Street – Suite 2940 ◇ Columbus, Ohio 43215-3414
Phone: 614-644-9110 ◇ FAX: 614-644-9504 ◇ Toll Free: 800-686-1525 ◇ Email: oig_watchdog@oig.ohio.gov
The Ohio Inspector General is on the World Wide Web at www.watchdog.ohio.gov

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