
Former OSHP Superintendent Fambro refused to speak with former DHS/ Govt IT Sys Admin on cyber security incidents regarding deletion of drug crime data, videos of Trafficking Incidents, Officer assualting females in Police Dept, compromised BMV Taxpayers and Law Enforcement personal data and other missing Police Public Records #blueleaksohio
RESIGNED
Ohio AG Building State Of Ohio
Docket Case: H2022-003478
makeOHIOgreat.com

DAVE YOST

OHIO ATTORNEY GENERAL

May 17, 2021

Mike Woods, Acting Police Chief
Columbus Police Department
120 Marconi Boulevard
Columbus, OH 43215

Richard Fambro, Colonel
Ohio State Highway Patrol
1970 W. Broad St.
Columbus, OH 43223

Dear Chief Woods and Colonel Fambro:

As you know, Mr. Bob Hinkle, Chief Deputy Auditor for the State of Ohio, re
the state's Unemployment Compensation Modernization and Improvement Co
office's serious concerns after the Ohio Auditor of State' (AOS) recent qualifi
regarding unemployment compensation was issued as part of the FY 2020 Stat

In re claim of:

Brian Weaver - Appellant
*SSN XXXXXXX

*If the complete SSN is needed to identify the claimant, please call UCRC Staff at 1-866-833-8272. Due to privacy laws, the Commission can confirm, but not provide the full SSN.

Claimant Representatives

Employer:

Ohio Department of Public Safety
UCO No.: 0800761001
Issues: DISCH

Employer Representative:

Date this notice mailed: February 01, 2023

HEARING SCHEDULE

DATE AND TIME: February 22, 2023 at 12:30 PM, ET

LOCATION: 30 E. Broad Street, 31st Floor
ODJFS Legal Hearing Room
Columbus OH 43215

Docket No: H-2022003478

State of Ohio
Unemployment Compensation Review Commission
P.O. Box 182299
Columbus, Ohio 43218-2299

DECISION

In re claim of:
Brian Weaver - Appellant

Claimant Representative:
Jessica Olsheski - Olsheski Law Co., LPA

Employer:
Ohio Department of Public Safety
UCO No.: 0800761001-0000

CASE HISTORY

The claimant, Brian Weaver, filed an Application for Determination of Benefit Rights. The Director allowed the application with a benefit year beginning December 27, 2020.

During claimant's employment, he was assigned to attend numerous training courses on cybersecurity. During these courses, employees are told that everyone in the organization has a responsibility when it comes to cybersecurity, and that they should report any potential cybersecurity incidents. Employees are provided with contact information to make such reports. Throughout the DPS building are posters which state "Be A Good Digital Citizen – Cybersecurity Is Our Shared Responsibility." The posters were provided by the Multi-State Information Sharing & Analysis Center ("MS-ISAC"), and the logo for this organization is prominently displayed.

On August 30, 2021, claimant responded to a help desk request from Col. Richard Fambro, Superintendent of the Ohio State Highway Patrol. While claimant was assisting Col. Fambro with his technical request, they spoke about mutual acquaintances and other issues. During this friendly discussion, claimant mentioned that he had some concerns about potential cybersecurity flaws that he had observed in his previous work with a local police department. Col. Fambro thanked claimant for sharing his concerns.

The following day, claimant sent an email message outlining his various concerns to multiple recipients at DPS, and copied several recipients at other Ohio agencies including the Ethics Commission, the Inspector General, the Attorney General, the Public Utilities Commission, and the Auditor's office. In addition, he sent copies to other recipients who had been listed in his training as individuals to notify of cybersecurity concerns, including MS-ISAC. Claimant was discharged the following day for "using his state email account for non-work-related purposes." Claimant had received no formal disciplinary action prior to his discharge.

ISSUE

Was claimant discharged by Ohio Department of Public Safety without just cause in connection with work?

LAW

An individual is not disqualified for benefits if the individual was discharged without just cause in connection with work. *Section 4141.29 (D) (2) (a) O.R.C.*

REASONING

Claimant was discharged from his employment with DPS on September 1, 2021, for "using his state email account for non-work-related purposes." Claimant had received no formal disciplinary action prior to his discharge.

Claimant does not dispute the employer's assertion that on August 31, 2021, he sent an email message outlining his various cybersecurity concerns to multiple recipients at DPS, and copied several other recipients. However, claimant explained that he did so because he had been assigned to attend numerous training courses on cybersecurity, and that he was instructed in these courses to report any potential cybersecurity incidents. He further explained that the non-DPS recipients of the email were contacts provided in the training. Claimant also explained that his job description included promoting systems security and awareness. Finally, claimant stated that he had spoken about his concerns with Col. Fambro, who had thanked claimant for sharing his concerns. Claimant presented credible, sworn testimony that Col. Fambro did not tell him not to share this information. The weight of the evidence shows that the email in question was sent for work-related purposes and therefore does not constitute just cause for claimant's discharge.

The employer argues that there were two prior incidents which contributed to the decision to discharge the claimant. First, the employer argues that claimant had been cautioned for asking why there weren't photos for some employees on the Table of Organization. However, no specific policy violation was alleged by the employer. Claimant explained that he had asked the question because the office location numbers were not always correct on the work orders, and it helped him locate the employees who needed assistance when he could visually recognize them. The Hearing Officer notes that this would not be a valid reason for disciplinary action or discharge.

Second, the employer argues that claimant was cautioned for revealing another employee's personal medical information. However, claimant presented credible, sworn testimony that he was explicitly told that the discussion about this issue was not disciplinary. He further explained that the discussion stemmed from an email he sent in his official capacity because a system update had caused the ZoomText software used by a blind employee to stop working. In this circumstance, the fact that the employee was blind was the sole reason he required the specialized software to do his job. Claimant explained that he had later told his employer that he was particularly interested in helping to fix this problem because of his interest in advocating for other disabled individuals. The Hearing Officer notes that this would not be a valid reason for disciplinary action or discharge.

In light of the evidence presented in this case, the Hearing officer finds that claimant was discharged from his employment with the Ohio Department of Public Safety without just cause in connection with work. The suspension previously imposed upon his benefit rights is removed.

DECISION

The Director's Redetermination, issued December 29, 2021, is reversed.

The claimant was discharged by Ohio Department of Public Safety without just cause in connection with work. The suspension of benefits is removed.

This decision rules only on the issue set forth above.

Emily Briscoe Welter, Hearing Officer

/EBW

Ohio Department of Job and Family Services (ODJFS)

To Enroll, Please Call:
(833) 525-2721
Or Visit:

makeOHIOgreat.com

January 27, 2022

Dear Brian Weaver,

Like the rest of the nation, Ohio experienced an unprecedented number of unemployment claims over the course of the pandemic. Unfortunately, this influx of claims and additional money made it a rich target for criminals. You are receiving this notice because you have informed us that you were a victim of identity theft associated with this criminal activity. Most likely, your personal information was previously stolen—perhaps years ago—and eventually used to file a false unemployment claim through the Ohio Department of Job and Family Services (ODJFS) systems. Over the past two years, ODJFS has made multiple changes to identify potential fraud. You can find more information about those efforts in the "News Room" section at jfs.ohio.gov.

While we have no indication that any ODJFS system has been hacked, we understand that this may have been the first indication that your identity was compromised. Therefore, we have made the decision to offer you one year of identity theft protection services through IDX, a company specializing in these issues. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if you learn of other instances where your identity is improperly used.

#blueleaksohio

Legal Hearing Docket State Of Ohio Docket Case: H2022-003478 at Grove City Council meeting on 3-20-23 of numerous Cyber Security incidents that former OSHP/ DHS Superintendent Col Rick Fambro who resigned from OHSP in Aug and is current Grove City Police Cheif who started in Sept 2022 has announced his resignation abruptly by Mayor Ike after the Legal Hearing Docket was read by former DHS/ OHSP/ Grove City Law Enforcement IT Sys Admin on March 20 2023 during Public Reading with less than 6 months as Grove City Police Cheif.

Chief Fambro is aware of cyber security incidents including deletions of Drug records, Trafficking Involved Videos, Child Sex crime Cover up by Grove City School Teacher, Officer Assualting female civilian videos at Law Enforcement Agencies including the compromised unencrypted DB of BMV data including Ohio Taxpayers and Law Enforcement personal information in violations of FBI CISA laws.

#BlueLeaksOhio
Realtime Video and GPS Tracking of Law Enforcement Crusier Cameras due to Ohio Lawmakers/ Police Admins cover up/ neglect on cyber security issues with unsecured vendors/cloud databases - another Officer in Ohio died on 3-31-22

#BlueLeaksOhio Owning A Cop Car Digital

This Crusier Camera System was tested in City of Gahanna Ohio, where former Grove City Lt is now Gahanna Chief

Grove City Ohio Officers still use same Police Camera Crusier System and OSHP Col. Fambro, AG Yost, and OCJIS is fully aware of issues that real time GPS and cameras/ mic can be viewed externally in 2018/2019/2021/2022/2023

DHS EPA IT Employee kicked out of open public meeting with ODPS/ DHS to prevent truth being revealed while Fambro was OSHP Superintendent

Over 30 out of 40 ODPS IT Staff (DHS, Narcotics and Human Trafficking Unit) and many Law Enforcement Officials resigned in past weeks due fear retailation of documentation of Cyber Issues/ Law Enforcement/ Narcotics Laptops INC5421332 and Records misconducts deleted/missing.

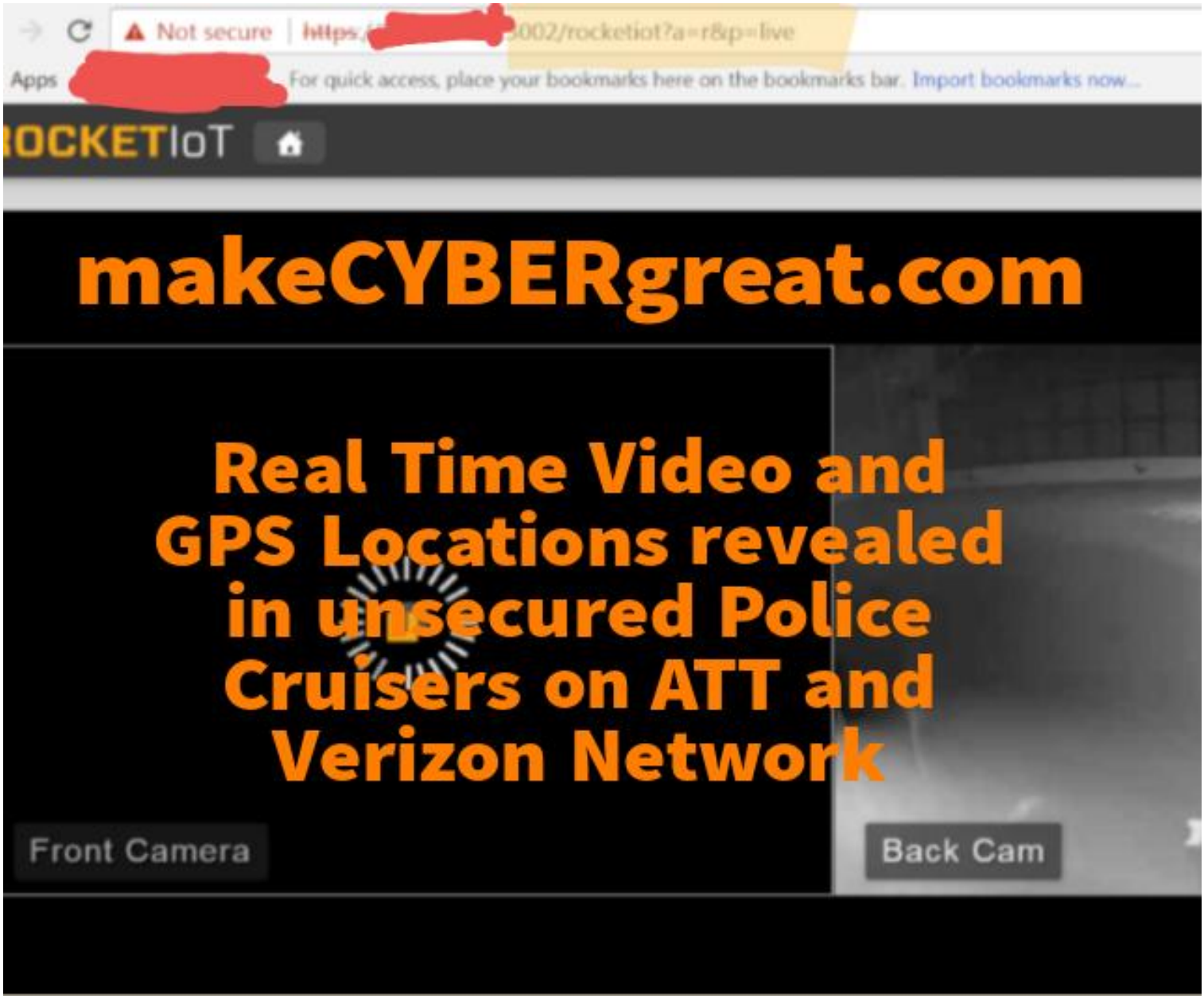
https://www.nbcnews.com/id/wbna42884924

https://www.computerworld.com/article/2471321/hacking-to-pwn-a-cop-car.html

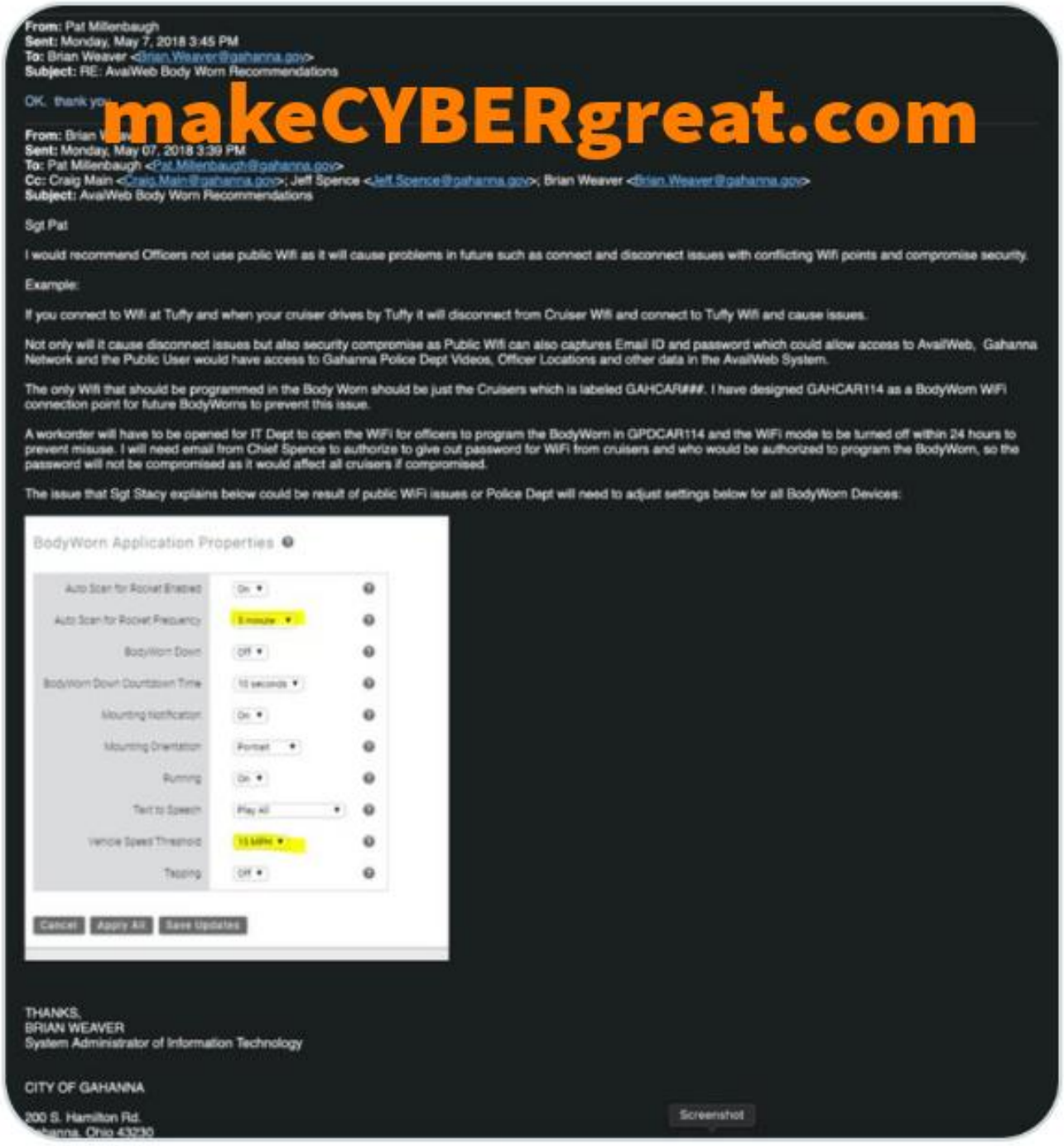
Technical Details
https://bit.ly/3ENE0jL

Video of Grove City Police w/Audio:
https://youtu.be/JbsmWfrkY0Q

The hack was "nothing short of shocking when it occurred in real time," Finisterre said. "There was an officer in his vehicle heading somewhere in traffic in the middle of the day. He was clearly trying to respond to an incident or go where he was told to go, and I was able to see this in real time."


Not secure
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
ROCKETIoT
makeCYBERgreat.com
Real Time Video and GPS Locations revealed in unsecured Police Cruisers on ATT and Verizon Network
Front Camera
Back Cam

Jesus dude, you seriously had to tell them to not connect Police equipment to public **Wifi**? #SeemsLegit



Grove City Division of Police officer Aaron Grassel displays one of the division's new body-worn cameras. The division is using BodyWorn devices, which look like smartphones, made by Utility Associates Inc.

SHANE FLANIGAN/THISWEEK

ALAN FROMAN | THISWEEK | 12:09 pm EST February 3, 2022

#blueleaksohio

Legal Hearing Docket State Of Ohio Docket Case: H2022-003478 at Grove City Council meeting on 3-20-23 of numerous Cyber Security incidents that former OSHP/ DHS Superintendent Col Rick Fambro who resigned from OHSP in Aug and is current Grove City Police Cheif who started in Sept 2022 has announced his resignation abruptly by Mayor Ike after the Legal Hearing Docket was read by former DHS/ OHSP/ Grove City Law Enforcement IT Sys Admin on March 20 2023 during Public Reading with less than 6 months as Grove City Police Cheif.

Chief Fambro is aware of cyber security incidents including deletions of Drug records, Trafficking Involved Videos, Child Sex crime Cover up by Grove City School Teacher, Officer Assualting female civilian videos at Law Enforcement Agencies including the compromised unencrypted DB of BMV data including Ohio Taxpayers and Law Enforcement personal information in violations of FBI CISA laws.

#BlueLeaksOhio
Realtime Video and GPS Tracking of Law Enforcement Crusier Cameras due to Ohio Lawmakers/ Police Admins cover up/ neglect on cyber security issues with unsecured vendors/cloud databases - another Officer in Ohio died on 3-31-22

#BlueLeaksOhio Owning A Cop Car Digital

This Crusier Camera System was tested in City of Gahanna Ohio, where former Grove City Lt is now Gahanna Chief

Grove City Ohio Officers still use same Police Camera Crusier System and OSHP Col. Fambro, AG Yost, and OCJIS is fully aware of issues that real time GPS and cameras/ mic can be viewed externally in 2018/2019/2021/2022/2023

DHS EPA IT Employee kicked out of open public meeting with ODPS/ DHS to prevent truth being revealed while Fambro was OSHP Superintendent

Over 30 out of 40 ODPS IT Staff (DHS, Narcotics and Human Trafficking Unit) and many Law Enforcement Officials resigned in past weeks due fear retailation of documentation of Cyber Issues/ Law Enforcement/ Narcotics Laptops INC5421332 and Records misconducts deleted/missing.

https://www.nbcnews.com/id/wbna42884924

https://www.computerworld.com/article/2471321/hacking-to-pwn-a-cop-car.html

Technical Details
https://bit.ly/3ENE0jL

Video of Grove City Police w/Audio:
https://youtu.be/JbsmWfrkY0Q

The hack was "nothing short of shocking when it occurred in real time," Finisterre said. "There was an officer in his vehicle heading somewhere in traffic in the middle of the day. He was clearly trying to respond to an incident or go where he was told to go, and I was able to see this in real time."

Gmail **Make Deaf <makedeafgreat@gmail.com>**

Cyber Security is Our Shared Responsibility- LEADS, BMV, CJIS

brweaver@dps.ohio.gov <brweaver@dps.ohio.gov> Tue, Aug 31, 2021 at 11:07 AM
To: "JZachariah@dps.ohio.gov" <JZachariah@dps.ohio.gov>, "LShoaf@dps.ohio.gov" <LShoaf@dps.ohio.gov>, "FMoretti@dps.ohio.gov" <FMoretti@dps.ohio.gov>, "ITSupportAll@dps.ohio.gov" <ITSupportAll@dps.ohio.gov>, "Dgatton@dps.ohio.gov" <Dgatton@dps.ohio.gov>, "slmarzec@dps.ohio.gov" <slmarzec@dps.ohio.gov>, "tjbridgman@dps.ohio.gov" <tjbridgman@dps.ohio.gov>, "edburkhammer@dps.ohio.gov" <edburkhammer@dps.ohio.gov>, "jfluebbers@dps.ohio.gov" <jfluebbers@dps.ohio.gov>
Cc: "Brian.Ring@ethics.ohio.gov" <Brian.Ring@ethics.ohio.gov>, "Watchdog@oig.ohio.gov" <Watchdog@oig.ohio.gov>, "siu@ohioauditor.gov" <siu@ohioauditor.gov>, "ContactThePUCO@puco.ohio.gov" <ContactThePUCO@puco.ohio.gov>, "robert.c.richardson.civ@ndu.edu" <robert.c.richardson.civ@ndu.edu>, "bci@ohioattorneygeneral.gov" <bci@ohioattorneygeneral.gov>, "soc@msisac.org" <soc@msisac.org>, "STACC@dps.ohio.gov" <STACC@dps.ohio.gov>, "homelandsec@dps.ohio.gov" <homelandsec@dps.ohio.gov>, "cyber@ohio.gov" <cyber@ohio.gov>, "cengle@dps.ohio.gov" <cengle@dps.ohio.gov>, "OHSCyberTraining@dps.ohio.gov" <OHSCyberTraining@dps.ohio.gov>

ODPS OHSP, IT, CJIS, Traffic, Cyber Team Mgmt

With recent news of Gov DeWine statement:
Ohio Governor Mike DeWine today (Aug 25 2021) applauded the U.S. Air Force's announcement that the Mansfield Air National Guard Base, home of the 179th Airlift Wing, has been selected as the preferred site for the Air National Guard's first Cyber Warfare Wing.

Homeland Security Motto- If you see something Say something

In part of the Job Description as ODPS IT Support, ***"Promotes Systems Security and Awareness by adhering to Agency's and/ or State IT Security Policy and Standards" , which also includes reporting any violations of LEADS/CJIS.***

Keeping line with numerous posters in ODPS IT Dept stating "Cyber Security is Our Shared Responsibility" as ODPS is member per MS ISAC ***(Multi State Information Sharing Analytics Center) along with Jerry Zachariah weekly IT Meetings with Cyber Security Tabletop discussions with employees should be encouraged to report any potential cyber security incidents and should know no penalty for doing so that is also in line with DHS CISA standard in slideshow shown at end of email***.

As an ODPS IT Employee see that ODPS IT Dept, Homeland Security and CyberSecurity is doing much work to keep our BMV, LEADS and CJIS Data secured but ***it does no good if other Law Enforcement Agencies I have been in as IT Staff are not following the LEADS CJIS policies as they are connected to same Ohio Data Sources or no enforcement of policies and giving false statements in LEADS CJIS Audits that is compromising the same data ODPS BMV, LEADS and CJIS*** is trying to protect as I observed increase from 39 daily penetration to 4,000 penetration from former Law Enforcement Agency and told not to document or report numerous cybersecurity issues I observed with LEADS and CJIS Law Enforcement, BMV and Taxpayers data as Ohio Officials and 911 Dispatchers Systems had unauthorized software with piracy Movies and Music connected to LEADS/BMV and was permitted by Administration- it is well known that piracy movies and music has malicious intent to obtain data. If need source documentation let me know and I can help you obtain it.

Whom can I contact and get follow up feedback or perform proper protocol Cyber Security reporting as ODPS IT Employee on observations of following cyber security items and unethical events affecting Law Enforcement below affects Ohio Taxpayers and Law Enforcement databases including LEADS and CJIS?

- Observations of thousands of piracy movies and music, unauthorized software violations from Ohio Official such **as Plex, Windows XP with Dropbox and Remote Desktop enabled on Ohio Govt network connected to Law Enforcement and LEADS Network compromising Law Enforcement personal family data, BMV data and CCW permits holders data** and using non Public Records data for a unauthorized Marketing business (Ohio Entrepreneurship Incubation) on Windows XP with Dropbox and Remote Desktop enabled using Ohio Taxpayers database with no others users permitted to have access?

  Ohio Officials **will not provide Public Records of target and origination IP address of Ohio Official's work issued desktop Plex Servers connected to Ohio Govt Network with LEADS/ unsecured Taxpayers Databases** and no Investigation was conducted or Police Report was not filed even though **CopLogic reports T20000149 and T20000148 were filed with Citizens Online Reporting according to CISA CJIS protocols even** with this **Ohio Official partnered with OSU ten years ago creating largest Chinese Student program in Ohio with Agency's local school district**. Also this Ohio Official Agency has Solarwinds monitoring on network that is based out of Austin Texas near the China Embassy in Houston Texas, where the Dallas PD also deleted 22TB data from cloud services in April 2021 and not reported until Aug 2021 when many Texas Officals were aware of 22TB data deletions and not reported to Texas AG or LEADS/CJIS. Solarwinds- Follow the IP Address and money to non profit organizations and family members. (makeGAHANNAyours, Man can, Ohio Entrepreneurship Incubation)

  Another African American IT staff with "never having access" to LEADS or Law Enforcement data performed same LEADS/CJIS violations with piracy movies and music in 2017 and was filed Police Report 17GAH -19515, was investigated, harassed and terminated when **Ohio Official whom has Admin access to LEADS, Law Enforcement and Taxpayers Network and unsecured Databases along with Tyler Technology Financial Systems and Solarwinds (Ohio Agencies Court, Payroll and Financial Systems) that was hacked months after Ohio Official Plex Server was reported** as Ohio Official was former IT Director for several Ohio Govt Agencies prior to becoming Ohio Official using same admin access accounts with his IT Director access as an Ohio Official using Plex server on Law Enforcement network connected to LEADS/ BMV and unsecured

Taxpayers Databases performed same violations LEADS CJIS activities with no disciplinary action, no Investigation, no Police Report filed when reported to HR Dept by Network Administrator and IT Sys Admin was terminated 6 days later in retaliation for reporting numerous violations of LEADS/CJIS cyber security issues to HR.

- Observations **of numerous unsecured unencrypted DB with Law Enforcement and BMV data stored in Cloud backups and Cloud services not LEADS/CJIS compliance** which states all backups and **Law Enforcement data must be kept on US CJIS cloud services not on foreign servers.**

- Observations with recent Ohio Unemployment fraud of up to $330 millions dollars and millions of Ohioans health and financial security destroyed due not able to get Ohio Unemployment in timely manner as the fraud data have come from data leaks from Law Enforcement and Ohio Officials LEADS CJIS violations unsecured DBs stored on non LEADS CJIS foreign servers from my observations as IT professional, that should be investigated to ensure Ohio Taxpayers, BMV and Law Enforcement data are secure and safe in ODPS mission of

"What will you do today to contribute to a safer Ohio?"

I still not paid Unemployment of 21K due Ohio Systems overwhelmed with fraud and applications and not have ability to use phone to call as can't go to Ohio Unemployment onsite due to lockdown as VRS (ASL Interpreter) Systems disconnects when on hold for long time with Ohio Unemployment.

- Observations of **LEADS, CCW, BMV Data stored in unsecured clear text with any users able to access without any authentication or audit logs of user accessing CAD/ RMS vendor along with third party vendors with no security and authentication required to remotely access Law Enforcement data using third party remote software not FBI CJIS compliance**. Also **numerous LEADS and FBI CJIS Applications including BCI FBI fingerprint machines access accounts stored in clear text format when IT Sys Admin stated needs to be in Keypass or other encrypted password keeper program to comply with LEADS/CJIS a**nd reprimanded numerous times for informing Law Enforcement and Ohio Officials management of cyber issues I observed

- Observations of numerous **Ohio Crash Reports marked non fatality on report but in the Database it is showing marked all fatality** and numerous other errors in Database of Crash Submission reports causing **Ohio Traffic Integrity issues and ORI/ NCIC/LEADS/CJIS violations**

- Observations **of thousands of unsecured unencrypted Ohio taxpayers W2 financial DBs stored on CDs being given to Ohio Officals and sent unsecured** via US mail with no chain of custody.

- Observations of **numerous unlicensed software with unauthorized/unsecured/ unverified LEADS/CJIS network connections on 911 Dispatcher Systems connected to LEADS and Law Enforcement databases**, reprimanded for documenting. This would also be **same third party vendors used at multiple Central Ohio 911 Dispatchers Agencies.**

- Observations **of Law Enforcement videos being manipulated or changed retention dates to delete without Workorders or documentation before sent to Courts.**

- Observations of **140TB of data deleted including Law Enforcement data with no documentation or workorder to cover up data misconducts according to Ohio Sunshine Law**, similar to recent issue of 22 TB of data deleted in April 2021 in Dallas PD with IT Dept demand to be quiet until evidence was found missing in court date couple of weeks ago Aug 21 2021 and now Officials are backtracking their statements while under TX AG investigation. **Ohio Pay to Play IT Services with switching of Phone Systems, Email Systems, Backup Systems, Financial Systems without letting IT Dept know as switched to IT Director and Ohio Officials former employers with kickbacks to non profit , so vendors could delete all old data misconducts before new Ohio Officials Administration arrives in office**

- Observations of **Law Enforcement Milestone Security Camera Systems with Artificial Intelligence/ Facial Recognition being connected to Schools Security Cameras Systems without written School Board or Parents consent since March 2018** without any written documentation or Policy of Security Camera uses in direct violations of Children Privacy Laws. Also **third party vendor has unlimited/ unmonitored third party software remote access to PD Security Camera Server which also connects to PD Network connected to LEADS** in violations of NCIC/LEADS/CJIS. #BlueLeaksOhio

- Observations of **Law Enforcement Cruisers Live Real Time Cameras and GPS able to be reviewed by external hackers /users due to numerous violations of noncompliance LEADS/CJIS passwords not enforced exposing safety of Law Enforcement real-time coordinates and Video/ Audio as Crusiers are connected to Public Cellular IP addresses in violations of LEADS/CJIS**. PD Chief demanded that IT Dept not report any issues when asked, when brought to PD Administration attention of Law Enforcement real time GPS and Camera view exposed by IT Sys Admin #BlueLeaksOhio

- Observations **Drug Door Access Logs are not kept per LEADS/CJIS and deleted, and Law Enforcement Agency states they don't keep Door Access Logs or Phone Logs which is required for LEADS and CJIS**

- Observed of **unreported ransomware that locked/ lost numerous Building permit Inspection Records in City View Building Dept Systems from Ohio Govt Agency connected to City View Connect as this is national Building Dept Inspection Permit Systems used by multiple Ohio Govt agencies including Florida Govt Agencies**

- Observations of deleted Emails, deleted/ missing Elections Data, **all PD Door access logs including Drug Door Evidence logs being deleted in violations of LEADS/CJIS, all phone logs deleted so Public won't know whom is calling who** and Ohio Govt Agency switched Phone Carriers to delete all prior Phone Logs and all new phone calls logs are no longer Public Records as **new phone company is Ohio Official former coworker at ATT with new Phone Company operations out of residential house in violations of LEADS/CJIS on Law Enforcement phone data not safely secured along with evidence of Pay to Play IT Services to non profit organization and family members to secure State of Ohio No Bid Contracts**.

- Observations of **Ohio Elections data being deleted and missing from Public Records Request such as emails and other elections data after numerous cyber security incidents reported to Ohio Officials**.

- Observations of **Unethical Drone use Ohio PD states no data collection or don't maintain drone logs (all Drones have internal flight logs) or no policies of drone use**. No Investigation by FAA to get internal flight logs and FAA reports no flights been called in by Law Enforcement Agency as this would be direct violations of flying without FAA approval as PD Dept 1 mile away from CMH

- Observation of **thousands of Drug and Evidence photos were deleted without Workorders or any documentation by Law Enforcement Administration that IT Sys Admin observed of Law Enforcement misconducts**.

- Observations of **PD Security Camera Videos that was deleted by Administration/ Vendor**. In PD Conference Room would show Lt wearing a black shirt with kahki pants, IT Director wearing light blue shirt, Dispatchers Supervisor wearing black Polo Shirt, Police Officer wearing black t shirt, and myself wearing black striped shirt of harassment as **Law Enforcement Agency Public Records states there is 1 TB of videos as PD conference room was setup to record when motion in room and too large to export but then later all videos deleted/ not available suspiciously and now recording with switch on the wall, when I requested Public Records request of recording of harassment of PD staff meetings** of requesting Workorders and documentation of cyber issues with 911 Systems outages crashes, Corrupted PD reports, Drug Evidence photos deleted, LEADS Account IDs created without Workorders or signed policies and Cruisers Safety issues with electrical corruption of PD reports. Same thing happened with **911 Dispatchers Security Cameras being disabled without Workorders/ documentation to IT Dept- vendors remoted in and disabled with Law Enforcement Administration request to cover up misconducts** - just weeks after Public Records request of numerous misconducts and corruption reported in 911 Dispatchers Room, which is violations of LEADS/ CJIS, along with Door Access Logs deleted/ missing to Dispatchers Room and PD Weight Room where drugs are stored at Law Enforcement Agency.

- Observations of **Ohio Officials and IT Director switching of phone services without letting IT Dept know many Public Safety and PD phone calls were not recording or lost recordings in violations of Public Safety data Integrity**. Pay to Play IT Services with switching of Phone Systems, Email Systems, Backup Systems, Financial Systems without letting IT Dept know as switched to IT Director and Ohio Officials former employers, so vendors could delete all old data misconducts before new Ohio Officials Administration arrives in office including up to 140 TB data.

I also was at DHS Homeland Security Live Exercise Training this past weekend on Aug 28 2021 to assist with Firefighters and Law Enforcement for the training that occurred Franklin County Wide to help do all we can do to make Ohio Safer with current threats in our communities. I worked with numerous First Responders and communicated with several **ATT First Net Technicians on numerous vulnerabilities I have personally observed in several Law Enforcement Agencies on public cellular data networks/ unsecured web applications in direct violations of LEADS/CJIS laws including able to view Real Time Cruiser Videos and GPS coordinates** as an Cyber Security White Hat hacker along with personal Law Enforcement data I have observed since 2015. Also I been working with Law Enforcement Today Agency before Social Media Platforms shut down all Social communications with my LET contacts CEO, as I can't use phone to communicate, as posted some of stories I gave to them of real time Cruiser Videos and GPS on their social media before they were shut down by social media platforms.#BlueLeaksOhio

ATT First Net was wondering why so many Law Enforcement switching Phone Carriers and I informed them due to Pay to Play IT Services I observed and violations of LEADS CJIS and gave them PUCO Case 645541 to investigate why they losing so many Law Enforcement Agencies services.

With many friends and family I have in Central Ohio Law Enforcement, I want to do my part to protect our Law Enforcement. These Law Enforcement Officers whom I played High School Sports, went camping with Boy Scout Troop 241 where the Sgts Father was our Boy Scout Leader when I obtained Eagle Scout rank. Also had a mother of Sheriff contact me personally that her house was targeted as her Sheriff son lives in different house but had her address to target to intimidate her son who is Sheriff of nearby county in Ohio. #BlueLeaksOhio
(Page 41- Virtual Town Hall)

The last Law Enforcement Officer that has contacted me and told me he was targeted was Aug 23, 2021 and another one informed me Aug 29 2021, he resigned from Law Enforcement due to lack of protection from Administration and Ohio Officials and been in Law Enforcement for over 20 plus years, as many other resigned Officers in past years also reported similar stories to me personally. #BlueLeaksOhio

There needs to be accountability in Law Enforcement Internal Affairs to gain public trust and Law Enforcement trust as attached Public Records I obtained from another Agency provided me states retired and current Law Enforcement don't trust Internal Affairs:

Law Enforcement Chief admits K9 attacked female PD Front Desk Civilian on mouth and bleeding- No Incident Report, No Investigation, No OHSA Report, No required Use of Force, No Required Reported K9 Incidents as cover up by Law Enforcement Officals as it happened outside of my IT Office and female was Lt Professional Assistant Daughter in Law. Lt did not perform any investigation and transferred to another Law Enforcement Agency to cover up misconducts. **Hallway Security Camera was deleted that would show the K9** and PD Female Civilian husband wearing black shirt with white designs on front and back who is Lt's Professional Assistant Son coming inside PD yelling and threatening to sue PD Dept for no Investigation and allowing K9 to attack his wife. Shortly after - female and Lt transferred to other Law Enforcement Gahanna and became Chief without investigation to avoid investigation and cover up numerous misconducts in Agency.
K9 works with kids at schools (Page 28- Virtual Town Hall)

I had meeting with Law Enforcement Chief regarding unauthorized Shooting/ K9 Assault/ BlueLeaksOhio on 8-28-20 requested transcript and had another meeting with Grove City Administration again Feb 2021 stating they already had transcript of 8-28-2020 meeting and "did not know I wanted it still" on Feb 20 2021 as transcript was allegedly already completed and will give it to me in couple of days, but **transcript is dated March 15 2021 was not given until 6-3-21 and K9 had "Surgery" on 6-8-21 and died 6-9-21 in attempt cover up misconducts in PD Drug operations** as again Public losing trust in Law Enforcement with false information given on Police Miscommunication in shootings, Assault and PD Data leaks reported by IT Depts. (Page 28- Virtual Town Hall)

K9 was Drug and Trafficking, only attacks when smell Drugs or ordered to attack

Officer that performed **the unauthorized shooting took all the evidence and uploaded the "evidence" pictures with no accountability of another Officer performing the tasks** which shows lack of accountability in Internal Affairs

HR Director that had retaliation complaints filed on her performed the Internal Affairs investigation interviewing the person filing the complaint for Internal Affairs, instead of another HR person that was to do the Internal Affairs investigation.

I setup Law Enforcement Phone Systems and the **Anonymous Tip Line is not Anonymous as IT Dept gives the caller ID to Law Enforcement and this seriously loses people trust in Law Enforcement for leaving tips for Drugs and Trafficking with numerous deletions of phone logs, drug photos, evidence photos and trafficking photos I observed to cover up numerous Law Enforcement misconducts** as Sgt Greg Barber even admits corruption in Law Enforcement with Drug/ Trafficking Task force along with several of my Law Enforcement Officers friends that has admitted to me after they retired or resigned recently due to observations of internal corruption themselves and encourage me to keep exposing the corruption, so future Law Enforcement Officers can have a chance to be trusted again once corrupted Officers/ Administration are removed as Ohio AG Organized Crime Unit is located inside Grove City Police Dept where I have worked for 10 years setting up numerous 911/ Phone/ Security Camera Systems and Cruisers GPS Dash Cameras. Many are fearful to report as afraid to lose Law Enforcement pension and benefits or retaliation.

I repeatedly asked Law Enforcement and Ohio Officials to put in writing per ADA in a Workorders of what data to be deleted or IDs to be created as some IDs were not employees with Law Enforcement/ Ohio Agency or not signing the LEADS CJIS and Computer policies when have direct access on Law Enforcement Agencies databases. They said we don't do that here **and harassed me weekly as I was documenting cyber issues, with "planned" electrical outages corrupting Drug Reports, Phone Reports, Evidence, Dispatchers and 911 Services and Radio Systems. Resulted in intimation by Law Enforcement and Ohio Officials management saying in meetings turn up f.. belltones, you motherf... idiot, stupid men... disabled people can carry themselves up steps (elevator not working at Law Enforcement Agency) then repossessed my new hearing aids I been wearing for a year with no issues after reporting harassment and misconducts to HR.**

City Council President is Ohio Attorney General and Board of Elections Supervisor is unethical conflict of interest to protect parties involved.

I would like to request if a meeting of how to properly resolve or report and discuss the items above to protect ODPS BMV/LEADS/ Ohio Taxpayers data, to have ASL interpreter present with written transcript of meeting , as when I get nervous I revert to primary language ASL and may need Interpreters to communicate effectively.

It would be best to do **onsite visits at Law Enforcement Agencies as LEADS Audit as many of items are technical with Audit Logs to follow the violations and I can show the numerous vulnerabilities with LEADS/ BMV in real time and request everything be video recorded as I show the cyber security issues in real time affecting multiple 911 and Law Enforcement Agencies due to neglect of enforcement of LEADS/ CJIS policies and false statements made by IT Directors in LEADS CJIS Audits** I and Network Admins were demanded/ intimidated not to disclosure or be included in LEADS Audit meetings to hide misconducts and numerous cyber security LEADS CCJIS issues

Some of the best security advocates are the ones that lived through the trials in real time, to share their real life experiences to protect the next generation of security exploits such as Deaf FBI Agent Susan Thomas (Movie FB Eye).

Per Col Fambro own words- *"It will take a community - If you don't have the cooperation and relationship with courts it is much more difficult to accomplish the goal" (my addition) of earning Public's trust in Law Enforcement Agencies in the communities and keeping Ohio BMV, LEADS and Taxpayers data secured.*

I am being now placed I position where I am a man of Integrity and will be under Oath and will have to reveal that I work at ODPS and will have to testify and produce same evidence of what ODPS Directors and Management have with numerous evidence #BlueLeaksOhio presented to investigate the exposed LEADS, BMV, Ohio Taxpayers and CCW and numerous LEADS/CJIS violations and don't want to put the ODPS Management on this email list in bad negative light or embarrassment of not knowing the numerous LEADS/CJIS violations that has been revealed in this document.

Technical Details Documentation
https://bit.ly/3jkAzcz

I can provide additional evidence, audit logs, staff meeting recordings and screenshots upon request as I want to Make Ohio Great place to live and work, as I still not been provided in Public Records request from numerous Agencies attempt to cover up numerous Cyber Security issues with Ohio Govt Law Enforcement, LEADS, BMV, and Taxpayers data.

As currently, I am working under Gov DeWine Executive Order 2019 3D with placement by Ohio Dept of Disabilities as Part Time Information Systems looking to obtain Full Time ODPS as Cyber Security or ODPS Forensic Investigator with my 15 years of IT Law Enforcement cyber security LEADS CJIS experiences to keep Ohio Taxpayers, BMV, LEADS data safe and secure with the thousands of data sources I have gathered past 15 years to share numerous cyber issues within State of Ohio regarding LEADS, BMV, Law Enforcement data and Taxpayers data

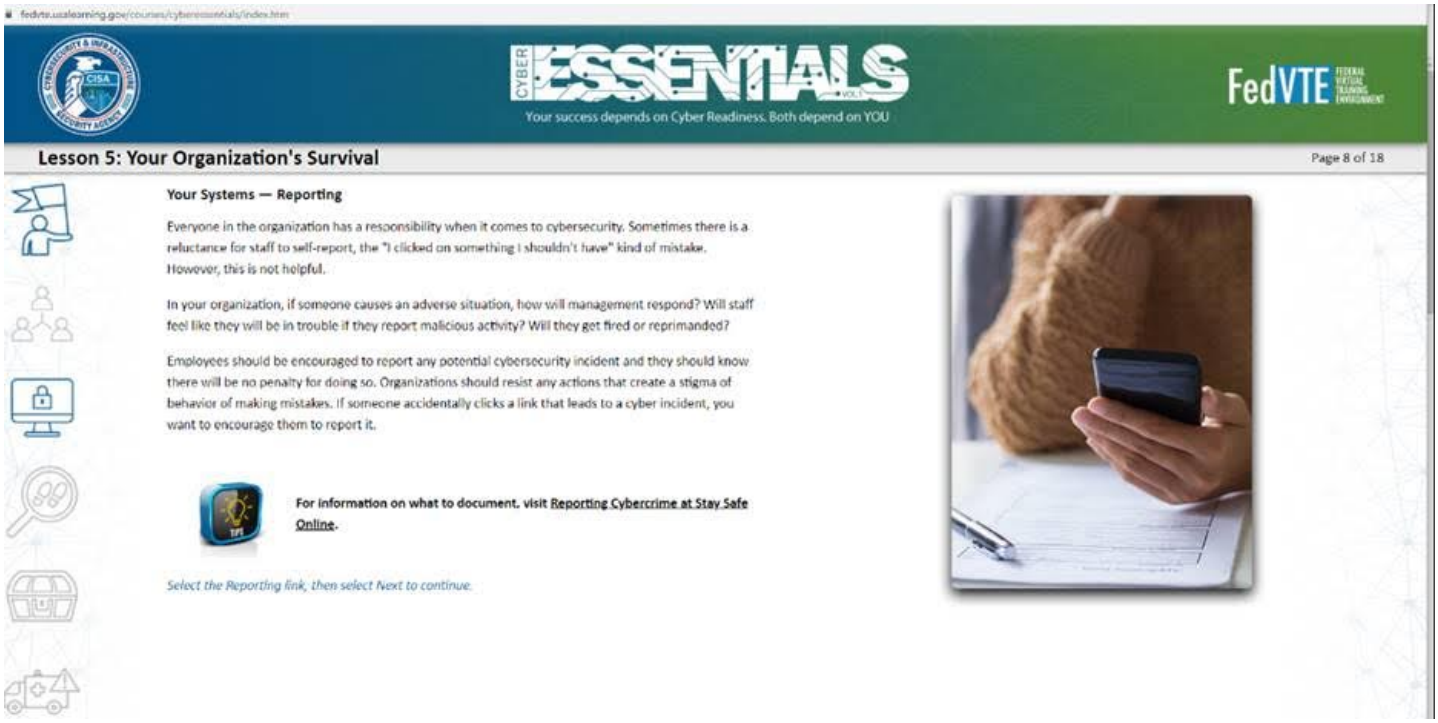
Technical Details Documentation
https://bit.ly/3jkAzcz

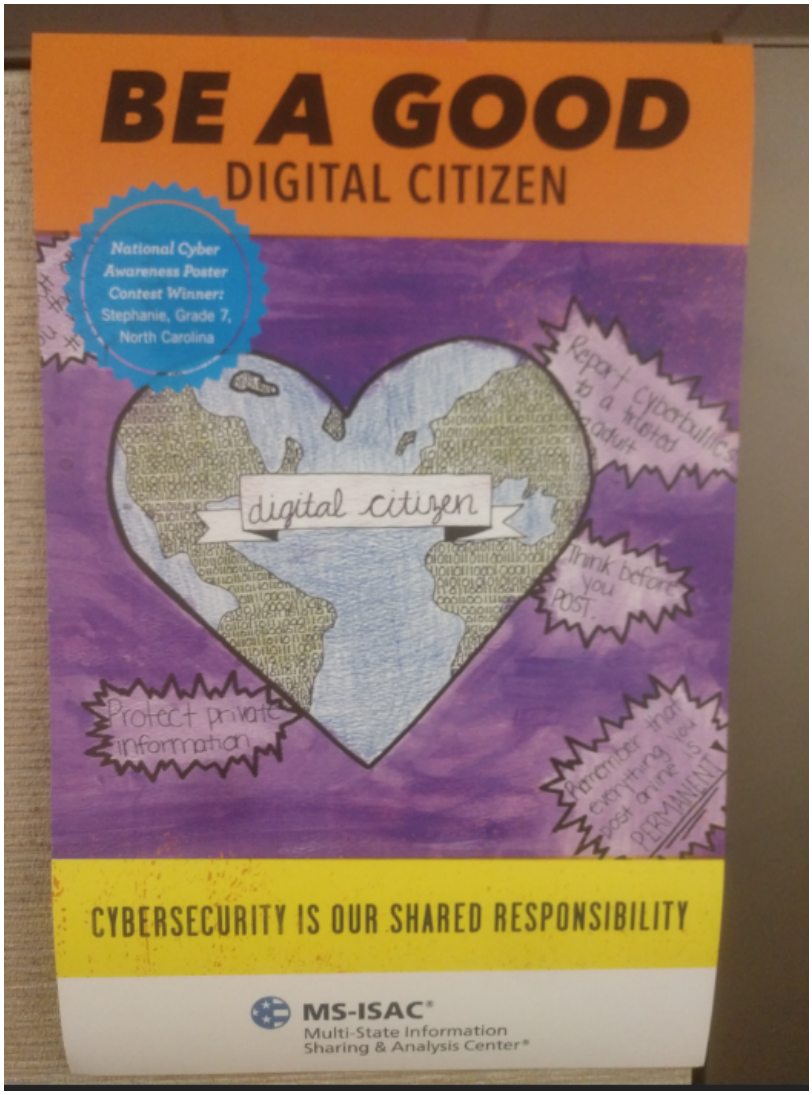
Attached are my certificates of following

- CISA Security
- FBI/CJIS Security
- Ohio Sunshine Law
- Ohio Ethics
- Solarwinds Certified

Please excuse my written English as ASL is not english and feel free to correct any grammatical differences into english

If need any additional information please let me know





Brian Weaver

Ohio Department of Public Safety

Office of Information Technology

1970 W. Broad Street, Columbus, OH 43223

brweaver@dps.ohio.gov

614-644-2921

Ohio | Department of Public Safety

---

5 attachments

Encourge to Report Cyber Issues CISA Slide.PNG
986K

non CISA Weaver Cert June 22 2021.pdf
1617K

CISA July 27 2021 Combined.pdf
573K

8-28-20 Grove City Division of Police Virtual Town Hall full size.pdf
518K

Weaver Ohio Unemployment _Redacted.pdf
171K

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

makeOHIOgreat.com
“Protect Our Community and Kids”

Subject RE: Incident INC5554288 Assigned to DPS - PC Support: DPS - URGENT - Colonel Fambro's printer in his office is not loading paper

To: [rsfambro@dps.ohio.gov <rsfambro@dps.ohio.gov>]

From brweaver@dps.ohio.gov <brweaver@dps.ohio.gov>

Date Mon, Aug 30, 2021 at 2:28 PM

Col Fambro

I know several people in Law Enforcement in Central Ohio Agencies and US Military, as they are my family members and many close friends including some from my childhood in School and High School Sports. Several of my friend's fathers were my Boy Scout Leaders and we all went camping together every month in Boy Scouts, I obtained my Eagle Scout Rank in Lancaster Ohio when you were Command Post in Lancaster in 1999. I still have the OSHP plastic badge somewhere in my childhood box, I received in Boy Scouts for Merit Badges.

I will do everything in my capability to protect my family members and close friends from childhood, as I know Law Enforcement are targeted with current worlds events with their mothers very concerned contacting me directly in person past several months, as their houses have been targeted recently but scared to report it for fear of retaliation of exposing Law Enforcement personal data has been exposed on Ohio Govt networks by Ohio Officials as far back as 2018/2019 that has been reported to numerous Ohio Officials Agencies with no resolution or investigation per Public Records emails I have been given by Law Enforcement staff – now recently involved with Ohio Unemployment fraud and hacks not be investigated as personal friends of several Law Enforcement Agencies have informed me privately and providing me Public Records and emails due to fear of retaliation of personal unsecured Ohio taxpayers and Law Enforcement databases exposed due to neglect of FBI/CJIS laws, they and myself has observed.

The last Law Enforcement Officer that has contacted me and told me he was targeted was Aug 23, 2021 and another one informed me Aug 29 2021, he resigned from Law Enforcement due to lack of protection from Administration and Ohio Officials and been in Law Enforcement for over 20 plus years.

So I promised the mothers and Law Enforcement friends and Officers I will protect them and to ensure our Law Enforcement personal data is kept secured with my 20 + years of IT Cyber Security/ Forensic experiences, as I would love to get FT Job at ODPS as Cyber Security or OSHP Forensic Data Investigator as currently I am currently PT as IT PC Support with Gov DeWine's OOD Disabilities IT Apprentice program.

I also was at Homeland Live Exercise Training this past weekend on Aug 28 2021 to assist with Firefighters and Law Enforcement for the training that occurred Franklin County Wide to help do all we can do to make Ohio Safer with current threats in our communities. I worked with First Responders and communicated with several ATT First Net Technicians on numerous vulnerabilities I have personally observed in several Law Enforcement Agencies on public cellular data networks/ unsecured web applications in direct violations of FBI/CJIS laws including able to view Real Time Cruiser Videos and GPS coordinates as an Cyber Security White Hat hacker along with personal Law Enforcement data I have observed since 2015. Also I been working with Law Enforcement Today Agency before Social Media shut down all Social communications with my LET contacts I been working with as I can't use phone to communicate as they posted some of stories I gave to them of real time Cruiser Videos and GPS on their social media before they were shut down by social media platforms.

I would recommend maybe an Anonymous tip line for Law Enforcement to call, so they can report without fear of retaliation of reporting being targeted, so Law Enforcement Administration will know how big the issue is in Ohio, with the amount of data I have received from Law Enforcement and mothers in past two years are concerned as it is alarming with the data I have been collecting for past several years from Law Enforcement privately from retired, resigned, and current Officers off duty and on duty.

I am looking forward in any way I can do to help community advocating for ODPS “Communication Disability Law” mission of “What will you do today to contribute to a safer Ohio” with State of Ohio to make Ohio great place to work and live.

Please excuse my written English as ASL is not english and feel free to correct any grammatical differences into english

If you need assistance with anything else feel free to contact me and have a great week and stay safe.

Brian Weaver

Ohio Department of Public Safety

Office of Information Technology

1970 W. Broad Street, Columbus, OH 43223

brweaver@dps.ohio.gov

614-644-2921

Ohio | Department of Public Safety

From: Fambro, Richard <rsfambro@dps.ohio.gov>
Sent: Monday, August 30, 2021 12:22 PM
To: Weaver, Brian <brweaver@dps.ohio.gov>
Subject: Re: Incident INC5554288 Assigned to DPS - PC Support: DPS - URGENT - Colonel Fambro's printer in his office is not loading paper

Weaver, first, thank you for taking care of my printer issue! I’m not sure how I jacked it up, but I’m so glad you were able

To resolve it!

OMG, it's a small world! Are you talking about Tim and Francis Gillis???

Sent from my iPhone

On Aug 30, 2021, at 12:04 PM, Weaver, Brian <brweaver@dps.ohio.gov> wrote:

Col Fambro

I was able to successfully resolve the Lexmark Printer (B18001529) not loading with "Paper Error Code 34". Couple of issues I found listed below when troubleshooting and corrected printer settings and all is operational.

- Paper Tray Size was in unlocked position and on Legal Paper Size
    - Trained Christi Hawk in event the Lexmark gives Paper Tray error in future when reloading Paper
- Paper Tray in the Lexmark Settings was set to Legal Paper in Tray 1
- Verified all Windows and Security Updates were successfully applied on your Desktop

I enjoyed reading the Newspaper articles on your Office Wall regarding your story how you rose through the ranks and demonstrated strong relationships with Ohio communities to be Col for OSHP. As a close friend of mine a retired Dayton Post Dispatcher and her retired Sherriff husband speaks highly of you and shows your true character as an "Community Relationship Advocate", as they worked with you in Dayton/ Springfield Post Dispatcher Office and as OSHP Cadet and remember you getting Trooper of the Year award in 1994. Reading the newspaper articles confirmed the great stories my retired Dayton Dispatcher/ Cadet friend have told me in the past months regarding their relationship with you in Dayton/Springfield and OSHP, since they learned I work as IT Professional at ODPS Shipley.

I am looking forward in any way I can do to help community advocating for ODPS "Communication Disability Law" mission of ""What will you do today to contribute to a safer Ohio" with State of Ohio to make Ohio great place to work and live.

If you need assistance with anything else feel free to contact me and have a great week and stay safe.

Brian Weaver

Ohio Department of Public Safety

Office of Information Technology

1970 W. Broad Street, Columbus, OH 43223

brweaver@dps.ohio.gov

614-644-2921

<image001.png>

From: State of Ohio <das.customersupport@das.ohio.gov>
Sent: Monday, August 30, 2021 10:56 AM
To: Maddox, Brandon <bmmaddox@dps.ohio.gov>; Camara, Oumar <OCamara@dps.ohio.gov>; Hammond, Charles <CHammond@dps.ohio.gov>; Merencio, Renee <rlmerencio@dps.ohio.gov>; Sarnor, Ahmadu <azsarnor@dps.ohio.gov>; Hill, Jemel <jbhill@dps.ohio.gov>; Watts, David <dcwatts@dps.ohio.gov>; Caron, William <WCaron@dps.ohio.gov>; Shah, Hetal <hmshah@dps.ohio.gov>; Bridgman, Thomas <tjbridgman@dps.ohio.gov>; Damier, Yvens <ydamier@dps.ohio.gov>; Weaver, Brian <brweaver@dps.ohio.gov>; Bearns, Christopher <cjbearns@dps.ohio.gov>; Hall, Keith <kahall@dps.ohio.gov>
Subject: Incident INC5554288 Assigned to DPS - PC Support: DPS - URGENT - Colonel Fambro's printer in his office is not loading paper

Incident: INC5554288

Title: URGENT - Colonel Fambro's printer in his office is not loading paper

State: Assigned (Group)

Requester: Christi Hawk

Requester division: OHIO STATE HIGHWAY PATROL

You will receive emails from the State of Ohio whenever there is activity on your Incident.

If you have an internal State of Ohio User Account, you may optionally review your Incident by selecting "Take me to the Incident". You will be required to log in using your state ID and Password. External users will not have access, but will be able to follow the Incident updates via email.

Take me to the Incident

Priority: 4 - Low

Category: Printer / Scan Device

Comments:

DPS Service Desk | 614-752-6487 | ServiceDesk@dps.ohio.gov

Ref:MSGOH55916532_AIheMZiVkmxJokdeh

Subject: FW: New IP cameras Search Failing on MileStone Servers

Brandon:

Sound Communications trying to add the AXIS Cameras into Milestone but we will need the following port and services opened on switches to perform the scan from VLAN [redacted] I have CC the tech from Sound Communications if need additional clarification. I will be leaving for an appointment at 3:30 today and can assist tomorrow if needed.

Is there any plans to have a separate VLAN for Cameras to reduce traffic interference?

[redacted]-VIDEOMGMT Server Name
[redacted] IP Address

Cameras to search Mac Address:
accc8e9b3[redacted]
accc8e9b39[redacted]

AXIS Software Search Tool

Port 5353 UDP uses BonJour Services ADM/ ACM Server and Device mDNS Discovery search for cameras Multicast 24.0.0.251

THANKS,
BRIAN WEAVER