The Geauga County Automatic Data Processing Board met on Thursday, October 9, 2025, at 11:00 a.m. at 231 Main Street in the Appraisal conference room and via Microsoft Teams for a Special meeting. **Members present:** Chuck Walder, County Auditor; Michael Risko, representing Celesta Mullins, County Recorder; Caroline Mansfield, representing C.P. Hitchcock, County Treasurer; Michelle Lane, Board of Elections Director; Scott Hildenbrand, County Sheriff; Sheila Bevington, Clerk of Courts; Jim Flaiz, County Prosecutor; Carolyn Brakey, County Commissioner; Nora McGinnis, Board of Elections Deputy Director; and Andrew Haupt, County Engineer.

Also present: Pam McMahan, Chief Operations Officer; Frank Antenucci, Chief Deputy Administrator; Carol Benton, League of Women Voters of Geauga; Samantha Harris, Prosecutor's Office; Zach McLeod, ADP; Joe Birli, ADP; Akshay Raikar, ADP; Chief Tom Swaidner, Russell Township Police Department; Lieutenant Scott Lillash, Russell Township Police Department; Emma MacNiven, Geauga Maple Leaf; Diane Jones and Ryan Patrick from Simvay, LLC.

Absent: John Urbancic, M.D., County Coroner, and Common Pleas Court Judge.

Update on Russell Township Police Department Request

Request to maintain the Russell Township Police Department domain block until ADP staff is satisfied the block can be lifted; the matter would only come before the Board in the event of an impasse.
Motion: by Jim Flaiz, seconded by Chuck Walder, to maintain the Russell Township Police Department domain block until ADP staff is satisfied the block can be lifted, and the request does not need to come before the Board again unless there is an impasse.

The Russell Township Police Department came to the Board to request removal of the domain block.

On September 30, Russell Township appointed Kristina Port, who is the board chairman, to serve as Russell Township's incident response lead and legislative authority designee for the cybersecurity reporting requirements. Generally, an elected official is not used as an incident response lead. Typically, someone is appointed because their duration is more predictable than that of an elected official, whose term is every four years. Russell's policy requires the appointed lead to be the reporting agent. The Request for Removal form was not signed by Kristina Port, the incident response lead. Chuck is concerned that ADP is considering a form that is not signed by Russell's incident response lead.

Jim Flaiz stated he was offended after reading the report from the vendor. Jim felt it was very unnecessary to include an entire section of the report accusing an ADP employee of being unethical. The vendor accused ADP employees of conjuring up a plan to obtain Russell Police business. Jim believes this is 100% the vendor's fault. Instead of being professional with the ADP staff and working toward a solution, they immediately launched accusations. Since the vendor has been involved with the remediation form, Jim does not want to approve it, as he has zero faith in the vendor.

Chuck did not show the Board the balance of the vendor's final document because he wanted to de-escalate rather than escalate. The report contained more emotion and opinion about ADP's processes, operations, and protocols, and less about the incident and what was done to fix it. Chuck stated they had very limited data at the onset of this exposure. They were initially told this was a deployment of an MFA update. After they discovered DNS issues going to Russia and Spain, the Board was told this was normal because SentinelOne is a global company. ADP believes this is a Direct Send issue. An outside consultant also advised the Board that this is a Direct Send issue.

Direct Send became nationally publicized as having a vulnerability. There was no evidence that SPF was enabled in the environment. ADP immediately contained the issue when they received an alert from the CrowdStrike Falcon agent. ADP was told verbally by the vendor that they were doing an update and that this was normal, but ADP did not believe that to be true. The DNS requests got through the connection from Spillman and were captured on the county umbrella, which could have been catastrophic.

In good faith, Chuck cannot recommend lifting a blocked domain during an election lockdown and putting the county at unnecessary risk.

Jim asked if Direct Send was turned off. Frank stated the domain unblock form does indicate Direct Send was remediated. Chuck added the report that was provided did include a screenshot of a PowerShell window where they toggled the switch for Direct Send. However, there are also other steps recommended. CISA recommended immediately toggling off Direct Send. The Russell Police Department turned off Direct Send two days after the incident occurred.

Sheila asked what is occurring that is affecting Russell's ability. Chief Swaidner stated the biggest issue is a lack of communication between the Sheriff's Office, Prosecutor, and the Courts. The functionality of the police department is significantly affected. He also stated they do not have full access to Spillman. They can use Spillman on the Mobile Data Terminals (MDTs) but not on the workstations.

Jim stated they need to clamp down on entities that are not under ADP that have access to Spillman. Chuck stated the arguable issue is whether this is in the eradication or the recovery stage. MDTs are considered OT (Operational Technology), not IT (Information Technology). It is a function of the Sheriff's Office to deploy a product that the Sheriff's IT staff maintain, monitor, and set regulations on. When it bumps up against the IT of the County, ADP must become aware. Chuck's concern with the use of MDTs out in the field is that their credentials are very high, typically administrative credentials. That is problematic because if those credentials were user-based, then someone could not install a program because administrative credentials would be required. Anything that comes through the County network on a VPN is automatically higher risk.

Carolyn asked if ADP saw data leaving the police network. DNS requests, not data, did leave the police network and got into the county umbrella. There is an internal alert within umbrella that captures potential threats. Three were blocked; one went out.

Ryan stated that other than the DNS request being resolved, there is no information that would indicate any type of compromise. It is an indicator that something could be wrong, but he believes you do not launch a full incident response process based on that information. Ryan has not heard any evidence to stop the Russell Township Police Department from emailing. The DNS requests are device network communication items, which do not have anything to do with email communication, which occur through Microsoft systems. No one from the County or ADP received any phishing emails from russellpolice.com. The vendor was able to substantiate that there was no risk.

Carolyn asked Ryan how confident he was that this was a setup error and not an intrusion. Ryan stated he is 100% confident. He only had 20 minutes of logs from when SentinelOne was on the device. He was able to clarify items that ADP and their findings have already provided. Ryan stated they are making sure they are answering everything one by one. Direct Send is a vulnerability associated with people who have secure email gateways. There is almost minimal risk for Direct Send when you are using Microsoft protection. When a layer is added on top of that, you expose yourself to direct vulnerabilities, which is why the mitigation was happening in tandem with the other projects. The confusion and frustration from Ryan's side comes from the fact that there is no substantial evidence or security reasons to prevent Russell Police from using their email and unnecessarily restrict the department's ability to communicate.

Carolyn asked Frank and Zach if they agreed with Ryan. Frank replied that he agreed that ADP blocked the domain as part of the standard process. ADP blocks a domain very quickly when CrowdStrike alerts them that there could be a compromise on machines touching the domain. They operate in a zero-trust environment. The matter then comes to the Board, and the Board makes the decision to unblock based on the data received. The initial unblock form ADP received from Russell Police did not provide any insight. A week later, they received a lengthy report, which is not ADP's standard process or policy. Regardless of what people outside of the Board or County think about ADP's policies, this is their policy to protect the network. There might be some consternation over three or four weeks for Russell Township, but ADP's responsibility is to protect 300 million dollars in taxpayer monies.

Carolyn asked if there was any evidence that an email was compromised. Zach stated that for the DNS requests to show up in the environment, Direct Send had to have been turned on. The attacker sends phishing emails to users in their environment. They would have had to interact with it or open an attachment to an email for those requests to appear. DNS requests do not just show up for no reason. ADP has very specific policies and procedures. ADP looks at the logs to determine what made the request, and sometimes it is benign.

Ryan disagreed with Zach. The way Outlook desktop functions is that if you receive an email from a source you have not received from before, there is an option to trust or not trust it. If it is not trusted, certain images and links will not load ahead of time. This is because images and links within that email do reach out over the internet and provide feedback. That is standard SOP for how Outlook desktop works. There is only evidence that whoever logged in to the laptop received a phishing email; however, that does not mean the user took any action or was compromised in any way.

Zach replied that because this was Direct Send, these were specifically spoofed phishing emails.

Jim stated the ADP Board is overly conservative and sometimes a big pain, but it is worth it because they do not have any issues. ADP owes it to the taxpayers to keep the county network safe. They represent all the taxpayers.

Chuck asked Ryan if they enabled strict DMARC and SPF records. Ryan indicated the form is geared toward a user or a domain where that user has been compromised. If there is no such evidence and you are spoofed, you are not compromised. Compromise is the actual takeover of a user or device. Frank clarified to the Board that their form is intentionally open-ended so a narrative can be provided describing what was done. Chuck told Ryan that if strict DMARC and SPF records were enabled, it should have been included on the form.

Carolyn asked what Zach and Frank would like to see from the Russell Police Department so they can email again. Zach stated he would like to see a log showing where the DNS originated. They know it did not occur on just one computer. Every time the Russell Police sent their deployment package, ADP could see the DNS requests. They would like to see logs indicating the activity is benign. They want to ensure there is not an active compromise or infection in the environment.

Ryan stated he provided logs from their Sentinel agent that was on the device for 20 minutes. The Excel file is fully embedded in the PDF, which contains thousands of lines for review. The CrowdStrike agent was present for an extended period of time on the SRO laptop. The log should be available in CrowdStrike, which shows the full event history for the installation of SentinelOne and where the calls originated. Zach told Ryan they did see the log, but it does not make sense, which is why they are asking for his assistance with it.

The Sheriff feels Ryan and Zach need to get together and figure this out. They need to satisfy each other and come up with a solution so Russell can have email again. Chuck stated he attended a Russell Trustee meeting a few weeks ago and told them they could request a temporary email address under the umbrella domain of the Russell Trustee and communicate the next day.

Jim agreed with the Sheriff; Ryan and Zach need to get together, and if the matter is resolved to the satisfaction of the ADP staff, then the domain can be unblocked. Jim feels the unblock should occur after the election.

Frank stated ADP needs to be satisfied. They are welcome to come to ADP, and ADP will mediate and obtain the necessary information. Michelle stated that if ADP understands and recognizes all the requirements of the Secretary of State and feels comfortable that the situation has been resolved, then the block can be lifted.

The Sheriff stated he does not believe this should come before the Board unless Ryan and Zach reach an impasse.

Voice votes: 10 ayes, 2 absent, 0 abstain. **Motion carried.**

Regular Business
None

Public Comment
None

BEING NO FURTHER BUSINESS TO COME BEFORE THE BOARD, Caroline Mansfield motioned to adjourn.

Respectfully submitted,

Charles E. Walder, Auditor
Secretary/ADP Board

Michelle Lane
Board of Elections Director

Sheila Bevington
Clerk of Courts

Celesta Mullins
Geauga County Recorder

Scott Hildenbrand
Geauga County Sheriff

Nora McGinnis
Board of Elections Deputy Director

Andrew Haupt
Geauga County Engineer

Christopher Hitchcock
Geauga County Treasurer

Abstain WAS not present
Carolyn Brakey Spidalieri
Geauga County Commissioner

James R. Flaiz
Geauga County Prosecutor

John Urbancic M.D.
Geauga County Coroner

Common Pleas Court Judge