This is a follow up document to our 9-01-21 meeting where Albert / CIS was discussed.

The Albert Sensor is currently provided at no charge to WA Counties by the SOS and managed by The Center for Internet Security/CIS. CIS is a non-profit with ties to Democracy Works, which is a member of the Bridge Alliance.* CIS has deployed the Albert Sensors in most all states including WA. Its function is to monitor county network traffic, looking for malware intrusions and provide alerts to users.

More specifically, Albert is being promoted as providing security for election systems via the Election Infrastructure Information Sharon and Analysis Center (EI-ISAC).

In our WSRP EIC 9-1 meeting, Cyber Symposium Data Analysis Specialist Sean Smith from Colorado spoke and answered questions about the Albert monitoring system, which is entirely internet based, saying Albert is not even remotely possible as a security system due to its ease of hacking and attack. IT Expert Trevor Marquis of Skamania County EIC spoke about Albert / CIS and the lack of security because of the internet connection. This violates WAC 434-335-040 (3 c, d).

Also, Lincoln County Chair Mary Blechschmidt shared their county's experience with Albert / CIS as they never wanted it and were pressured by the WA State SOS and the DHS to have it installed.

In 2018-19 Lincoln County (LC) was approached by the SOS, as were many counties, to sign an agreement to have Albert installed/hooked into the WA county network, to make it more Secure." It was explained that LC's network was already covered by a security system. But the SOS and the DHS said Albert would be additional security. After a heavy-handed pressure approach from the SOS / DHS, LC agreed to take on Albert and signed an agreement in Oct 2020. Weeks later, following the 2020 Nov election, LC was the victim of a ransomware attack. There is no proof that Albert played a part in the hack. However, CIS NEVER alerted LC to the ransomware hack, as would be expected. Okanogan County was also the victim of a ransomware hack in Jan 2021.

Mary encouraged all counties to verify if they have Albert (ask your IT department, or even do a FOIA request). If your county has Albert, advocate having it removed from the county auditors' offices.

Also, last week I spoke to Joe Carter with the Technology Services Department at Grant County. He is the IT official for Grant County who declined Albert. Grant County was approached multiple times by people from the WA SOS. Joe was asked repeatedly to have Albert installed, and his answer was always emphatically "No" for the following reasons: ·

- Albert comes free and installed (to the county). Something worth having isn't usually free. This was an initial red flag.

- In the rules and stipulations that govern the use of Albert, it states that Albert will listen to ALL data traffic on the county network. Everything. No differently than a program called Wireshark (www.wireshark.org). If they can listen, they can capture all data traffic and store for later analysis and use.
- If the county intends to change anything on its own network, it must give CIS 30 days prior written notice. That is, in Joe's mind is another huge red flag. Grant County's network is far too large and dynamic to restrict being able to make changes at any given moment for any number of reasons.

- Grant County would never see, nor would they ever be allowed to see or monitor the Albert Sensor dashboard (graphical user interface that most apps have). They would never be given reports on what the Albert Sensor captured. They would also never be given reports of what the Albert Sensor "observed."

- It was also stated that the software that runs the Albert Sensor is Open-Source; the SOS technicians indicated that it made it safer. Regardless of who makes an application, there are inherent flaws, and all things can be hacked. It's only a matter of time before they are compromised.

- Albert Sensors have two network interfaces. An inward facing "listening" interface, and an outward facing interface for remote control by CIS. Placing the Albert Sensor on the network gives unknown outside control of the Albert, which circumvents any existing firewalls. Think of this like a hardware-based Trojan horse. This means that there is a node on our network that we have zero control over, we are contractually obligated to keep in place, that we cannot touch, that could be doing anything it wants, and we would never know about it.

- It was stated that once the Albert Sensor was installed, it would only be "listening," that it was configured to not be able to have bi-directional traffic on the inward facing interface. Joe had major concerns that the interface could be reconfigured remotely to be able to send bi-direction traffic and inject data packets onto our network. There would be no way to know if this was ever happening until it was too late to do anything about it.

Additionally, Jefferson County WSRP EIC member and IT specialist Dave Brader, who has decades of experience working with computers and data systems, verifies and agrees with all of Joe Carter's above statements. Dave says beware of Albert, as the Open-Source software allows packet capture data to be bundled up to CIS. Also, even though Albert may not be in some counties, Albert is a set of applications that can be loaded into an existing computer already in a county Local Area Network (LAN) and does not have to be in a specific hardware box that is installed. Dave also warns that Microsoft and Amazon are heavily invested in Albert / CIS and have access to the data from the counties via cloud storage.

Given the above it would be logical to assume that DHS also has access to all the Albert-provided data.

If appropriate please consider sharing pertinent related info with your County Commissioners, Auditor, and IT Department. If you have Albert, you are probably under contract / memorandum of agreement with the SOS, and it should stipulate an opt-out clause of 90 days' notice to the SOS.

*Bridge Alliance, a left-wing coalition of over 100 member organizations, including George Soro's Open Society. Source: (influencewatch.org)

Thank you!

Bill Bruch
WSRP EIC Chairman
(360) 820-1700