**Albert Sensors & Election Surveillance by CIS**

[July 7, 2022](https://whocountsthevotes.com/2022/07/07/)



**Albert Sensors Don’t Monitor Elections**

The [Albert Network Monitoring Sensor](https://www.cisecurity.org/services/albert-network-monitoring) is provided at no charge to WA Counties by the SOS and managed by [The Center for Internet Security/CIS](https://www.cisecurity.org/services/albert-network-monitoring). CIS is a non-profit with ties to [Democracy Works](https://democracyworks.org.za/), which is a member of the Bridge Alliance. \* CIS has deployed the Albert Sensors in most states including WA. Its function is to monitor county network traffic, looking for malware intrusions and provide alerts to users.

Albert is being promoted as providing security for election systems via the [Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)](https://www.cisecurity.org/ei-isac/). However the sensor is not attached to the election system, but rather the county network. Since we are constantly told that the election systems are not connected to the internet, we know these are not able to monitor elections.

Additionally, the Albert monitoring system, which is entirely internet based, is not even remotely possible as a security system due to its ease of hacking and attack. This violates [WAC 434-335-040 ( 3 c, d)](https://apps.leg.wa.gov/WAC/default.aspx?cite=434-335-040).

If there was an intrusion from within the county’s own network, or even from a frequently used device or address, the system would not detect anything, as it is designed to identify traffic from known malicious sources.

Aside from all of these facts, the SOS and the County Auditors want us to believe that having the Albert sensors monitor the county network should give us peace of mind that our elections are secure.

**Of Note:**

In 2019 Lincoln County, WA (LC) was approached by the WA State SOS / DHS, as were many counties, to sign an agreement to have Albert installed into their county internet network, to make it more “secure.”

It was explained by LC to the SOS that LC’s network was already covered by a security system. But the SOS / 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.

There was a similar situation in Okanogan County. Their network was hacked, and they were not even notified of the attack.

**The Cons**

Albert comes “free and installed” (to the county). Something worth having isn’t usually free. 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](https://www.wireshark.org/)). If they can listen, they (THIS INCLUDES HACKERS) 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. Counties never see, nor would they ever be allowed to see or monitor the Albert Sensor dashboard (graphical user interface that most apps have). They are never given reports on what the Albert Sensor captured. They also are never given reports of what the Albert Sensor “observed.”

Albert Sensor is Open-Source; the SOS technicians say it makes it safer. However, there are inherent flaws, and it can be hacked.

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 Albert, which circumvents any existing firewalls. Think of this like a hardware-based Trojan horse. This means that there is a node on the network that counties have zero control over, are contractually obligated to keep in place, that they cannot touch, that could be doing anything it wants (accessible to hackers) and they would never know about it.

The SOS says 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. The concern is that the interface could be reconfigured remotely to be able to send bi-direction traffic and inject data packets onto county networks. There would be no way to know if this was ever happening until it was too late to do anything about it.

Albert Open-Source software allows packet capture data to be bundled up to CIS. 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 physical box that is installed.

Microsoft and Amazon are heavily invested in Albert / CIS and have access to the data from the counties via cloud storage.

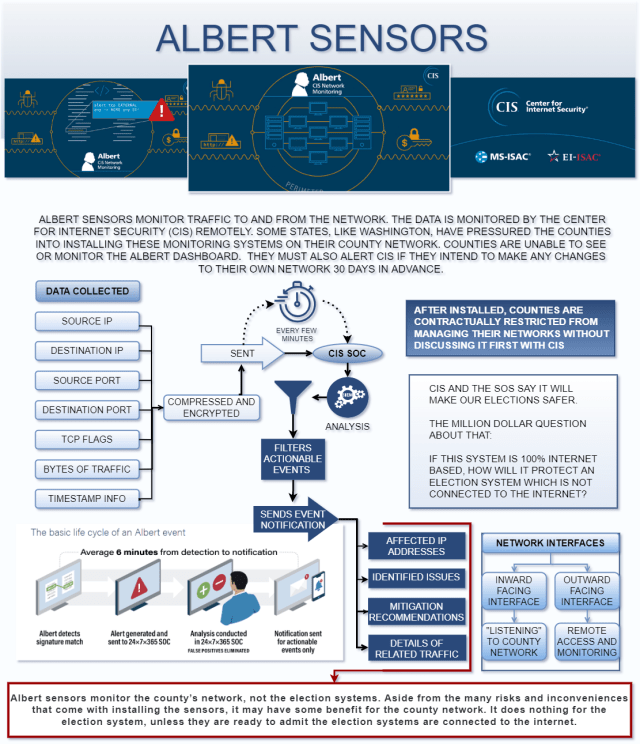
It would be logical to assume that the DHS has access to all the Albert-provided data.

**Promoted by Former WA SOS**

After former Washington SOS resigned right after she won re-election and went to work for the Biden Administration with the CISA, Kim Wyman is still pressuring Washington counties to install and agree to the monitoring by the CIS through Albert sensors. The CIS is not related to the CISA. Why is Wyman still pitching them to the counties?

**Conclusion**

Albert sensors monitor the county’s network, not the election systems. Aside from the many risks and inconveniences that come with installing the sensors, it may have some benefit for the county network. It does nothing for the election system, unless they are ready to admit the election systems are connected to the internet.



To learn about the other ineffective security measures we rely on in Washington State [SEE THIS ARTICLE.](https://whocountsthevotes.com/inadequate-security-measures/)

[Here is another good source of information on Albert Sensors.](https://letsfixstuff.org/2022/12/albert-sensors-front-door-to-sensitive-election-data/)

\*[Bridge Alliance](https://diversityreport-thebridgealliance.nationbuilder.com/2021_diversity_report), a left-wing coalition of over 100 member organizations, including George Soro’s [Open Society. Source:](https://www.opensocietyfoundations.org/) (influencewatch.org)