The NE Secretary of State has granted the federal government essentially full access to county election systems through surveillance devices called “Albert Sensors” provided by a private, non-profit called Center for Internet Security (CIS). CIS is a main player in the censorship scheme carried out by our own federal government, Democrat non-profits, big tech, and state election officials to silence Americans’ concerns about the 2020 election.

In 2018, an agency under the Department of Homeland Security (DHS) called the Cybersecurity and Infrastructure Security Agency (CISA) partnered with CIS to provide “Cybersecurity Services” for state election entities. DHS began to pressure state and local election officials to install Albert Sensors in their networks so they can be monitored 365 days a year by the federal government.

Our SOS jumped on board with the Albert Sensor program almost as soon as it was launched by signing a Memorandum of Agreement with CIS. As part of the agreement, our SOS was required to give CIS a complete network diagram of Nebraska’s election systems, internet access to manage devices, a complete list of IP addresses of county computers, a list of servers, and other information. In return, CIS claimed they would monitor traffic going into and out of Nebraska’s election networks and employ an intrusion detection system to detect security threats. Most, if not all states, have since followed Evnen’s lead and installed Albert Sensors on their election networks.

The MOA requires the entity accepting its services to provide notice to its employees and contractors that they “have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from [the SOS/County] information systems, and any communications or data transiting, stored on or traveling to or from the [the SOS/County] information system may be monitored disclosed or used for any lawful government purpose.”Excerpt from MOA between CIS and NE SOS ceding all expectation of privacy on NE election networks

Counties may not be aware that their networks are being monitored 24/7 by the federal government this is a shocking revelation.

Prior to the 2016 election the DHS drew the dismay of then Secretary of State of Georgia, for attempting to hack into his election system without permission or warning shortly after the 2016 General Election. Such a hack violated 18 USC 1030, which makes attempting to gain access to protected computer systems illegal.

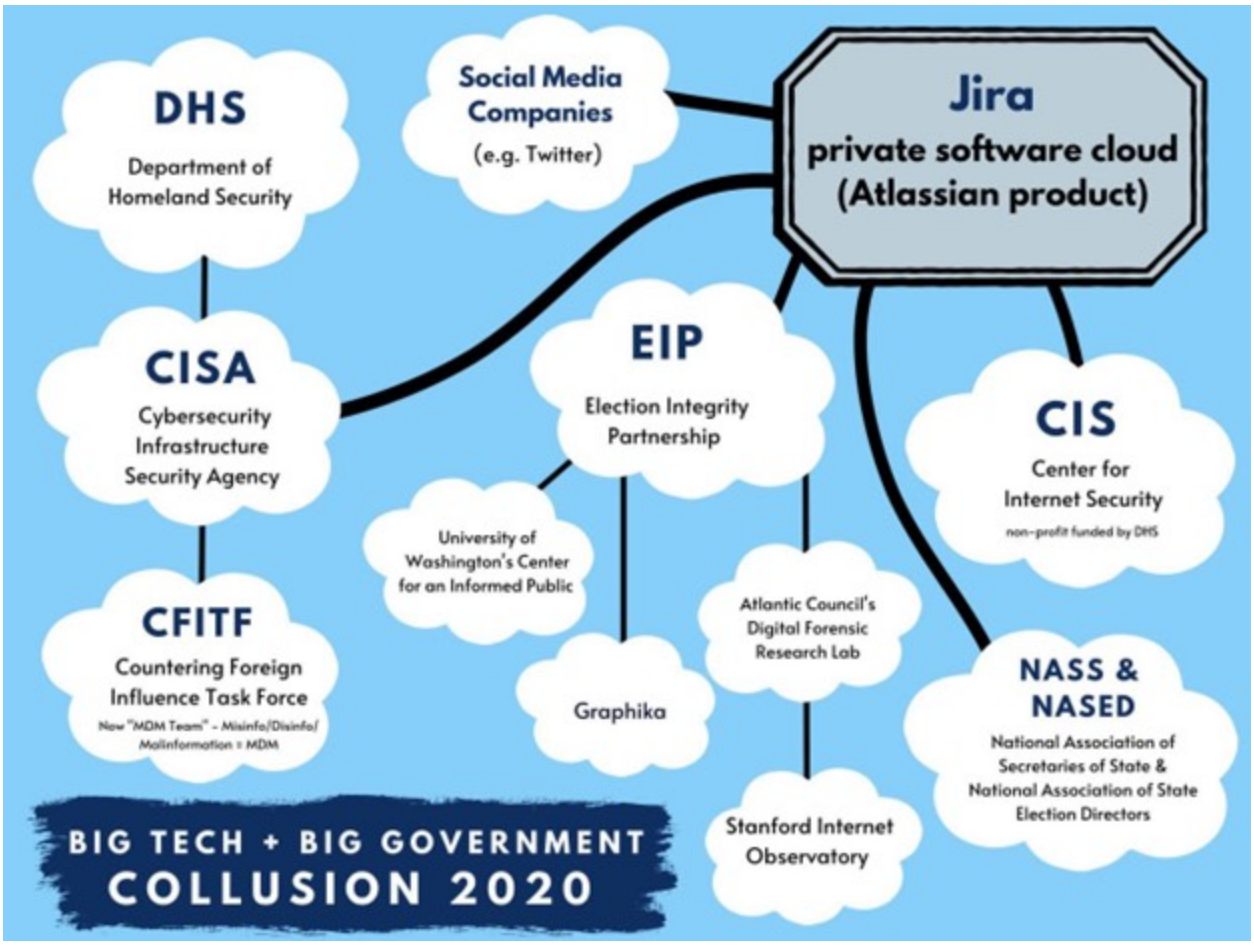
If the DHS would attempt to illegally hack into a state's election system, why should anyone trust them to have their hands in election networks all over the country?

Recent occurrences in Washington state suggest Albert Sensors don't even work as advertised.

Two Counties in Washington were both victims of cyber-attacks after the installation of their Albert Sensors, but CIS failed to detect the hacks or alert the counties. Lincoln County canceled its contract with CIS as a result and inspired nearby Ferry County to cancel theirs as well.

What seemed like a reasonable course of action to the county commissioners in these Counties based on the failure of CIS's service to alert them of a serious intrusion, caused state- sponsored media, NPR, to conduct a national smear campaign against tiny Ferry County with an article and audio report branding the Ferry County Commissioners as misinformation-spreading election deniers.

Further, we are constantly told that our elections are secure and not exposed to the internet. Then why is the federal government, some election officials, and state-sponsored media so worried about a tiny county who decided to ditch their Albert Sensors?



The graphic describes the players in a scheme between government, big tech, Democrat organizations, and election officials to outright violate the first-amendment rights of Americans when it comes to our elections, the COVID response, and information on the Hunter Biden laptop. **All the entities responsible for bringing us Albert Sensors are on this graphic**, and NE Sec of State is a member of NASS.

Until the 2020 election, there has never been widespread questioning of the results of a U.S. election, or widely held concerns over the election systems themselves.

So why were certain sectors of the government, the Democrat party, election officials, and biased social media platforms anticipating the need to crush open discussion of the multitude of anomalies and illegal actions that occurred during the 2020 election? Why were those same entities busy setting up Albert Sensors in as many counties as possible between 2016 and 2020 elections to give the DHS the ability to “see the entire landscape of what’s happening in cyberspace at...local election offices”?

It’s almost as if they knew millions of people were going to question the outcome of 2020, and they had to be prepared to shut it down through name-calling, public shaming, and censorship.

The facts are clear: the DHS, CISA, CIS, NASS, and Our Secretary of State were getting Albert Censors installed in as many counties as they could, while they were simultaneously setting up a far-reaching, powerful censorship network.

Albert Sensors failed to alert counties of real, harmful intrusions all while a big government Faustian bargain was struck. An Orwellian surveillance program was installed in local counties, with most clerks ignorant to its existence. Yet, the SOS signed off on an agreement where local officials have *no reasonable expectation of privacy of their data*.

The conclusions seem obvious: DHS, CISA, NASS, and our Sec. of State actions are concerning. Our elections are exposed to the internet, Albert Sensors can give corrupt pockets of our government real-time data about the outcome of our elections, and time to react if the data doesn’t support the political outcomes they desire. When legitimate investigators and auditors uncover disturbing manipulation of our elections, the censorship regime quickly attempts to silence, smear, and destroy anyone that reveals the truth.