CRITICAL INFRASTRUCTURE SUBSECTOR	Election Systems
SUBJECT	Center for Internet Security
COMPONENT SCOPE	Election Management Systems
RISK LEVEL	High
ELECTION RECORDS IMPACTED	All election records

1 Introduction

The Center for Internet Security (CIS) manages the Election Integrity Information Sharing and Analysis Center (EI-ISAC) under contract to the Department of Homeland Security (DHS) to secure election systems which we are told are not connected to the internet. In this capacity, CIS has privileged access to sensitive election records with negligible public oversight due to its status as a Non-Government Organization (NGO). Significant public trust has been placed in this organization. We believe that the general public should be informed as to the risks associated with this trust.

2 Background

On January 6, 2017, DHS Secretary Jeh Johnson released a notice stating that Election Infrastructure should be designated as a subsector of our Government Facilities critical infrastructure sector. This designation triggered the creation of the EI-ISAC and subsequent EI-ISAC management contract between DHS and CIS.

2.1 EI-ISAC Membership

As of 2022, there were 3,217 official members of the EI-ISAC. Membership spanned all 50 states and 2,532 of 3,143 counties. In addition to government entities, 40 electronic voting system vendors and 5 other NGO's were members.

The NGO's include Democracy Works, the Electronic Registration Information Center (ERIC), National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and Democracy Live Inc.. Municipal organizations participating in the EI-ISAC are required to sign agreements with the Center for Internet Security[1].

2.2 Privileged Access to Election Records

Government entities which sign agreements with CIS for Federally Funded Endpoint Security Services agree to provide CIS with the ability to "inspect network traffic in a decrypted state". This

[1] Sample agreement between CIS and Wayne County, MI can be viewed at https://electioncrimebureau.com/wp-content/uploads/2024/09/Endpoint_Security_Services_MOA_Wayne_County_Michigan-Clerks-Office-6-23-22_Redacted-1.pdf

means that CIS has privileged access to sensitive election records such as voter registration data, pollbook entries, tabulation data and election night results without any public oversight.

> 2. **Endpoint Detection & Response (EDR)**. Deployment and maintenance of an EDR software agent on Entity's identified endpoint devices, which will (a) block malicious activity at a device level if agreed to by the Entity; (b) remotely isolate compromised systems after coordination with the Entity; (c) identify threats on premise, in the cloud, or on remote systems; (d) inspect network traffic in a decrypted state on the endpoint for the limited purpose of identifying malicious activity; and (e) identify and remediate malware infections.

Figure 1 Endpoint Detection & Response (EDR) Services provided by CIS per Wayne County, MI Agreement

In addition to sensitive election information, CIS also has access to all network communications for employees and contractors that use the government entity's election system network.

2.3 Centralized Access to Election Records

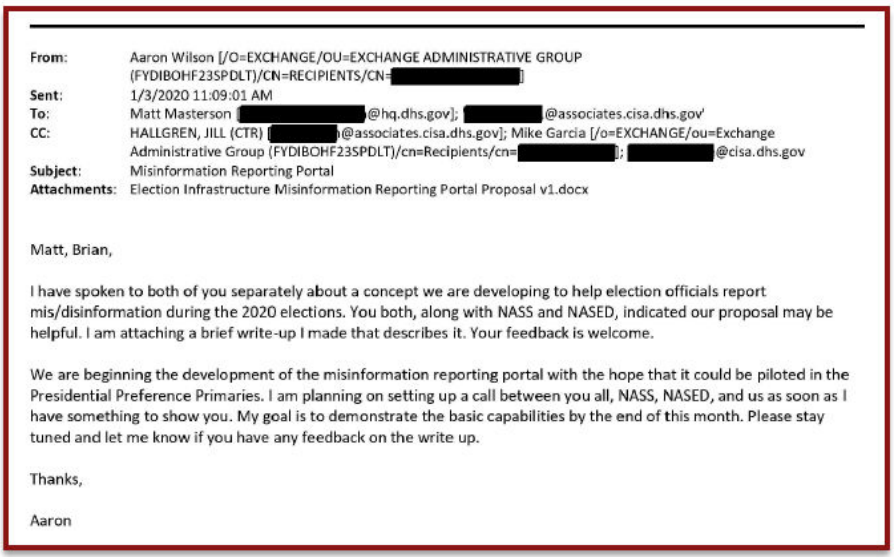
In their agreements, Government entities grant CIS the ability to monitor all of their network traffic via their Security Operations Center (SOC). This means that the information on their election system network is accessible by the SOC.

> 3. Centralized management of ESS data to allow system administration, event analysis and reporting by CIS SOC. Additionally, Entity will be able to interact with its own ESS data through the management system

Figure 2 Centralized Management Services provided by CIS per Wayne County, MI Agreement

2.4 Election Integrity Partnership

The Election Integrity Partnership (EIP) was a collaboration between the federal government and NGO's to manage the flow of information regarding elections in the United States. According to a Congressional Report by the Weaponization of Government subcommittee, the EIP engaged in a campaign "to monitor and censor American's online speech in advance of the 2020 presidential election". Communications between federal employees and CIS employees indicate that CIS played a central role in the conception and implementation of a "misinformation reporting portal".



From: Aaron Wilson [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 1/3/2020 11:09:01 AM
To: Matt Masterson [[redacted]@hq.dhs.gov]; [[redacted]@associates.cisa.dhs.gov'
CC: HALLGREN, JILL (CTR) [[redacted]@associates.cisa.dhs.gov]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]; [redacted]@cisa.dhs.gov
Subject: Misinformation Reporting Portal
Attachments: Election Infrastructure Misinformation Reporting Portal Proposal v1.docx

Matt, Brian,

I have spoken to both of you separately about a concept we are developing to help election officials report mis/disinformation during the 2020 elections. You both, along with NASS and NASED, indicated our proposal may be helpful. I am attaching a brief write-up I made that describes it. Your feedback is welcome.

We are beginning the development of the misinformation reporting portal with the hope that it could be piloted in the Presidential Preference Primaries. I am planning on setting up a call between you all, NASS, NASED, and us as soon as I have something to show you. My goal is to demonstrate the basic capabilities by the end of this month. Please stay tuned and let me know if you have any feedback on the write up.

Thanks,

Aaron

Figure 3Communications Showing CIS Collaboration with DHS to Create a "Misinformation Reporting Portal"(Page 23 of Report By Congressional Subcommittee on the Weaponization of Government)

2.5 Funding Sources

CIS receives the majority of its funding from government grants. Through these grants, they provide their Endpoint Security Services for free to other government entities. In addition to government grants, CIS receives significant funding from the Democracy Fund. A major contributor to the Democracy Fund is Pierre Omidyar.

Contributions, Gifts, Grants and Other Similar Amounts	1a Federated campaigns	1a		
	b Membership dues	1b		
	c Fundraising events	1c		
	d Related organizations	1d		
	e Government grants (contributions)	1e	15,498,146	
	f All other contributions, gifts, grants, and similar amounts not included above	1f	180,165	
	g Noncash contributions included in lines 1a - 1f:$	1g		
	h Total. Add lines 1a-1f	▶		15,678,311
Program Service Revenue		Business Code		
	2a SECURITY BEST PRACTICES	541519	27,406,848	27,406,848
	b PARTNER PAID	541519	6,848,305	6,848,305
	c PRODUCT SALES	541519	974,319	974,319
	d DEMOCRACY FUND	541519	290,555	290,555
	e C. CYBER SECURITY NETWORK (2-1-1)	541519	190,064	190,064
	f All other program service revenue.		10,967	10,967
	g Total. Add lines 2a–2f.	▶	35,721,058	

Figure 4 2020 Form 990 Center for Internet Security (See https://electioncrimebureau.com/wp-content/uploads/2024/09/2020-Form-990-CIS.pdf)

3 Impact

3.1 False Sense of Security

The outsourcing of election security services to CIS is likely to give election officials a false sense of security resulting in lax security practices.

3.2 Indirect Election Subversion

CIS services enable anyone employed or contracted by CIS to intercept and relay sensitive election records. This data intelligence could in turn be transferred to 3rd parties for the purpose of providing them with early notice of voter turnout, individual voter history information, and even vote tallies for specific races. This information could in turn be used by 3rd parties to engage in fraudulent election practices such as the injection of fraudulent ballots in dropboxes.

3.3 Direct Election Subversion

In addition to the risk of the transfer of early election data to 3rd parties, CIS is effectively a trusted Man-in-the-Middle (MITM). The level of access provided to CIS would enable them or anyone with access to their systems to modify the state of key election records without a trace. Furthermore, the centralized ability of the CIS SOC to monitor election system data in all 50 states would simplify the election subversion efforts of any entity such as a nation-state Advanced Persistent Threat (APT) team.

3.4 Censorship

The role of CIS in the conception and implementation of the “misinformation reporting portal” introduces the very likely risk of censorship of American citizens in collusion with the federal

government, social media companies and traditional media companies. Such censorship would violate numerous civil rights guaranteed under the First Amendment of the U.S. Constitution.

3.5 Disinformation

The flipside of the censorship risk is the risk of the deliberate presentation of false narratives regarding our elections as the truth. Once again, the CIS ability to collaborate with the federal government, social media companies and traditional media companies to promote such narratives would be detrimental to election integrity.

4 Risk Mitigation Strategy

If there were no electronic voting systems which connect to the internet, there would be no need for the Center for Internet Security. If state law permits the removal of electronic voting systems, election officials should:

- Remove electronic voting systems
- Define and implement hand count procedures
- Maintain local voter rolls on equipment that is not connected to the internet

If state law mandates the use of electronic voting systems, election officials should:

- Cancel their membership in EI-ISAC
- Uninstall all Albert Sensors and associated CIS software
- Conduct a professional security audit to detect and remove any security vulnerabilities
- Conduct regular security audits to detect vulnerabilities

Hand counts of paper ballots coupled with offline management of voter rolls eliminates a significant number of unnecessary security vulnerabilities that are introduced by the use of electronic voting systems.

5 Conclusion

The Center for Internet Security (CIS) has been contracted by DHS to provide security for election systems which we are told are not connected to the internet. CIS is a Non-Government Organization (NGO) with privileged access to sensitive election records and communications across all 50 states. Since they are an NGO, they are not subject to FOIA requests. This means that CIS executes critical government functions without public oversight. Not only are they not subject to public oversight, they also play a key role in violating our Bill of Rights via the censorship of American citizens by the federal government as revealed by Congressional investigations. There would be no need for CIS involvement in our elections if we did not use electronic voting systems. It appears that government officials have once again created a problem for which they already had a solution that infringes upon our most precious civil liberties including our right to vote.