Zero Trust: How to Secure American Elections When the Losers Won't Accept They Lost

EXECUTIVE SUMMARY

The 2020 U.S. election was unprecedented in American history. Everyone anticipated disruptions as a result of the COVID-19 pandemic dramatically changing voting methods, places, and personnel. While many have detailed what went wrong (or right), reports have largely overlooked the group most impacted by these changes: election officials. Election officials anticipated problems, quietly pivoted with each changing health measure and court case, and faced many of the worst repercussions of viral and inflammatory misinformation.

Trust in American elections is under attack from abroad and at home. Election processes—highly logistical and technical matters—have always been politicized, but politicization is worsening. Domestic actors are achieving the goals of adversaries by both undermining Americans' faith in democracy and increasing threats to election administrators. Election officials are at the frontlines of democracy, but the public's poor understanding of their work has made administering and auditing elections increasingly challenging. The federal government's support framework, while improved, remains ill-equipped to effectively ameliorate the issues election officials face.

In this report, we outline **three exigent threats to election processes** following the events of the 2020 general election. Then, we provide **11 targeted recommendations to best address these threats** in preparation for the 2022 midterm elections and beyond. This report reflects months of interviews with election officials from around the country and across the political spectrum. An oral history and compendium of videos from these interviews is available online. Their stories inform our recommendations to improve the security of our elections and, critically, to shore up voter confidence in their outcome.

Threats to Election Processes

1. **Election officials' capacity to do their jobs is degraded by physical threats and broad distrust fomented by bad-faith actors.** These threats undermine officials' ability to conduct critical community outreach, and could contribute to brain-drain at a time when competence at the local level is needed most.

2. **The playbook for undermining confidence in election results is well-defined and available for foreign and domestic influence agents.** The 2020 election prominently featured attempted election interference from

actors foreign and domestic. Influence agents are emboldened by 2020, while defenders of election integrity are under-resourced and uncoordinated, leaving them vulnerable to repeated tactics.

3. **Inconsistent funding and lack of governance structures around elections IT continue to perpetuate vulnerabilities.** Despite marked progress since 2016, emerging threats such as ransomware continue to expose critical election systems to crippling attacks. In defending election systems, under-resourced local governments face off daily against well-funded nation-state adversaries and cyber criminals, a disparity that continually exposes election systems to attack.

Recommendations

1. **Fund elections consistently at the state, local, and federal level.**
2. **Foster resilience to mis- and disinformation by employing inoculation theory and better coordinating civic integrity stakeholders.**
3. **Prepare state and local election officials to respond to mis- and disinformation in future elections.**
4. **Educate the public about the trusted role of election officials.**
5. **Encourage states to implement paper-based pre-certification audits.**

6 **Reform the Election Assistance Commission (EAC) and designate the Cybersecurity and Infrastructure Security Agency (CISA) as the elections technical lead.**

7 **Provide election offices with more scalable and proactive services through CISA and EI-ISAC.**

8. **Mandate reporting of election cyber incidents to CISA and the FBI.**
9. **Establish a minimum cybersecurity baselines for state and local election offices and election vendors.**
10. **Centralize election IT infrastructure at the state level.**
11. **Support good-faith security research and vulnerability assessments.**