IDENTIV WHITE PAPER

Unlocking U.S. Election Cybersecurity with Security Keys

Hardened security devices coupled with swift, impenetrable multi-factor authentication keeps sensitive data safe and fends off domestic and foreign cybersecurity threats

Cybercrime:
U.S. Elections' Ultimate Opponent

Cybersecurity is high on the business agenda for organizations in every industry, and governments are no exception.

2018 CYBERSECURITY INCIDENTS
were reported by federal agencies

2019[2] U.S. GOVERNMENT ACCOUNTED FOR 5.6%
of all data breaches and 2.1% of exposed data.

In 2018 alone, over 31,000[1] cybersecurity incidents were reported by federal agencies. In 2019[2], the U.S. government accounted for 5.6 percent of all data breaches and 2.1 percent of exposed data.

2020 broke records for all the wrong reasons: While the COVID-19 pandemic dominated the headlines, data breaches in government multiplied and metamorphosed.

Hackers and state actors cemented their unsavory alliances, forging greater tactical cooperation. They upped their game in both the number and sophistication of attacks, harnessing the power of emerging technologies such as artificial intelligence, machine learning, and 5G for their own nefarious purposes.

In **October 2020**, the U.S. government revealed Iranian hackers targeted state election websites to download voter registration information and conduct a voter intimidation campaign. In the same month, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) announced a Russian hacking group breached U.S. state and local government networks.

In **December 2020**, over 200 organizations worldwide and multiple U.S. government agencies revealed breaches by Russian hackers.

Most recently, in **May 2021**, a ransomware attack against the Colonial Pipeline – the largest fuel pipeline in the U.S. – significantly impacted the flow of refined oil across America. How did it happen? Hackers breached Colonial's systems using a single compromised password[3]. This allowed them to enter the company's networks through a virtual private network (VPN) account designed to allow employees to remotely access the corporate systems.

These disturbing events shine the spotlight on the need for a more proactive, preventative, and cohesive approach to tackling advanced cybersecurity attacks from nation-state actors or even domestic threats.

U.S. Government Election Cyber-risks

Government elections are an attractive target for cybercriminals aiming to disrupt and destabilize the foundations of U.S. democracy.

Elections comprise a heterogenous and fluid ecosystem and involve many moving parts and players: the voting public, high-risk/high-profile election candidates, campaign teams, departments and agencies, contractors, election staff and volunteers, businesses, the media, and more.

Cybercriminals seek to exploit any potential weak links introduced by this complexity.

Official election workers, who have access to systems and databases, are popular targets. Threat actors will look for ways to capitalize on this privileged status to exfiltrate sensitive material and information or even lock down campaign operations through coordinated malware and ransomware attacks.

Although poll worker volunteers are unlikely to have access to

1 https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/

2 Centripetal (2021). The Key Challenges for Federal Government Cybersecurity.

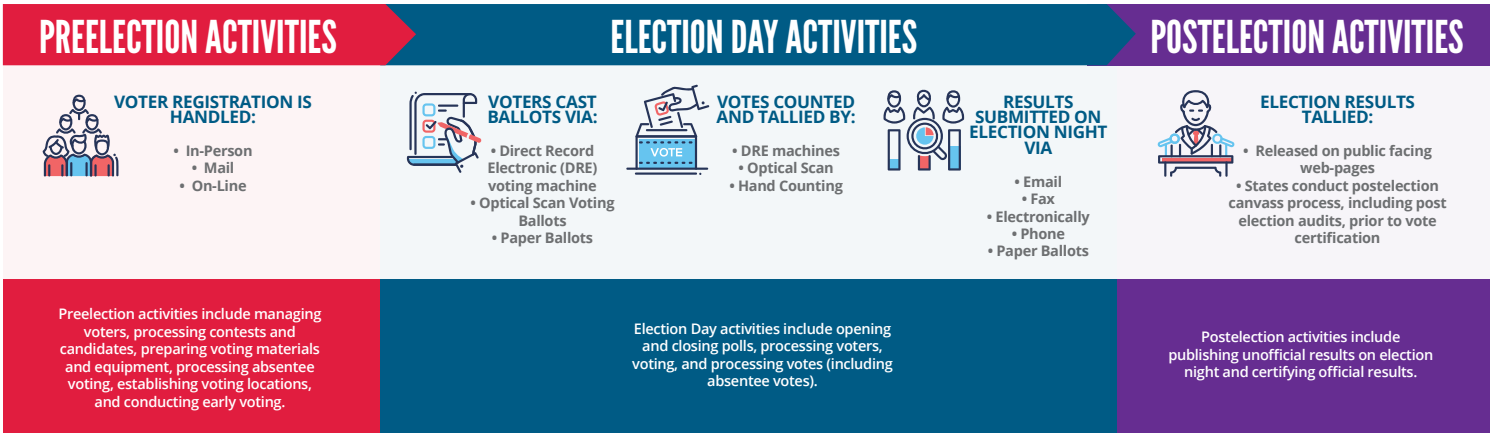
3 Bloomberg (2021). Hackers Breached Colonial Pipeline Using Compromised Password.

core election infrastructure, they typically log onto the networks at polling locations via their laptops or other mobile devices. By successfully targeting a volunteer's personal device, attackers could find a back door in the network, grant themselves privileges, and move laterally throughout the network to launch a ransomware or other attack on polling precincts.

To illustrate the magnitude and scope of the cyber-risk presented by government elections, consider this visual depicting information from the National Institute of Standards and Technology (NIST).

Social media: As the recent Twitter hack[5] taught us, social media is a ripe target for cybercriminals. In the election context, identity-centric attacks designed to gain unauthorized access to or take over social media profiles could spread disinformation regarding polling locations and times. They could even be used to announce fake election results before the polls close, confusing and distressing voters countrywide.

Clearly, the political, legal, reputational, public trust, and financial repercussions of successful election-focused cyber-exploits are incalculable.



Source: DHS CISA[4]

Election-specific Cybercrime Tools and Tactics

Given the myriad of attack vectors cybercriminals can home in on to disrupt free and fair electoral proceedings, it is important to understand precisely how and where the greatest cyber-risk lies, as well as the potential fallout of any successful attempts.

Email compromise: If cybercriminals successfully intercept and exploit confidential emails, they could compromise or undermine the entire or parts of the political ecosystem.

Hacked devices: Threat actors can target computers, laptops, and mobile devices containing sensitive information and delete, modify, unlawfully share or leak it, or render it inaccessible.

Voter registration database manipulation or misuse: Voters' personally identifiable information (PII)/voting history could be compromised or databases corrupted, resulting in voter manipulation or disenfranchisement.

But how exactly do these attacks happen?

A simple oversight like someone clicking on a fake link or inadvertently installing a bad application could result in the download of malware resulting in the disabling of a device or even an entire voting system. Ransomware, which is commonly distributed via email, effectively "locks" a computer or system, rendering its contents inaccessible until the victim pays the attacker a ransom.

Phishing attacks trick users into logging onto a phony website. In an election scenario, a voter administrator could unwittingly share their username and password, giving the attacker all they need to log onto the legitimate website and access data like voter registration information or other sensitive documentation.

On an even more serious note, sophisticated malware, including worms and trojans, could program a system to change votes.

4 Nist.gov (2021) https://www.nist.gov/news-events/news/2021/03/help-protect-our-elections-nist-offers-specific-cybersecurity-guidelines/

5 Justice.gov (2021). Man Arrested in Connection with Alleged Role in Twitter Hack.

Raising the Bar Against Election Cybercrime: Government and Industry Interventions and Protocols

Ensuring elections are protected from any form of cyber-interference means securing the underpinning information and communications technology (ICT) infrastructure and systems managing everything from maintaining voter registration databases to scanning in-person and mail-in ballots and tallying votes.

The current and previous administrations translated the learnings from past election cybercrime experiences into action. Over the last two years, there are encouraging moves away from a previously federated, decentralized, and reactive approach to cybersecurity to a more consolidated, centralized, and proactive stance.

Recent notable interventions and regulations include:

Cybersecurity and Infrastructure Security Agency Act of 2018

In late 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018[6]. This legislation established the Cybersecurity and Infrastructure Security Agency (CISA), which is tasked with building the national capacity to defend against cyberattacks. Its mandate includes working with the federal government to offer cybersecurity tools, incident response services, and assessment capabilities to safeguard government networks.

Biden Executive Order on Improving U.S. Cybersecurity

The recent spate of cyberattacks exposed worrying areas of weakness in critical U.S. infrastructure assets. In response, earlier this year, President Biden signed a new Executive Order (EO)[7] to help bolster the country's cybersecurity. The EO requires all agencies to adopt multi-factor authentication (MFA) and encryption for data at rest and in transit as far as possible. MFA necessitates users to provide two or more verification factors to access a resource like an application, an online account, or a VPN. It is a core component of a strong identity and access management policy.

NIST Cybersecurity Framework Election Infrastructure Profile

In March this year, NIST published a cybersecurity guide (NISTIR 8310)[8] specifically geared towards securing election infrastructure. It provides strategies to help local officials protect their election-related technology from cyberattacks and covers all the technology involved before, during, and after polls are opened.

New cybersecurity industry protocols and standards were also introduced, and others updated or enhanced to respond to the persistent specter of cybercrime. These include:

FIDO2 and FIDO U2F

Consider these statistics[9]:

- **Passwords are the root cause of over 80% of data breaches**
- **The average user has more than 90 online accounts**
- **Up to 51% of passwords are reused**

The FIDO Alliance is dedicated to solving the world's password problem and addressing traditional authentication issues.

FIDO Authentication[10] enables password-only logins to be replaced with secure, fast login experiences across websites and apps. The FIDO protocols use standard public key cryptography techniques to provide stronger authentication and leave zero data at rest.

FIDO2 is the term for the FIDO Alliance's latest set of specifications. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

FIDO U2F is an open standard providing additional security and streamlining Universal 2nd Factor (U2F) authentication.

6 Corridor News (2018). What Is the New US Cybersecurity and Infrastructure Security Agency?

7 Whitehouse.gov (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

8 Csrc.nist.gov (2021). Cybersecurity Framework Election Infrastructure Profile.

9 FIDO Alliance (2021). FIDO Authentication is the Answer to the World's Password Problem.

10 https://fidoalliance.org/how-fido-works/

What Are Security Keys and How Can They Help?

Despite best efforts, we need to be mindful that cybercriminals are always upping their game.

They are well-organized and well-funded.

When the next election cycle rolls around, we can be sure they will be armed with the very latest tools and tactics.

History teaches passwords and SMS-based two-factor authentication (2FA) alone simply are not enough. The good news is advances in security key technologies promise to provide an additional layer of protection for critical election infrastructure, software, and systems.

How Do Security Keys Work?

Security keys blend robust MFA with public-key cryptography:

- **During registration with an online service, the user's client device creates a new key pair**
- **It retains the private key and registers the public key with the online service**
- **Authentication is done by the client device proving possession of the private key to the service by signing a challenge**
- **The client's private keys can be used only after they are unlocked locally on the device by the user**

Who Can Use Security Keys?

Security keys are ideal for anyone involved in election-related activities or duties, such as:

- **Employees or contractors**
- **Citizens accessing government services**
- **Public safety and first responders**
- **Emergency communications personnel**

Why Choose uTrust FIDO2 GOV Security Keys?

While there are many security key vendors in the marketplace, Identiv's uTrust FIDO2 GOV Security Keys (available late 2021) are the smart choice for those administering government elections.

Replace passwords with a secure, rapid, scalable login solution available at an attractive price point.

uTrust FIDO2 GOV Security Keys strengthen any election cybersecurity effort. Here are some of the top security features:

- **Based on public-key cryptography (i.e., the keys stay on the device)**
- **No server-side shared secrets to steal**
- **Multi-protocol FIDO U2F, FIDO2, personal identity verification (PIV) smart card, and one-time password (OTP) support means security keys are resistant to phishing, man-in-the-middle, and replay attacks**
- **No linkability between services or accounts and no third party in the protocol**
- **Lower breach risks, potential damages, and password reset costs**
- **Compatible with modern browsers and operating systems: Windows, Linux, macOS, Android, and iOS**

Beyond these advanced features, security keys are easy to set up and use – even for non-tech-savvy users.

The keys use contactless near-field communication (NFC), supporting short-range communication between compatible devices, including smartphones. NFC requires a fraction of the power consumed by Bluetooth and offers superior connectivity speed. This makes it well-suited for election administrative and field workers.

If you are running or administering an election, you need to make every dollar count. Identiv's security keys eliminate extensive development, provisioning, and maintenance costs. The investment is future-proof: your keys will not become obsolete once the election is over.

Identiv's uTrust FIDO2 GOV Security Keys complement our other election security solutions leveraging government-standard encryption, contact, contactless, and radio frequency identification (RFID) technology.

Read more about the uTrust family of election security solutions.

Cyber Resiliency for All

There is consensus among government entities and stakeholders from the cybersecurity industry and the private sector: we need to detect, disrupt, and respond to interference with election apparatus more effectively.

Bold and brazen or underhand and stealthy, cyberattacks represent a clear and present danger to U.S. constitutional democracy.

Securing the future of U.S. elections calls for a particularly sharp focus on identity and access management.

Make Identiv Your Running-mate

Identiv champions the campaign to digitally secure the physical world. Our uTrust FIDO2 GOV Security Keys are recognized as the responsible choice for those seeking to protect government electoral institutions against the scourge of cybercrime. Our election security solutions can help keep your and your constituents' votes safe and secure.

Visit identiv.com, request a demo, or schedule a site-walk with our team to learn more.