Press Briefing: Election Security & the Midterms

Joseph Lorenzo Hall, Maurice Turner (CDT)

9 Sep 2018

Outline

- Brief background on technical aspects of elections
- Election best practices and cybersecurity controls
- CDT's efforts and materials for election officials
  - Useful for those covering elections too!

Introduction and Motivation

CENTER FOR DEMOCRACY & TECHNOLOGY

- Who are we? What is CDT?
  - CDT is a non-profit advocacy and research org
- Our Background
  - Joseph Lorenzo Hall, Chief Technologist:
    - UC Berkeley: PhD, MIMS (Information Systems), MA (Astrophysics)
    - Worked on election technology issues since 2003
  - Maurice Turner, Senior Technologist:
    - University of Southern California: MPA; Georgetown: Cybersecurity
    - Worked in the intersection of technology and civic life for 30 years.

Background on Election Tech

- Attention on election tech is episodic:
  - 2000-2002 *(Bush v. Gore*, HAVA*),* 2007 (TTBR, EVEREST), 2016 (…)
  - Threats: nation-states, opportunistic hackers, organized crime, insiders
- Election tech is varied, mostly old… highly under-resourced
- Voting machines are important, but narrow part of election systems
  - Voter registration, electronic pollbooks, election-night reporting, election office networks, etc.
- Various different kinds of voting systems (see VVF's Verifier):
  - Hand-count, lever/punch-card, fully electronic (DRE), electronic with a paper trail (DRE+VVPAT), optical scan (large/small), ballot-marking device

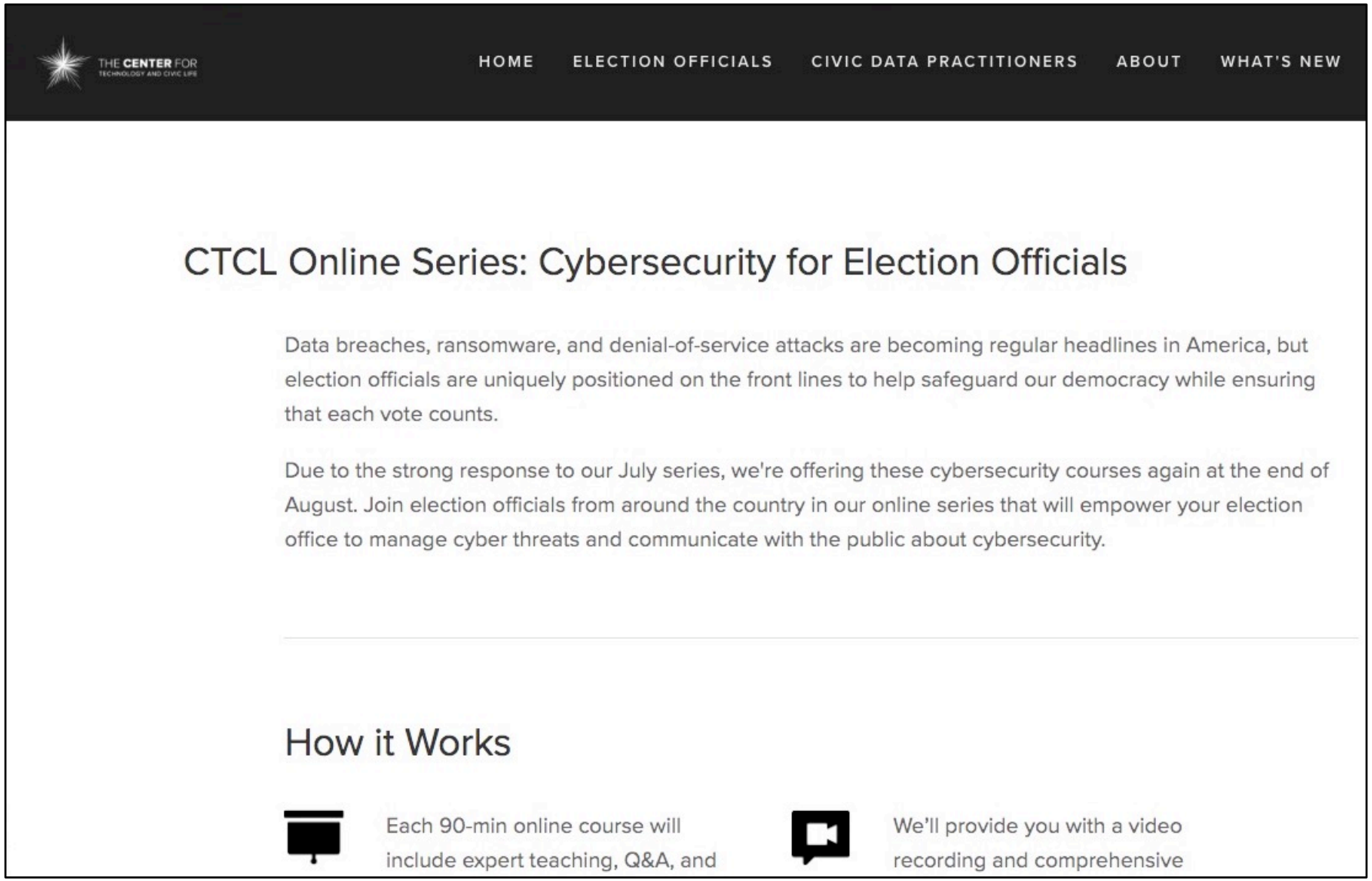
Best Practices and Cybersecurity Controls

- Belfer Center, Harvard:
  - State and Local Election Cybersecurity Playbook (2017)
  - Election Cyber Incident Comms Coordination Guide (Template) (2018)
  - Tabletop Exercise Guide (not yet released)
- Center for Internet Security:
  - A Handbook for Election Infrastructure Security (2017)
- National Academies of Science, Engineering, and Medicine
  - "Securing the Vote: Protecting American Democracy" (2018)

CDT's Efforts

- Election Cybersecurity 101 education
- Producing usable materials for election officials
- Direct outreach to election officials
- Working on issues in the margins
  - Harnessing local cybersecurity talent
  - Election cybersecurity for tribal and territorial governments
- Defensive: blockchain is bad, paper+audits are good (necessary but insufficient)

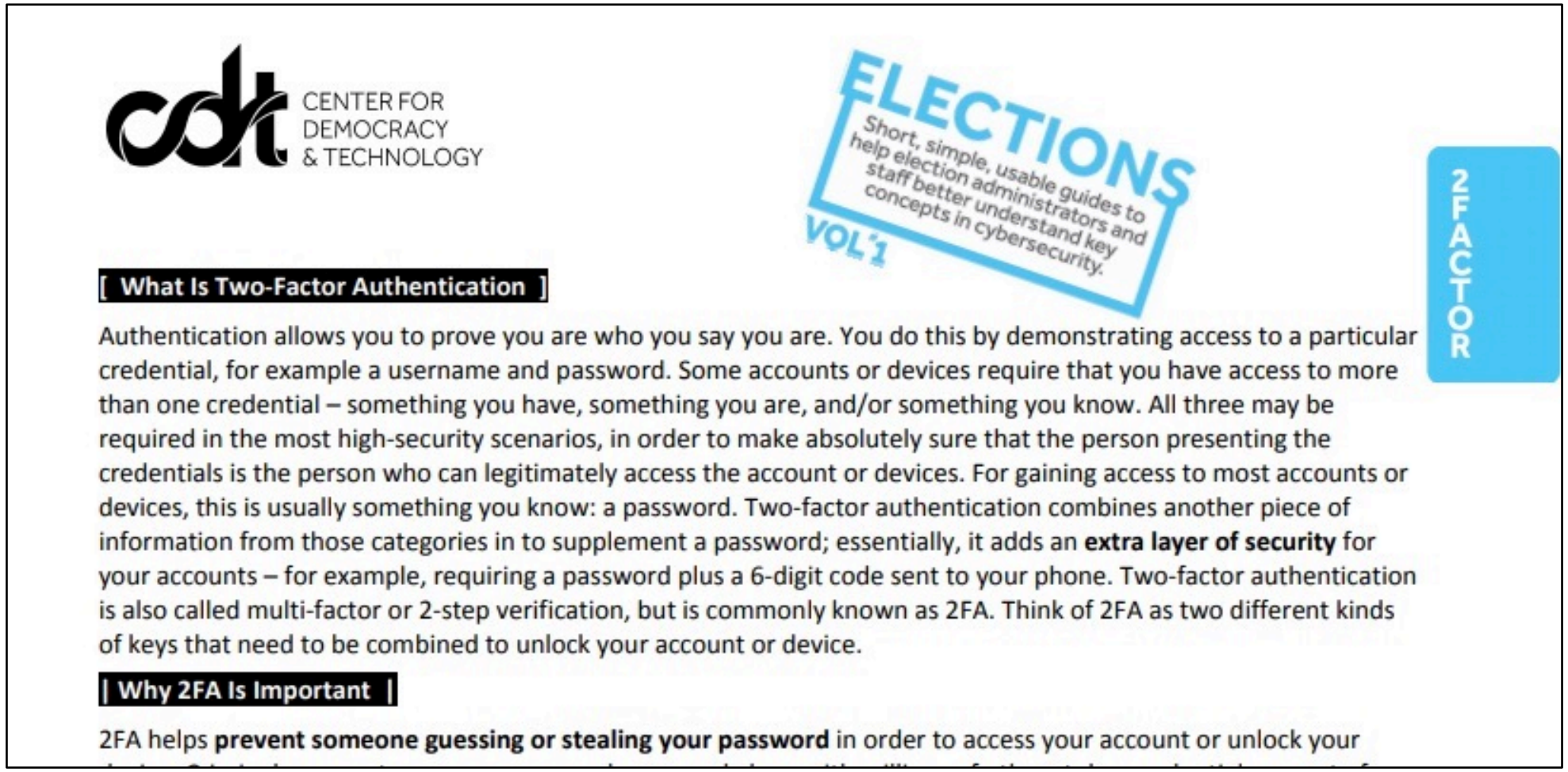
CDT & CTCL Election Cybersecurity 101



CDT's Efforts

- Election Cybersecurity 101 education
- Producing usable materials for election officials
- Direct outreach to election officials
- Working on issues in the margins
  - Harnessing local cybersecurity talent
  - Election cybersecurity for tribal and territorial governments
- Defensive: blockchain is bad, paper+audits are good (necessary but insufficient)

CDT election cybersecurity field guides (1)



CENTER FOR DEMOCRACY & TECHNOLOGY

ELECTIONS
Short, simple, usable guides to help election administrators and staff better understand key concepts in cybersecurity.
VOL 1

2FACTOR

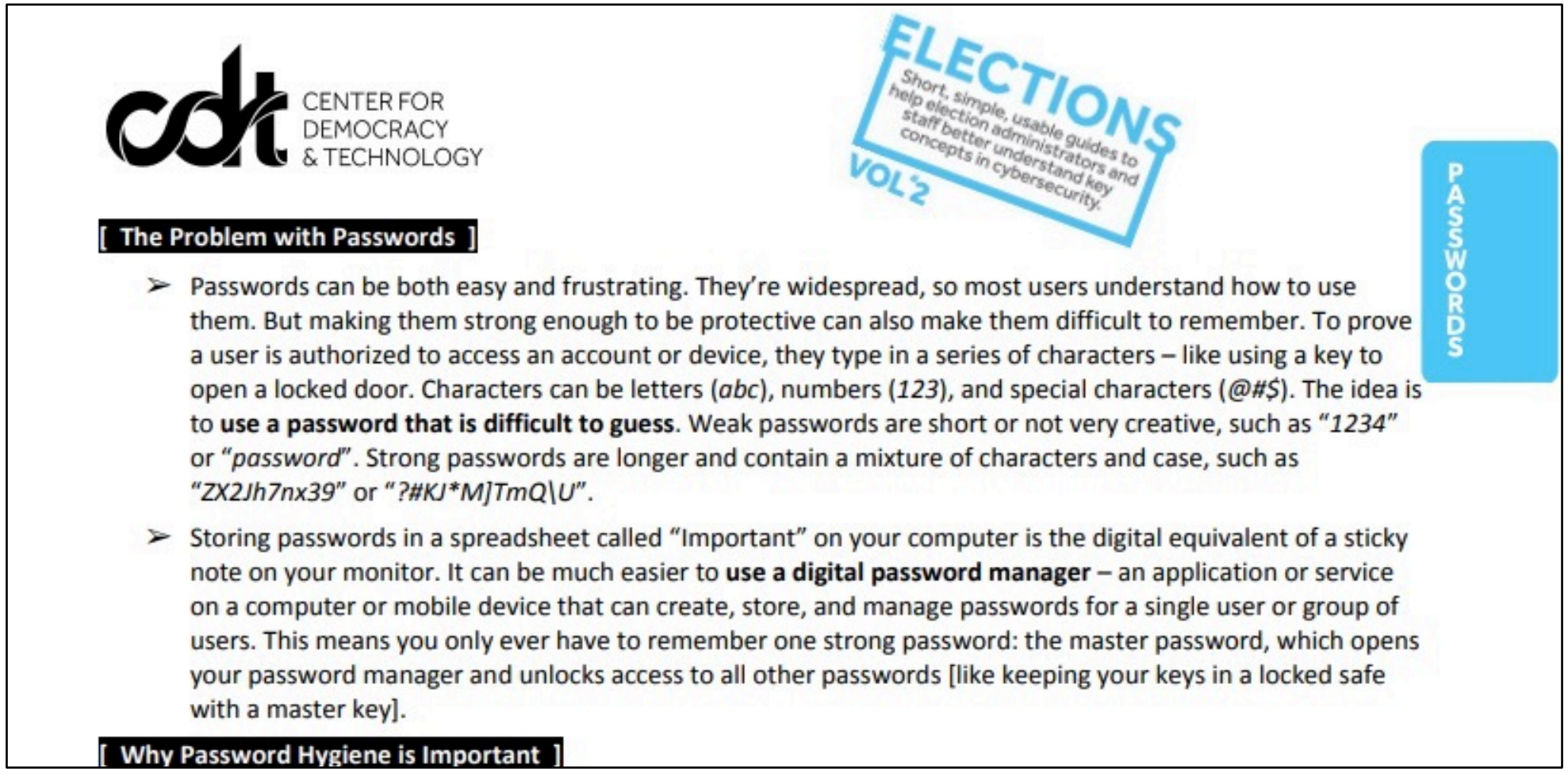
[What Is Two-Factor Authentication]

Authentication allows you to prove you are who you say you are. You do this by demonstrating access to a particular credential, for example a username and password. Some accounts or devices require that you have access to more than one credential – something you have, something you are, and/or something you know. All three may be required in the most high-security scenarios, in order to make absolutely sure that the person presenting the credentials is the person who can legitimately access the account or devices. For gaining access to most accounts or devices, this is usually something you know: a password. Two-factor authentication combines another piece of information from those categories in to supplement a password; essentially, it adds an **extra layer of security** for your accounts – for example, requiring a password plus a 6-digit code sent to your phone. Two-factor authentication is also called multi-factor or 2-step verification, but is commonly known as 2FA. Think of 2FA as two different kinds of keys that need to be combined to unlock your account or device.

| Why 2FA Is Important |

2FA helps **prevent someone guessing or stealing your password** in order to access your account or unlock your

CDT election cybersecurity field guides (2)



CENTER FOR DEMOCRACY & TECHNOLOGY

ELECTIONS
Short, simple, usable guides to help election administrators and staff better understand key concepts in cybersecurity.
VOL 2

PASSWORDS

[The Problem with Passwords]

- Passwords can be both easy and frustrating. They're widespread, so most users understand how to use them. But making them strong enough to be protective can also make them difficult to remember. To prove a user is authorized to access an account or device, they type in a series of characters – like using a key to open a locked door. Characters can be letters (*abc*), numbers (*123*), and special characters (*@#$*). The idea is to **use a password that is difficult to guess**. Weak passwords are short or not very creative, such as "*1234*" or "*password*". Strong passwords are longer and contain a mixture of characters and case, such as "*ZX2Jh7nx39*" or "*?#KJ*M]TmQ\U*".
- Storing passwords in a spreadsheet called "Important" on your computer is the digital equivalent of a sticky note on your monitor. It can be much easier to **use a digital password manager** – an application or service on a computer or mobile device that can create, store, and manage passwords for a single user or group of users. This means you only ever have to remember one strong password: the master password, which opens your password manager and unlocks access to all other passwords [like keeping your keys in a locked safe with a master key].

[Why Password Hygiene is Important]

CDT's Efforts

- Election Cybersecurity 101 education
- Producing usable materials for election officials
- Direct outreach to election officials
- Working on issues in the margins
  - Harnessing local cybersecurity talent
  - Election cybersecurity for tribal and territorial governments
- Defensive: blockchain is bad, paper+audits are good (necessary but insufficient)

Direct outreach to election officials

CDT's Efforts

- Election Cybersecurity 101 education
- Producing usable materials for election officials
- Direct outreach to election officials
- Working on issues in the margins
  - Harnessing local cybersecurity talent
  - Election cybersecurity for tribal and territorial governments
- Defensive: blockchain is bad, paper+audits are good (necessary but insufficient)

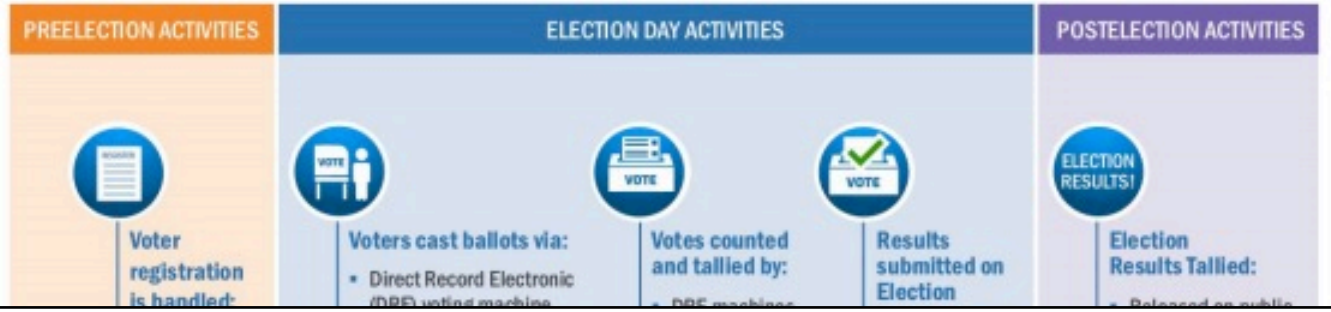
Spotlight on local cybersecurity talent

CENTER FOR DEMOCRACY & TECHNOLOGY

Infosec Toolkit for Election Volunteering

From federal data breaches to foreign governments phishing political campaigns to malware shutting down city services, our nation is under attack. You can help – starting right in your own community. Local and state officials are working to build a more resilient electoral process, but their capacity is limited. They need civic-minded infosec professionals to combine their knowledge and talents as technical volunteers for Election Day and beyond. The information below will help you understand the election process and provide tips on how you can get involved.

Election Process Overview



CDT's Efforts

- Election Cybersecurity 101 education
- Producing usable materials for election officials
- Direct outreach to election officials
- Working on issues in the margins
  - Harnessing local cybersecurity talent
  - Election cybersecurity for tribal and territorial governments
- Defensive: blockchain is bad, paper+audits are good (necessary but insufficient)

Thank you

- CDT: https://cdt.org
- CDT elections work: https://cdt.org/campaign/election-security/
- Joseph Lorenzo Hall (@JoeBeOne):
  - Chief Technologist
  - joe@cdt.org
- Maurice Turner (@TypeMRT):
  - Senior Technologist
  - maurice@cdt.org