Homeland Security

Fact Sheet: Designation of Election Infrastructure as Critical Infrastructure

Consistent with Presidential Policy Directive (PPD) 21, the Secretary of Homeland Security has established Election Infrastructure as a critical infrastructure subsector within the Government Facilities Sector.

Election infrastructure includes a diverse set of assets, systems, and networks critical to the administration of the election process. When we use the term "election infrastrucure," we mean the key parts of the assets, systems, and networks most critical to the security and resilience of the election process, both physical locations and information and communication technology. Specficially, we mean at least the information, capabilities, physical assets, and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

Components of election infrastructure include, but are not limited to:

- Physical locations:
  - Storage facilities, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day.
  - Polling places (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day.
  - Centralized vote tabulation locations, which are used by some states and localities to process absentee and Election Day voting materials.
- Information and communication technology (ICT):
  - Information technology infrastructure and systems used to maintain voter registration databases.
  - Voting systems and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day.
  - Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night on behalf of state governments, as well as for postelection reporting used to certify and validate results.

Protecting and defending this infrastructure is the responsibility of state and local governments and election officials. DHS assists state, local, tribal, and territorial (SLTT) governments, on a voluntary basis, with the management of their cyber risk. This includes tools, services, and capabilities that can help election officials protect and defend this infrastructure.

January 2017