Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

July 6, 2018

The Designation of Election Systems as Critical Infrastructure

Prior to the 2016 federal election, a series of cyberattacks occurred on information systems of state and local election jurisdictions. Subsequently, in January 2017 the Department of Homeland Security (DHS) designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. The designation sparked some initial concerns by state and local election officials about federal encroachment of their prerogatives, but progress has been made in overcoming those concerns and providing assistance to election jurisdictions.

What Led to the Designation?

In August 2016, the Federal Bureau of Investigation (FBI) announced that some state election jurisdictions had been the victims of cyberattacks aimed at exfiltrating data from information systems in those jurisdictions. The attacks appeared to be of Russian-government origin. That same month, DHS contacted state election officials to offer cybersecurity assistance for their election infrastructure. Most states accepted the offer. Although the cyberattacks did not appear to affect the integrity of the election infrastructure, some observers began calling for it to be designated as critical infrastructure (CI). On January 6, 2017, the Secretary of Homeland Security announced that designation.

What Is Critical Infrastructure?

Under federal law, CI refers to systems and assets for which "incapacity or destruction … would have a debilitating impact on security, national economic security, national public health or safety, or any combination" of them (42 U.S.C. §5195c(e)). Most CI entities are not government-owned or -operated. Presidential Policy Directive 21(PPD 21) identified 16 CI sectors, with some including subsectors. Sectors vary in scope and in degree of regulation. For example, the financial services sector is highly regulated, whereas the information technology sector is not. Election infrastructure has been designated as a subsector (EIS) of government facilities. That sector includes two previously established subsectors: education facilities, and national monuments and icons.

The Homeland Security Act of 2002 (P.L. 107-296) gave DHS responsibility for several functions aimed at promoting the security and resilience of CI with respect to both physical and cyber-based hazards, either human or natural in origin. Among those functions are providing assessments, guidance, and coordination of federal efforts.

Each CI sector has been assigned one or two federal sector-specific agencies (SSAs), which are responsible for coordinating public/private collaborative efforts to protect the sector, including incident management and technical assistance. DHS has regulatory authority over two sectors: chemical and transportation systems. It serves as SSA for several, including the EIS.

The components of the EIS as described by DHS include physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns.

Does the Designation Permit Federal Regulation of Election Infrastructure?

DHS does not have regulatory authority over EIS. Five other agencies have significant roles with respect to federal elections, but none has claimed regulatory authority over the EIS:

- The Election Assistance Commission (EAC), created by the Help America Vote Act (HAVA, P.L. 107-252), provides a broad range of assistance to states, including development of voluntary technical standards for voting systems, voluntary guidance on implementing HAVA requirements, and research on issues in election administration. It also has statutory authority for administering formula payments to states to assist them in meeting HAVA requirements and improving election administration, including $380 million appropriated in FY2018 in response to security concerns.

- The National Institute of Standards and Technology (NIST) assists the EAC on technical matters, including development of the voting system standards, certification of voting systems, and research.

- The Department of Justice (DOJ) has some enforcement responsibilities with respect to requirements in HAVA and other relevant statutes.

- The Department of Defense (DOD) assists military and overseas voters.

- The Federal Election Commission (FEC) is responsible for enforcement of campaign finance law but is not involved in election administration by state and local jurisdictions.

HAVA expressly prohibits the EAC from issuing regulations of relevance to the CI designation, and it leaves the methods of implementation of the act's requirements to the states. However, it does permit DOJ to bring civil actions if necessary to implement HAVA's requirements.

What Does the Designation Mean?

While both DHS and the EAC provided assistance to states in addressing the security concerns that arose in the run-up to the November 2016 election, the CI designation had several notable consequences:

- It raised the priority for DHS to provide security assistance to election jurisdictions that request it and for other executive branch actions, such as economic sanctions under Executive Order 13964 that the Department of the Treasury can impose against foreign actors who attack elements of U.S. CI (the order has also been revised to expressly cover tampering with elections).

- It brings the subsector under a 2015 United Nations agreement (A/70/174) stating that nations should not conduct or support cyber-activity that intentionally damages or impairs the operation of CI in providing services to the public. It also states that nations should take steps to protect their own CI from cyberattacks and to assist other nations in protecting their CI and responding to cyberattacks on it. Twenty nations, including Russia and the United States, have signed the agreement.

- It provides DHS the authority to establish formal coordination mechanisms for CI sectors and subsectors and to use existing entities to support the security of the subsector. Those mechanisms are used to enhance information sharing within the subsector and to facilitate collaboration within and across subsectors and sectors. For example, both the FBI and the Office of the Director of National Intelligence (ODNI) have participated in briefing election officials on threats to the EIS.

Among the coordination mechanisms for the new subsector are the following:

- *Government Coordinating Council.* The GCC consists of representatives of DHS, the EAC, 15 state election offices, 8 local ones, and a state association of local officials. It facilitates coordination across government entities both within EIS and in other sectors. Activities include communications, planning, issue resolution, and implementation of the security missions of the entities.

- *Sector Coordinating Council.* The SCC consists of representatives of 16 private-sector entities, most of which are providers of voting systems and other election-related products and services. SCCs are self-organized and self-governed. They are intended to represent private-sector interests and to facilitate collaboration activities, including information sharing, among the private-sector entities in the CI sector and with government entities.

- *Sector-Specific Plan.* Public- and private-sector partners have created SSPs for each of the 16 CI sectors. There is also a plan for the State, Local, Tribal, and Territorial Government Coordinating Council. The plans are components of an overall National Infrastructure Protection Plan and provide a means for the sectors to establish goals and priorities for addressing risks. They are generally updated on a four-year cycle. The most recent versions were released in 2015 and therefore do not yet include the EIS.

The CI designation for election infrastructure is also intended to facilitate use of existing resources, such as

- *National Cybersecurity and Communications Integration Center.* The NCCIC is the primary federal focus for sharing CI cybersecurity.

- *Critical Infrastructure Partnership Advisory Council.* CIPAC provides election officials access to a broad range of relevant expertise and participation in sensitive planning conversations.

- *Multi-State Information Sharing and Analysis Center.* The MS-ISAC is one of the centers created to facilitate the sharing of security information for different CI sectors. It works with the NCCIC, all states, and many local governments to assist them in cybersecurity. The MS-ISAC supports the EIS-ISAC, created in 2018 to facilitate information-sharing activities for and among more than 500 members consisting of state and local election offices, as well as the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED).

For more information, see https://www.dhs.gov/topic/election-security, https://www.eac.gov/election-officials/elections-critical-infrastructure/, https://www.cisecurity.org/ei-isac/.

Why Was the Designation Initially Controversial?

Misgivings about DHS involvement were raised when it first offered assistance to election jurisdictions in August 2016. Some observers feared that DHS would begin to exert control over the administration of elections or to engage in unrequested security activities. A NASS press release on the EIS designation questioned the need for it.

Controversy over the federal role in election administration is not new. Concerns about federal regulation of the election process were prominent during the legislative debate over HAVA and led to the inclusion of the regulatory restrictions in the law. Furthermore, bills in prior Congresses that would have provided DHS broad regulatory authority over cybersecurity have all failed.

The CI designation does not contravene the HAVA restrictions on EAC regulations or create DHS regulatory authority for EIS. DHS provides assistance to election jurisdictions only on a voluntary basis. Among the more than 50 bills with election-security provisions introduced in the 115th Congress, a few would establish mandatory standards or federal rule-making authority, but none have received committee or floor action.

Eric A. Fischer, efischer@crs.loc.gov, 7-7071

IF10677