Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

March 5, 2020

The Election Infrastructure Subsector: Development and Challenges

In January 2017, in accordance with Presidential Policy Directive 21 (PPD-21), the Department of Homeland Security (DHS) designated the systems and assets used in elections as the Election Infrastructure Subsector (EIS) of the Government Facilities critical infrastructure sector. DHS defines critical infrastructure as "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."

The critical infrastructure designation was intended to help address some of the obstacles election stakeholders faced in responding to foreign interference in the 2016 elections, such as a lack of timely information sharing about threats to election systems. It gave DHS a new role in election security, authorizing it to help coordinate among and prioritize assistance to election security stakeholders.

This In Focus provides an overview of the EIS. It describes the formation and development of the subsector and some of the ongoing challenges it faces.

Background

DHS established the EIS under an existing policy framework for critical infrastructure security that was first outlined during the Clinton Administration. Current critical infrastructure security guidance derives from the most recent iteration of that framework, PPD-21, published in 2013. PPD-21 designated 16 critical infrastructure sectors, directing DHS to coordinate security collaboration among public and private stakeholders and prioritize provision of its support services to those stakeholders.

Primary coordination mechanisms for each sector include Government Coordinating Councils (GCCs), which consist of relevant federal agencies and other public sector stakeholders, and Sector Coordinating Councils (SCCs), which consist primarily of private sector stakeholders. These coordinating councils may also support independently organized Information Sharing and Analysis Centers (ISACs) to help identify and address threats to infrastructure in the sector they represent.

According to DHS, election infrastructure includes both elections-related information and communications technology, such as voter registration databases and voting machines, and physical infrastructure, such as polling places and elections storage facilities. DHS's Cybersecurity and Infrastructure Security Agency (CISA) serves as the lead federal agency for the EIS.

DHS and its federal, state, and local partners chartered the EIS GCC in October 2017, and private sector partners chartered the EIS SCC in February 2018. The EIS GCC created the Elections Infrastructure (EI) ISAC in 2018 to provide state, local, tribal, and territorial (SLTT) officials with services such as 24-hour threat monitoring, readiness exercises, and assistance with incident response. The same year, the EIS SCC and the industry-focused Information Technology (IT) ISAC established an Elections Industry Special Interest Group (EI-SIG). The EI-SIG focuses on the needs of elections industry companies, providing them with a platform to engage with other members of the IT sector and exchange information on common threats.

Sector Progress

The federal critical infrastructure security framework relies on voluntary participation and community-wide contributions to increase risk awareness and security. Observers have offered mixed assessments of the overall effectiveness of the voluntary collaboration framework, but they have generally found that critical infrastructure sectors become more effective as they increase active membership, pool resources, and find ways to more efficiently generate and share security-related information.

When DHS first designated election systems as critical infrastructure, it lacked experience with election administration practices or well-developed relationships with the SLTT officials who administer elections. Furthermore, officials from the National Association of Secretaries of State and the Election Assistance Commission—the federal agency with the most experience working with SLTT election officials—objected to the critical infrastructure designation as agency overreach.

However, observers have indicated that relations between DHS and federal, state, and local partners have since improved and that the EIS has made progress in the areas of active membership growth, resource pooling, and information sharing listed above. For example, as of February 2020, the EI-ISAC has nearly 2,500 members, including many SLTT election authorities. As such, the EI-ISAC was the fastest growing of the existing ISACs, according to DHS.

By design, the value of the services the EI-ISAC provides increases with the network of stakeholders that use them. For example, the EI-ISAC uses analysis of network traffic on SLTT government systems to help develop cyber threat signatures, so its ability to identify malicious network activity increases as more SLTT authorities share network data. Since 2018, the EI-ISAC has expanded deployment of intrusion detection sensors—known as Albert sensors—to elections-related systems in all 50 states. Some states have also deployed the sensors on local or vendor networks.

DHS officials report that states have also used the EI-ISAC, along with other EIS coordination mechanisms, to share information about common threats. For example, in one case described by a CISA official, state officials provided DHS with information about possible malicious activity targeting their election systems. DHS then distributed the information to relevant stakeholders and issued a national alert. Some state officials report a general increase in information sharing and collaboration at all levels of government following the creation of the EIS, which they believe has contributed to improvements in threat reporting and awareness nationwide.

Continuing Challenges

The Government Accountability Office (GAO) raised concerns about DHS's election security planning in a February 2020 report. CISA has since taken steps to address some of those concerns, including releasing a strategic plan, but GAO's focus on the importance of planning highlights the scope of some of the challenges facing the EIS.

One of those challenges is participation. Participation in the EIS has increased rapidly in general, but CISA and state officials have reported difficulty getting some local officials to engage with the subsector. Some states, localities, and vendors have also been reluctant to share information about threats and vulnerabilities in their systems, which is a common challenge across critical infrastructure sectors.

Some participation issues may be due in part to a mismatch between certain resources available through the EIS and the needs and capabilities of subsector stakeholders. The February 2020 GAO report recounted problems with the tailoring of certain CISA offerings, and some states have purchased third-party security services rather than using similar no-cost options from CISA. Some SLTT election officials have reported that the volume of information they receive as part of the EIS can be overwhelming and that security notifications are not always actionable. The scope of some of the resources provided is also limited. For example, Albert sensors provide security alerts about potential intrusions into a network but are not designed to block threats or detect malicious traffic within the network.

Some states have taken action to address these gaps—for example, by setting up systems to process EIS information for local officials—but that option might not always be viable for states with more limited resources. SLTT resource limitations represent a continuing challenge for the EIS. States and localities might lack the resources needed to act on information they receive through the EIS or implement recommendations from CISA. Election security fixes can be costly and may include ongoing costs like salaries or license renewal fees, which states and localities might not be able to fund without federal aid.

Issues for Congress

CISA has released plans to address some of these challenges, as described above, and the EIS has mechanisms for addressing others. For example, the EIS GCC has established protocols for improving communication among EIS stakeholders. Congress might opt not to intervene in the subsector's processes, allowing EIS stakeholders to address challenges within the existing policy framework.

However, Congress might also choose to be more involved. Congress has held hearings on election security preparations and directed GAO to examine DHS's elections work, and it might choose to conduct further oversight of the EIS. Some Members have also proposed legislation—including in the areas described below—to address subsector challenges.

- **Funding for States:** Congress appropriated $380 million for FY2018 and $425 million for FY2020 for payments to states to improve election administration, including election security. SLTT officials have requested further funding—and, in particular, ongoing funding—for election security. Congress might consider whether to provide either one-time or ongoing payments to states and, if so, whether to set conditions or limits on their use. Congress might also consider whether to provide for additional evaluation of states' use of existing funding.

- **Funding for DHS:** Congress might consider how much to appropriate to CISA for its election infrastructure security work and whether to specify funding levels for particular activities. For example, some Members expressed concern that CISA's budget request for FY2020 would not maintain EI-ISAC services at existing levels. Congress subsequently provided CISA with more FY2020 funding for its election security initiative than the agency requested, and CISA's director confirmed in a February 2020 hearing that the EI-ISAC would be fully funded.

- **Requirements:** Critical infrastructure sectors and federal action on election administration both generally rely on voluntary participation by stakeholders. However, some have suggested that there are advantages to universal adoption of certain election security measures, such as cyber incident reporting or risk-limiting audits. Congress might consider how to weigh the potential benefits of requiring adoption of such measures against other considerations, such as the roles and responsibilities of SLTT officials.

- **Codification:** Creation of the EIS was an agency action, which could be rescinded or otherwise challenged at the agency level. Some bills introduced in the 116th Congress would make the EIS permanent by codifying it in federal law (see, for example, H.R. 1 and H.R. 1612). Congress might consider whether to adopt such a proposal and whether to codify any of the specific activities that federal agencies carry out—or might carry out—as part of the EIS.

Brian E. Humphreys, Analyst in Science and Technology Policy

Karen L. Shanton, Analyst in American National Government

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.