We Make Scientific
Breakthroughs Possible

Establish a Cybersecurity Maturity Model Standard for Election Security

Background

The cybersecurity of the Nation's electoral system has come under intense scrutiny since the 2016 election cycle. Elections are the responsibility of each state and local authority. The cybersecurity of the systems involved in elections varies greatly due to funding, population density, state and local laws and regulations, and other disparate factors. In addition, the cyclical nature of elections makes instituting good cybersecurity practices difficult. For example, election infrastructure is often used only a few times per year and is temporarily deployed to large numbers of polling stations. In addition, volunteer workers may not have much knowledge about cybersecurity concerns and are not always provided with adequate training. These issues create complex challenges for election officials.

We propose that a cybersecurity risk model be developed and deployed that takes into account the special characteristics of our election system. The U.S. Department of Defense (DOD) is in the process of formulating a new cybersecurity risk framework. The Cybersecurity Maturity Model Certification (CMMC) will serve to shore up the cybersecurity of the Nation's defense supply chain. The DOD created an independent, third-party, non-profit organization to spearhead the development of the new standard. As the CMMC has developed, the utility of such a broad-reaching maturity-based model has become clear to not only defense contractors, but also to other federal contractors. As the security of the Nation's election sector continues to face great scrutiny and pressure, we propose to create a similar effort focused on the election sector.

Contact Us

2650 Park Tower Drive
Vienna, VA 22180

(202) 462-1676

info@aui.edu

www.adi.edu

View Document Online

Proposal

Our proposal is to establish an institute run by an independent, non-profit to formulate a cybersecurity maturity model well-suited to protect the cybersecurity of the Nation's election infrastructure. The institute would be tasked with working with state, local, and industry stakeholders to design a commonly accepted framework that provides an auditable level of security to these critical systems. Although the current CMMC DOD initiative targets organizations that handle federal contract information (FCI) or controlled unclassified information (CUI), this methodology can be leveraged for the elections environment.

Election data requires special care as its corruption or manipulation could pose a risk to national security and because it contains highly sensitive personal identifiable information (PII).

States and localities each administer elections in different ways, so a new CMMC-type standard

must be developed to encompass the diversity of data types and processes inherent in this sector. The purpose of using a maturity model approach would be to ensure that a model is developed to secure the most sensitive voting-related data at a level sufficient to protect against advanced persistent threats (APTs) while also ensuring that small local authorities have an achievable baseline of security. We propose that the organization tasked with creating this standard be closely aligned with the Cybersecurity Infrastructure and Security Agency (CISA) and be informed by the Nation's Intelligence Community. The organization promulgating these rules would also establish a procedure to enable low-cost audits of election infrastructure to ensure the Nation's electoral system is operating with appropriate levels of security. The organization would be responsible for formulating the framework, training auditors to perform the on-the-ground assessments, and serve a strong quality assurance role. It would also serve as a central reporting organization to the federal government regarding the state of the Nation's electoral system.

Proposed Funding

The institute selected to develop the standard should be funded at approximately $7M per year, operating for a minimum initial period of 5 years. After such time, the program and institute could be evaluated for further funding and support.