media@cisecurity.org

Center for Internet Security (CIS) Releases New Elections Technology Cybersecurity Supply Chain Guide

The guide identifies the most common attack types on supply chains and provides an analysis of each election infrastructure component, the supply chain threats impacting them, and mitigation approaches; the CIS guide was compiled with input from the broader election community to include election technology providers and the Cybersecurity & Infrastructure Security Agency (CISA).

EAST GREENBUSH, N.Y., Feb. 10, 2021 – The Center for Internet Security, Inc. (CIS®) released Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers today in response to a need identified by the broader election community. The guide is the first of its kind for the election technology industry and continues CIS's approach of providing cybersecurity best practices for the election community.

The guide is intended to assist election technology providers in identifying the most significant cybersecurity supply chain risks for their products and choosing appropriate risk mitigation approaches for those risks. It also aids in the development and implementation of a meaningful supply chain risk management program.

The guide focuses on the cybersecurity risks involving hardware, firmware, and software that are in the election technology supply chain. In addition to IT that ships with election equipment, this also includes externally-sourced tools used to develop hardware and software in-house, such as software development kits, code libraries, IT infrastructure, and the tools used to create, manage, and maintain that infrastructure.

"Elections officials and technology providers have identified the need for guidance on managing supply chain risk to address the large portion of election technology components that are obtained from upstream manufacturers and developers," said Aaron Wilson, CIS Sr. Director of Election Security. "This guide provides a supply chain threat assessment of each major component of election infrastructure to identify risks and suggest mitigations based on the unique architectures of each component."

Based on the threat assessment, the guide provides a set of attacker goals, the expected threat space, the most common attack types on supply chains, and an analysis of each election infrastructure component and the supply chain threats impacting them with mitigation approaches.

Managing Cybersecurity Supply Chain Risks in Election Technology also includes a non-technical overview of cybersecurity supply chain risk management, and describes a 5-step process for identifying and managing suppliers based on a prioritization of risk to election technology products and services:

- Identify and document supply chain, including asset identification
- Assess risks to prioritize critical components and services as those facing the most significant threats
- Assess your relationships with suppliers relative to criticality of products and services

- Align and manage supplier relationships to manage risk
- Conduct ongoing assessment and monitoring of key dependencies associated with critical components

Just prior to this guide being finalized, the world learned of the SolarWinds supply chain attack. While currently, there is no evidence that the SolarWinds attack impacted election offices, the new CIS guide also provides a SolarWinds supply chain attack case study.

"While details around the SolarWinds attack are still forthcoming, we know that a defense-in-depth strategy of layering different risk mitigation approaches increases the chance of preventing or limiting supply chain attacks," said Wilson. "The case study takes the viewpoint of an organization whose supplier has been successfully attacked, such as a customer of SolarWinds, and shows how to manage suppliers, limit the likelihood of successful attacks, and reduce the consequences when a successful attack occurs."

Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers highlights the importance of reviewing and re-assessing suppliers at regular intervals and verifying and monitoring products prior to and during production, aiding in the development and implementation of a meaningful election technology supply chain risk management program.

CIS would like to thank the Democracy Fund for its generous support of this guide's development.

You can find *Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers* and more Election Security Best Practices Resources on the CIS website: https://www.cisecurity.org/elections-resources/.

About CIS:
The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously refine these standards to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.