SECURITY BULLETIN

Security Management Practices

Every time voters head to the polls, they want to know their votes will be accurately counted and protected. At Election Systems & Software, we take extra precautions to ensure our software, hardware and data are well-insulated from harm.

100%
Every ES&S associate completes annual security awareness training.

0/1,000,000
Our EAC certified systems are required to complete testing with 0 errors in 1 million test ballots.

We don't just follow industry best practices; we help develop and distribute them through a partnership with the U.S. Department of Homeland Security. From internal protocols to training on every piece of equipment, we go above and beyond what's required to keep our elections safe.

HOW WE PROTECT OUR INFRASTRUCTURE

Physical Security

- All ES&S employees, contractors, temps and interns are required to wear an ES&S-issued photo ID badge on company grounds.
- All ES&S facilities are monitored by security cameras, alarms and door badge readers.
- ES&S employees are trained to manage all visitors to the facilities. Visitors are under constant supervision while on ES&S property.

Corporate IT Security

- All ES&S employees, contractors, interns and temps are required to use two-factor authentication when logging into corporate IT networks.
- ES&S uses internal and external security monitoring of our corporate IT environments, including five Albert sensors covering our voter registration environments.
- ES&S constantly prepares for malware attacks by using multiple systems to protect endpoints, servers, backup systems and software development.
- ES&S has DHS conduct cyber hygiene scans of our public-facing internet presence weekly.

PROTECTING ELECTIONS TOGETHER

- ES&S has close working partnerships with DHS, CIS, the FBI and others to share cyber threat information and best practices and prepare for cyber incidents.
- ES&S conducts free Secure The Vote™ training for our customers to develop cybersecurity awareness and the implementation of best practices to protect the equipment used for elections.
- ES&S participates in DHS election security tabletop exercises and has brought the DHS exercise team to our headquarters to conduct in-house tabletop exercises.
- ES&S conducts penetration testing of hardware, firmware and software by commercial third parties, and we have partnered with DHS and the Idaho National Lab to conduct penetration testing of our end-to-end voting systems.

ES&S Security Philosophy

Nothing is more important to ES&S than protecting America's democracy through secure and accurate elections. That's why every ES&S product reflects the company's three-part security philosophy:

- **Design:** All products are designed, without compromise, to meet the latest and ever-evolving standards in security, accuracy and reliability.

- **Testing:** In addition to ES&S testing protocols, all tabulation systems are rigorously tested and certified by the federal Election Assistance Commission (EAC), which reflects security and performance standards developed by scientists, academia and election officials. The ES&S testing protocol also involves testing by independent, accredited laboratories. ES&S submitted our end-to-end voting configuration for Cybersecurity and Infrastructure Security Agency (CISA) critical product evaluation (CPE) at Idaho National Labs.

- **Implementation:** The entire ES&S team is devoted to ensuring that each piece of technology performs as expected on election day, helping election officials uphold the laws of their state which mandate strict physical security and tight chain of custody of all voting machines.

Perhaps most importantly, ES&S' essence — its very being — is predicated on providing America with secure, accurate and accessible elections. Every person at ES&S holds themselves, and each other, accountable for this mandate, and is proud to serve a role in this noble purpose.