# Protecting Voting Systems from Bad Actors

**Safeguarding America's elections is serious business. That's why unauthorized possession of election software is a crime. It is illegal to possess or distribute election software without a license. Illegal activity can be found and prosecuted.**

The likelihood of stolen software by a bad actor impacting an election is extremely low due to the decentralized nature of elections and the many safeguards in place.

## Decentralization

- A bad actor attempting to impact a real-world election would require collusion within an elections office to gain specific election files and access to secured election equipment and encrypted USB flash drives. The ability to maliciously alter a live election is not possible without detection.
- America's election system is decentralized, with wide variations in the way voting is run from state to state or even within the same state.
- The practical administration of an election – from registering voters to organizing local polling places and counting ballots is handled by counties, cities and towns.
- Voting machines are stand-alone devices. To have a material impact on an election you would need physical access to every unit in every poll site.

## Security

- ES&S and election officials apply a multi-layer approach to security. Hardware and software controls are in place to prevent unauthorized changes to election-related data.
- Each ES&S voting machine pairs up with a USB flash drive secured with a unique 256-bit encryption key to ensure that only information specific to that election may be loaded on the machine.
- Voting machines are protected with locks and seals. If there is any indication of attempted tampering or unauthorized physical access, election officials are immediately notified.
- ES&S customers use only industrial-grade USB flash drives made in the U.S. by a U.S.-based company. They are the same quality flash drives used by the U.S. military and aeronautics industries.

## Auditability

- All ES&S voting systems maintain a system-generated audit trail used to verify that elections are administered accurately and accountably. The trail catalogs the date, time and description of every user- or system-initiated event that occurs on the unit. This audit trail would show any illegal or unauthorized software update or change.
- There are many steps taken before and after elections to ensure accuracy, including pre-election logic and accuracy testing and post-election audits. Election officials always have physical paper ballots that can be fully audited to ensure an accurate count.