Supply Chain Assurance

The ability to securely and accurately tabulate ballots begins with protecting the integrity of the equipment used to conduct elections. It's why ES&S takes a comprehensive approach to protect the company's supply chain and deliver solutions that states, jurisdictions and voters can trust. ES&S works with a wide range of supply chain stakeholders to maintain the most secure supply chain possible. With rigorous inspections at every step of the ES&S product life cycle process, ES&S works hard to ensure the integrity of every aspect and component of the company's supply chain.

This document provides a brief overview of ES&S' robust governance mechanisms and supply chain security and integrity practices for the manufacturing of our purpose-built tabulation products.

CONTINUOUS RISK ASSESSMENT AND IMPROVEMENT

The six phases of ES&S' product life cycle serve as a roadmap for the company's security strategy.

ES&S Product Life Cycle – Sustainability & Supply Chain Security

1. Product Requirements
2. Design & Vendor Selection
3. Development & Quality Assurance
4. Certification & Compliance
5. ISO Manufacturing, Incoming Inspection, QC, Order Fulfillment & Implementation, Repeatable Processes
6. Sustainable Engineering, Customer Support & EOL

1

Product Requirements

These initial product requirements include security-focused steps such as setting requirements in standards, development and partner vetting.

2

Design & Vendor Selection

ES&S meets with top engineers and management to evaluate their ability and willingness to meet the company's revision control notification requirements before changes are implemented. The companies that make up ES&S' supply chain are certified and audited by the International Organization for Standardization (ISO). This requirement ensures established processes and protocols are followed.

3

Development & Quality Assurance

ES&S controls more aspects of the design, manufacturing and maintenance of its election equipment than other providers in the industry because the company uses a purpose-built product strategy. This provides better control over which components are used and approval requirements of when each component is changed.

From the standpoint of security, not all parts are equal. Many parts are inert and cannot be compromised, such as a plastic shield for voting privacy. ES&S' top, most robust security measures are in place for any part considered to be a programmable logic device (PLD) — PLDs contain software, firmware or low-level settings, and they control how the equipment operates. ES&S pays extremely close attention to and has robust security protocols in place for sensitive items like PLDs.

ES&S controls more aspects of the design, manufacturing and maintenance of its election equipment than other providers in the industry.

4

Certification & Compliance

ES&S voting systems undergo a series of functional and environmental tests to ensure they meet or exceed the demanding test requirements set by the EAC. Further testing is conducted at the state level to ensure state-specific features perform as needed.

5

ISO Manufacturing, Incoming Inspection, QC, Order Fulfillment & Implementation, Repeatable Processes

ES&S employs multiple layers of protection include using only authorized suppliers for parts acquisition, ISO certified contract manufacturers, incoming parts inspections, quality control checks, firmware verification audits, QC configuration and equipment testing at customer sites.

6

Sustaining Engineering, Customer Support & EOL

This product life cycle concludes with sustainable engineering. While the word sustainability has come to mean many things in the elections industry, ES&S' role in sustainability primarily serves a need for reliable, timely equipment maintenance and certification of operability.

ES&S' strong financial standing, vast supplier relationships, large customer base and extensive research and development capability provide a foundation for long-term availability of its products and parts.

SUPPLIER GOVERNANCE

As is the case with many critical infrastructure sectors, ES&S has certain global supply chain dependencies. ES&S' Engineering Team continually reviews the ability to source components within the U.S. However, some components are sole-sourced, protected by a patent and/or intricate to the design of the circuit or sub-assembly, so there may be limited ability to procure from alternative suppliers. ES&S' experts evaluate the risk and impact of using those components. The company also assesses safeguards to limit risk when using sensitive components in our product offerings. Every aspect of our system is under a secure Engineering Change Order (ECO) control process, regardless of where individual components are produced.

Safeguarding the performance and integrity of the supply chain is critical to supplier governance. One hundred percent of ES&S' shipping partners are Customs-Trade Partnership Against Terrorism (C-TPAT) certified—which is the U.S. Customs and Border Protection's highest level of cargo security. C-TPAT is the Authorized Economic Operator (AEO) program for the U.S. All C-TPAT certified distributors are required to demonstrate that their supply chains are secure from the point of origin to the point of distribution. Other critical infrastructure sectors, including defense and healthcare, trust and use C-TPAT certified distributors.

One hundred percent of ES&S' shipping partners are Customs-Trade Partnership Against Terrorism (C-TPAT) certified.

ES&S' manufacturers use industry-authorized distributors and qualified suppliers for all materials used in the manufacturing of the company's products, which applies regardless of country of origin. ES&S tabulation products are EAC-certified and built following federal guidelines, including the National Institute of Technology (NIST) security protocols and standards and the Center for Internet Security (CIS) Critical Security Controls. Every unit is individually serialized for complete traceability, and ES&S conducts frequent audits and documents proof that the company produces the product-to-design specifications.

Prior to onboarding, ES&S performs a thorough review of potential suppliers and partners, which can include security assessments of manufacturing partners, site surveys and procedural reviews of potential suppliers. As part of ES&S' ongoing relationship with suppliers:

1. ES&S conducts thorough security reviews of its supply chain, including supply chain risk assessments using the NIST Cybersecurity Framework (CSF) tools and on-site visits of ES&S' suppliers, to ensure that every component is trusted, tested and free of defects. These audits utilize both on-site quality teams, as well as site visits to confirm that contract manufacturers are following prescribed processes. ES&S contract manufacturers' procurement and supplier oversight policies are thoroughly vetted by ES&S to ensure they meet the established requirements.

2. ES&S monitors the inventory control practices of all contract manufacturers and third-party suppliers. Third-party facilities must meet security, physical handling, storage and segregation requirements for maintaining inventory. ES&S suppliers and contract manufacturers are monitored for quality and accuracy to ensure customers receive the best product possible. These inventory processes and controls provide day-to-day governance that augments official audits. ES&S voting systems are produced in ISO-9001 manufacturing facilities to ensure procedures are adhered to, resulting in the production of high-quality products. As the entire voting system is managed by ECOs, changes to the voting system follow a formal closed-loop process. They must be internally and externally reviewed, verified, tested and approved before they can be incorporated. Contract manufacturers are notified of approved changes following the ECO process.

   Internal material handling is controlled through ES&S' warehouse control procedures, thereby limiting access to only necessary personnel, which mitigates the risk of missing or contaminated materials. All inventory is subject to incoming inspection procedures to verify the authenticity, accuracy and condition of the materials received from suppliers and contract manufacturers. Once the inspection is complete, the materials are entered into and managed by the company's inventory control system.

3 ES&S takes guidance from the Department of Homeland Security (DHS) to measure suppliers' security practices against industry best practices for physical security and for identifying/mitigating counterfeit components, tainted software and firmware, and intellectual property theft. When gaps are identified, ES&S issues corrective actions and works with suppliers to build their capabilities in meeting industry best practices. Developing a partnership and maintaining constant communication is critical to ensuring that suppliers and contract manufacturers understand the importance of maintaining the security of ES&S' products.

4 Recurring business reviews are conducted with all key suppliers to evaluate performance against ES&S' expectations. Between reviews, ES&S maintains close communication with suppliers via regularly scheduled meetings to address issues as they arise and mitigate their impact. The goal is to ensure ES&S' customers continue to receive high-level, quality products at a competitive price. Frequent executive-level interactions also help ES&S and our partners to respond quickly and effectively to changes in technology, demand, legislation or customer requirements.

SUPPLY CHAIN SECURITY

Supply chain security involves the consistent application of security initiatives, standards and measures to protect intellectual property, inventory, sensitive information and people. By focusing on physical, information, and personnel security, ES&S provides assurance by reducing opportunities for the malicious introduction of malware and counterfeit components into the company's supply chain. Security assessments are conducted on each manufacturing partner.

Physical Security

The factories where ES&S products are built must meet specific facility security requirements, including the use of closed-circuit cameras in critical areas, access controls and continuously guarded entries and exits. Additional controls are implemented at ES&S and supplier-managed facilities to address the various risks across transportation modes and regions. Some of these protections include tamper-evident packaging, security reviews of shipping lanes, locks and container integrity requirements.

ES&S uses in-transit security protocols to protect parts and assembled units as they travel between facilities and to customers. Tamper-proof seals are placed on truckloads, and access to freight terminals is restricted.

Information Security

As part of the company's normal course of business, ES&S acquires and uses sensitive information throughout the supply chain life cycle. Extensive measures are used to safeguard this sensitive information against exposure and misuse. For example, data transfers between ES&S and our partners use a combination of encryption methods and private communication channels. Where applicable, secure protocol and encapsulation technology best practices are also used. In addition, production lines are designed and built to restrict the ability to transfer information.

ES&S' internal network environment is secured through controls such as virus detection, robust password enforcement, email attachment scanning, system and application patch compliance, intrusion prevention, and firewalls. Controls have also been implemented to protect against malware and misuse of assets.

ES&S follows the principles of segregation of duties and least privilege. These principles help prevent misuse of data access across the business by ensuring access to sensitive information is only given to those who need it to perform their job.

ES&S employees, contractors, consultants, partners and any external entity operating under ES&S guidance do not accept any data containing personally identifiable information that is not needed for the specific purposes required. ES&S protects confidential data under a non-disclosure agreement (NDA) or other binding contractual provisions that restrict permissible uses and disclosures of the data.

Personnel Security

Personnel security controls are another critical part of information security and supply chain assurance. Screening employees and restricting access to data, assets and resources helps assure that internal security efforts are effective. ES&S' policy requires employees throughout the supply chain, including those at contract suppliers, go through a pre-employment screening process. This process includes security background checks, drug screening, identity verification and application verification as applicable and permissible by law.

As part of ES&S' annual security training, all employees, contractors, temps and interns (ECTi) are required to complete courses regarding information security and other ES&S security practices. All ECTis are also required to complete an annual comprehensive security training program that covers a wide range of cyber and physical security threats, mitigating controls, realistic scenarios and content module tests. This training program emphasizes good cyber hygiene to be used at home and at work to build respect for and awareness of cyber threats to ES&S' business.

SUPPLY CHAIN INTEGRITY

ES&S' strong supply chain integrity ensures equipment received by the customer is what the customer expected and that the equipment will operate as intended. A fundamental aspect of supply chain integrity is the development of a baseline specification of hardware and software that is safeguarded and used as a reference to verify there have been no unauthorized modifications.

Hardware

A variety of quality control processes are in place to help minimize the opportunity for counterfeit components to infiltrate the ES&S' supply chain. Parts are sourced from authorized distributors, and in the event parts need to be sourced from brokers, those parts are sent to U.S.-based third-party labs for authentication.

ES&S conducts thorough security reviews of its supply chain, including supply chain risk assessments and on-site visits to key suppliers.

ES&S' Quality Management System confirms continued adherence to engineering specifications and processes, including sourcing from approved vendors Each part, regardless of origin, undergoes a thorough incoming inspection by ES&S contract manufacturers before the assembly process. Once units are assembled, ES&S uses a domestic third-party expert to perform firmware verification on a sample of units in each container to confirm no malicious or unwarranted software is present.

Additionally, ES&S conducts thorough security reviews of its supply chain, including supply chain risk assessments and on-site visits to key suppliers to ensure that components are trusted, tested and free of malware. Once the hardware components are delivered to Omaha, ES&S performs several essential steps, including:

- Verification that the firmware on the PLDs within the hardware is exactly what it is expected it to be and not altered in any way
- Final hardware configuration
- Final end-to-end QC test which includes loading of the certified software and firmware

Software

Proactive verification, validation and security testing activities throughout the life cycle help ensure more secure software and reduce the likelihood of malware or coding vulnerabilities from being inserted into software. A robust cybersecurity program improves software integrity by preventing unauthorized access to source code and minimizing the potential for malware to be introduced into a product before it is shipped to the customer.

Each hardware and software release undergoes thousands of hours of independent performance testing and millions of test ballots, along with extensive security testing.

ES&S carefully monitors all software included in the company's solutions to ensure that these solutions continue to meet evolving security needs. If any gaps are highlighted in these software products, ES&S works to ensure the gap is mitigated either through software updates or segmentation of the software.

Part of each ES&S software release includes a review of all software components included in the release. This review consists of an analysis of the security features and any highlighted vulnerabilities. The ES&S security team carefully monitors all highlighted vulnerabilities to determine if any action is required to address the vulnerability. Firmware is verified upon delivery to customers.

In addition, as standard practice to ensure the proper performance of ES&S equipment, each hardware and software release undergoes thousands of hours of independent performance testing and millions of test ballots, along with extensive security testing, after which ES&S provides a complete set of software components to the voting systems testing labs (VSTL) for review.

STRONGER TOGETHER

- ES&S is committed to partnering with leading organizations that further the development of standards and industry best practices for mitigating supply chain and product security risks.
- ES&S is participating in discussions with DHS's National Risk Management Center (NRMC), NIST and CIS regarding the development of guidelines and best practices for ensuring that the company stays ahead of and mitigate new or emerging risks associated with supply chain components.
- ES&S has also been actively engaged with the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the Elections Infrastructure Subsector Coordinating Council (EI-SCC) and the Information Technology Sector Coordinating Council (IT SCC).
- ES&S is well-positioned to leverage best practices, technology, insights and expertise. The company understands the importance of working with federal, state and local agencies, suppliers and partners to improve on and deliver supply chain assurance to its customers.