SECURE THE VOTE™
Chris Wlaschin
Senior Vice President and CISO, ES&S

- Former CISO for HHS
- Deputy CISO for the VA
- Director of Security for National Research Corporation
- CISO for the University of Nebraska
- CIO for the Military Sealift Command
- Chief of Operations for the Defense Intelligence Agency Western Region
- 20+ years U.S. Navy
Who is ES&S?
“Maintain voter confidence and enhance the voting experience.”
Our Mission

Election Systems & Software is dedicated to providing valuable, trusted, and proven election equipment and services to our election administrators.

We continually evolve to meet the needs of our customers and technology’s ever-changing environment. We provide better elections every day to promote democracy in the jurisdictions we serve. We fulfill this mission by delivering the highest standards of accuracy, security, and reliability in our election products and services.

In pursuit of our mission and vision, ES&S is guided by six core values:

- **Strive for Excellence**
  Strive to exceed expectations. Bring the best version of yourself to work everyday. Challenge the status quo. Encourage the best in others.

- **Dream Big**
  Innovate. Encourage broader thinking from the team. Go past the walls of possibility and dig into the unimaginable. Push past your comfort zone.

- **Earn Trust & Respect**
  Commit every day to improving communication. Be a good listener. Do what you say you are going to do.

- **Embrace Differences**
  Foster an environment around acceptance. Create a collaborative and inclusive environment. Actively seek new ideas and perspective. Listen, learn and act.

- **Make a Difference**
  Have a positive impact. Leave it better than you found it. Make your imprint.

- **Have Fun**
  Fulfill a role that plays to your strengths. Express joy in your interactions with others. Celebrate successes.
Security Partnerships & Third-Party Testing

What have we done to keep raising the bar?

- 2018: Hired full-time SVP & CISO, Chris Wlaschin
- Enhanced physical and employee security
- Leadership roles in SCC
  - Vice Chair – 2018
  - Chair – 2019
- Instituted Cyber Incident Response Plans
- Participate in weekly DHS Cyber Scans
- First to join MS-ISAC; founding member of IT-ISAC
- Supply chain audited by DHS, NIST
- Deployed Albert Monitors in partnership with CIS
- Participated in independent penetration testing via ProCircular, BulletProof, multiple states and academic institutions
- Participate in testing at DHS Idaho National Lab
Email & General Security

Key Words & Tips to Protect
<table>
<thead>
<tr>
<th>Phishing</th>
<th>Spear Phishing</th>
<th>Social Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing is a social engineering technique where cyber attackers attempt to fool you into taking an action in response to an email.</td>
<td>Spear phishing describes a type of phishing attack that targets specific victims, so instead of sending out an email to millions of email addresses, cyber attackers send out a very small number of crafted emails to very specific individuals, usually all at the same organization.</td>
<td>The art of manipulating, influencing or deceiving you to get you to take some action that isn’t in your own best interest or in the best interest of your organization.</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>Denial of Service Attacks</td>
<td>Man in the Middle (MTM) Attacks</td>
</tr>
<tr>
<td>A way for attackers to read and/or alter the contents of a user’s database by manipulating forms that are publicly available or exposed.</td>
<td>Prevent legitimate users from accessing information (e.g. databases, websites) or services by disrupting access.</td>
<td>When attackers insert themselves between two or more parties and gain access to any information in transit between those parties.</td>
</tr>
</tbody>
</table>
### Social Engineering Red Flags

<table>
<thead>
<tr>
<th>From: <a href="mailto:YourCEO@work.com">YourCEO@work.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>To: <a href="mailto:you@work.com">you@work.com</a></td>
</tr>
<tr>
<td>Date: Sunday April 1, 2018  4:20 am</td>
</tr>
<tr>
<td>Subject: $$ I need to borrow m0ney $$</td>
</tr>
<tr>
<td>Attachment: IMG_0668.PDF</td>
</tr>
</tbody>
</table>

Hey,

I am out to dine with clients and I forget my wallet at the office. Could you wire me money for the dinner through my bank account at WellsFargo?

Send $400 to the special link below:

http://www.wellsfargo.com

See you tomorrow.

Your CEO

---

**From**

Do you recognize the sender email address? Is it an unexpected or unusual email for them?

**To**

Are there other are people you don’t know CC’d or it is an unusual mix of people?

**Date**

Was is sent at an unusual time, like 4 am?

**Subject**

Did I get an email with a subject line that is irrelevant or does not match the message content? Is the email message a reply to something I never sent or requested?

**Attachments**

Were you expecting an attachment? Is it a recognizable file type?

**Content**

Is the content out of the ordinary for the sender? Do you have an uncomfortable gut feeling?

**Hyperlinks**

Does hovering over a link show a different address for a different website?
Understanding Our Role in Cybersecurity

1. We are all a line of defense
2. We are all a target to exploit
3. Responsibilities
   • Manage passwords
   • Physically secure our computers
   • Protect the data we have access to
   • Avoid risky online behavior
4. “Think before we click”
5. Verify all requests for usernames, passwords and sensitive data
This educational video can be accessed at
Security - Election Systems & Software (essvote.com)
ES&S Voting System

Security Overview

Hash Validations
Digital Signatures
Encryption Keys
Certified USB Media
User Access Control

Electionware (EMS)

EQC

Election Definition

Results

Unofficial Results

Results
Layers of Security

Physical Controls
Restricted access to equipment, locks and seals

System Hardening
Limiting potential attack surfaces by locking systems down

User Authentication
Password protection and least privilege access

Encryption
Using secret keys to prevent data access / manipulation

Data Integrity Validation
Digital signature and hash checks to ensure data integrity

Audit Logs & Trails
System logs, chain of custody documents and audits of results
Layers of Security

Physical Controls

System Hardening

User Authentication

Encryption

Data Integrity Validation

Audit Logs
Supply Chain Security Considerations

• As is the case with many critical infrastructure sectors, ES&S has certain global supply chain dependencies.

• ES&S’ Engineering Team continually evaluates the ability to source components from U.S. sources. Some components are:
  ▪ Sole-sourced
  ▪ Protected by a patent
  ▪ Intricate to the design of the circuit or sub-assembly
  ▪ Not able to be procured from alternative suppliers

• ES&S’ experts evaluate the risk and impact of using those components and assess safeguards to limit risk when using sensitive components.

• Every aspect of our system is under a secure Engineering Change Order (ECO) control process, regardless of where individual components are produced.
ES&S works with leading security experts to create the most secure supply-chain possible — with rigorous inspections at every step — to provide accurate and reliable elections for our nation.
## ES&S Product Life Cycle

### Sustainability & Supply Chain Security

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Product Requirements</td>
</tr>
<tr>
<td>2</td>
<td>Design &amp; Vendor Selection</td>
</tr>
<tr>
<td>3</td>
<td>Development &amp; Quality Assurance</td>
</tr>
<tr>
<td>4</td>
<td>Certification &amp; Compliance</td>
</tr>
<tr>
<td>5</td>
<td>ISO Manufacturing, Incoming Inspection, QC, Order Fulfillment &amp; Implementation, Repeatable Processes</td>
</tr>
<tr>
<td>6</td>
<td>Sustainable Engineering, Customer Support &amp; EOL</td>
</tr>
</tbody>
</table>
ES&S conducts thorough security reviews of its supply chain to ensure every component is trusted, tested and free of defects, including:

- Risk assessments using NIST Cybersecurity Framework (CSF) tools
- On-site visits to suppliers
Supply Chain Security

**VETTING**
- Multi-point, in-depth checks on all ES&S supply chain partners.
- Tamper-proof seals & restricted freight terminal access in transit. Firmware verification upon delivery.

**PRODUCT AUTHENTICATION**
- All electronic components are certified to Electronic Components Industry Association standards.
- Prior to delivery to customers, all units undergo independent testing and final hardware configuration.

**ASSEMBLY**
- Trusted manufacturing partners inspect the components upon arrival.
- 100% of our shipping partners are Customs Trade Partnership Against Terrorism (CTPAT) certified.

**IMPORTING**
- CTPAT

**DELIVERY & INSTALLATION**
Videos on USB security and all of our video products can be found at Video Archives - Election Systems & Software (essvote.com)
Questions?

security@essvote.com