

[Home](#) > [About](#) > [Press Releases](#) > [2019 Press Releases](#) >

**Indiana Secretary of State Connie Lawson and FireE...**

---

# Indiana Secretary of State Connie Lawson and FireEye Partner in Preparation for 2020 U.S. Election

## FireEye to help Indiana protect its election infrastructure against potential breaches

MILPITAS, Calif., Nov. 19, 2019 – FireEye, Inc. (NASDAQ: FEYE), the intelligence-led security company, today announced its participation within the State of Indiana’s election security initiative to establish voter confidence in 2020 and beyond.

Through this partnership, FireEye will provide Indiana counties with internet traffic monitoring to protect against threats and state data intrusions. This includes implementing FireEye technologies at the county level, and FireEye Managed Defense service for active monitoring and hunting of bad actors within their environments to detect and block threats, backstopping their security officials should action need to be taken. This initial 40-month contract will carry the Indiana Secretary of State’s office and counties through the 2022 U.S. election.

“We selected FireEye because of its reputation – in election security, threat intelligence, and in incident response. FireEye has helped us address both detection and prevention with the context needed to act quickly as needed. This partnership also helps further collaboration between the Secretary of State’s office, Indiana counties, FireEye, and the U.S. Department of Homeland Security (DHS),” said Connie Lawson, Indiana Secretary of State and Chief Elections Officer. “This statewide

access to voter registration systems by requiring a multifactor authentication protocol for county election offices, implementing risk-limiting audits, and working with the DHS to perform regular cyber vulnerability scanning on the statewide voter registration system.

“Election security is a growing priority, and the Indiana Secretary of State is leading the nation with the infrastructure it has put in place,” said Tom Guarente, VP, External Affairs & Alliances for U.S. Public Sector at FireEye. “States like Indiana are tackling this challenge holistically and collaboratively by extending beyond just technologies to also focus on emergency management and preparedness. We applaud Secretary Lawson for her leading role in shoring up the State’s election defenses and believe other states will take to Indiana’s leading approach as well.”

FireEye remains committed to helping federal and state and local government entities stay informed on today’s cyber threats and what steps they can take regarding free and fair elections. FireEye election security materials can be found at [www.fireeye.com/elections](http://www.fireeye.com/elections)

### **About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 8,500 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

© 2019 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks or trademarks of FireEye, Inc. in the United States and other countries. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.

### **Media Inquiries:**

[Media.Relations@FireEye.com](mailto:Media.Relations@FireEye.com)

### **Investor Inquiries:**

[Investor.Relations@FireEye.com](mailto:Investor.Relations@FireEye.com)

Why FireEye?

Customer Stories

Careers

Certifications and  
Compliance

Supplier  
Documents

Resources

## EVENTS

Newsroom

Press Releases

Webinars

Events

Awards and  
Honors

Email Preferences

## SUPPORT

Incident?

Report Security  
Issue

Contact Support

Customer Portal

Communities

Documentation  
Portal

Threat Research

FireEye Stories

Industry  
Perspectives

## THREAT MAP

View the Latest  
Threats

+1 877-347-3393

STAY  
CONNECTED



## Cybersecurity Services Agreement

This Agreement between the Indiana Secretary of State ("The State"), Carahsoft Technology Corp., FireEye, Inc., and FireEye, Inc., DBA "Mandiant" ("The Contractors") and Clark County ("The County") is entered pursuant to the following terms and conditions.

Whereas, Securing state and county election infrastructure including associated information technology systems and networks is a matter of great public importance.

Whereas, The State has undertaken to secure an array of coordinated cyber and IT security services provided by The Contractors, available to The County pursuant to This Agreement.

Whereas, terms of IT and cyber security services available to The County from FireEye, Inc., are provided in Attachment A, a procurement by The State, funding for which has been provided by 2018 HAVA Election Security Grant Funds.

Whereas, The State has contracted for certain quantity of IT and cyber security *Incident Response Services* from FireEye, Inc., DBA "Mandiant" as provided in Attachment B, funding for which has been provided by 2018 HAVA Election Security Grant Funds.

Whereas, The State will endeavor to make *Incident Response Services* available to The County on application, based on priority, severity of need, and resource availability, at the sole discretion of The State.

Whereas, neither The State nor The Contractors will levy or assess any charge on The County for services detailed in Attachment A. Optional Utilization of *Incident Response Services* by The County may obligate The County to incidental expenses as detailed in Attachment B.

Whereas, The County acknowledges that in order to fully benefit from the services detailed in This Agreement, cooperation, coordination, effort, and optional incidental expenses on the part of The County will be required.

Whereas, the period of time services detailed in Attachment A and optional services detailed in Attachment B will be available to The County pursuant to This Agreement will be limited to the term of the agreement between The State and The Contractors, such term beginning approximately September 1, 2019 and ending December 31, 2022.

1. **Responsibilities of The County.** Specific responsibilities of The County are detailed in Attachment C.

2. **Responsibilities of The State.** Specific responsibilities of The State are detailed in Attachment D.

**3. Term.** This Agreement shall commence on the date approved by the last signatory and shall end on December 31, 2022.

**4. Definitions.**

**5. Confidential Non Public Infrastructure Security Information and Trade Secrets.**

The County acknowledges that pursuant to This Agreement, The State may provide or produce information designated as "*Non Public Infrastructure Security Information*" and The Contractors may provide or produce information designated as "*Trade Secret*". The County acknowledges and agrees that information designated as "*Non Public Infrastructure Security Information*" or "*Trade Secret*" received pursuant to This Agreement will be handled and maintained in a secure and confidential manner and in accord with the *Indiana Public Records Act* (IC 5-14-3) not provided to third parties or made available for public access without written authorization from The State or The Contractors as applicable.

**6. Federal Funding; Audits; Maintenance of Records.** The County and its contractors, if any, shall maintain all books, documents, papers, accounting records, and other evidence pertaining to services received under This Agreement. The County acknowledges that it may be required to submit to federal or state audit of services received or funds paid on its behalf. If it is determined that The County is a "sub recipient", and if required by applicable provisions of 2 C.F.R. 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements), The County shall submit to a financial and compliance audit, which complies with 2 C.F.R. 200.500 *et seq.*

**7. HIPAA Compliance.** If This Agreement involves services, activities or products subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The County covenants that it will appropriately safeguard Protected Health Information (defined in 45 CFR 160.103), and agrees that it is subject to, and shall comply with, the provisions of 45 CFR 164 Subpart E regarding use and disclosure of Protected Health Information.

**8. Other Federally Required Contract Provisions.** Services provided The County pursuant to This Agreement will be paid for using federal funds. The County acknowledges it may be responsible for compliance with requirements imposed by the federal government such as those set forth in Attachment E. The County will determine its need to comply with federal contract provisions.

**9. Assignment; Successors.** The County binds its successors and assignees to all the terms and conditions of This Agreement.

**10. Assignment of Antitrust Claims.** As part of the consideration for This Agreement, The County assigns to The State all right, title and interest in and to any claims The County may acquire, under state or federal antitrust laws relating to the products or services which are the subject of this This Agreement.



**10. Changes in Services.** The County will not order, commence or bind The State or The Contractors to any additional services, work or expenses, or change the scope of the services provided under This Agreement without written authorization by The State. The County shall make no claim for associated expenses or effort in the absence of a prior written approval and amendment executed by all signatories hereto. This Agreement may only be amended, supplemented or modified by a written document executed in the same manner as This Agreement.

**11. Funding Cancellation** When The State or the Director of the State Budget Agency makes a written determination that funds are not appropriated or otherwise available to support continuation of performance of This Agreement, This Agreement shall be canceled. A determination by the Director of State Budget Agency that funds are not available or otherwise appropriated to support continuation of performance shall be final and conclusive.

**12. Governing Law.** This Agreement shall be governed, construed, and enforced in accordance with the laws of the State of Indiana, without regard to its conflict of laws rules. Suit, if any, must be brought in the State of Indiana.

**13. Indemnification.** The County and The State shall each be solely responsible for their own acts or omissions or acts or omissions of their employees, officials, agents or contractors. Each of the parties to This Agreement is a governmental entity for the purposes of the Indiana Tort Claims Act ("ITCA"), IC 34-13-3 *et seq.* Accordingly, neither party shall be required to indemnify the other, and each party shall bear its own risk of loss in connection with This Agreement.

**14. Insurance.** The State is prohibited by IC § 4-13-1-17(a) from purchasing insurance to cover loss or damage to property and is prohibited by IC § 34-13-3-20(c) from purchasing insurance to cover the liability of The State or its employees. The County shall keep in force during the period of This Agreement such insurance as it deems necessary to protect its interests.

**15. Merger & Modification.** This Agreement constitutes the entire agreement between the parties. No understandings, agreements, or representations, oral or written, not specified within This Agreement will be valid provisions of This Agreement. This Agreement may not be modified, supplemented, or amended, except by written agreement signed by all necessary parties.

**16. Notice to Parties.** Whenever any notice, statement or other communication is required pursuant to This Agreement, it will be sent by first class U.S. mail service or established commercial courier service to the following addresses, unless otherwise specifically advised.  
*Note: See Attachment C "Responsibilities of the County" for notification of IT technical issues, security incidents, or for customer support.*

**A. Notices to The State shall be sent to:**

**Jerold Bonnet, General Counsel  
Office of the Indiana Secretary of State  
200 W. Washington St. Room 201  
Indianapolis, IN 46204**

**B. Notices to The County shall be sent to:**

**17. Order of Precedence; Incorporation by Reference.** Any inconsistency or ambiguity in **This Agreement** shall be resolved by giving precedence in the following order: (1) **This Agreement**, (2) attachments prepared by **The State**, (3) attachments prepared by **The Contractors**. All attachments, and all documents referred to in this paragraph, are hereby incorporated fully by reference.

**18. Severability.** The invalidity of any section, subsection, clause or provision of **This Agreement** shall not affect the validity of the remaining sections, subsections, clauses or provisions of **This Agreement**.

**19. Termination for Convenience.** **This Agreement** may be terminated, in whole or in part, by **The State**, which for the purpose of this paragraph shall include IDOA and the State Budget Agency, whenever, for any reason, **The State** determines that such termination is in its best interest. For the purposes of this paragraph, the parties stipulate and agree that IDOA shall be deemed to be a party to **This Agreement** with authority to terminate the same for convenience when such termination is determined by the Commissioner of IDOA to be in the best interests of the State.

**21. No Warranties.** With respect to **This Agreement** and services provided by **The Contractors**, **The State** makes no warranties of any kind. **The State** disclaims responsibility for any representations or any warranties express or implied made by **The Contractors** or contained in any part of **This Agreement** or attachments hereto.

**22. Waiver of Rights.** No right or responsibility conferred on either party under **This Agreement** shall be deemed waived, and no breach of **This Agreement** excused, unless such waiver is in writing and signed by the party claimed to have waived such right. Neither **The State's** review, approval or acceptance of, nor payment for, services provided pursuant to **This Agreement** shall be construed to operate as a waiver of any rights or responsibilities under **This Agreement**.

**11. Authority to Bind Contractor.** The signatory for **The County** represents that he/she has been duly authorized to execute **This Agreement** on behalf of **The County** and has obtained all

necessary or applicable approvals to make This Agreement fully binding upon The County when his/her signature is affixed, and accepted by The State.

*The remainder of this page is intentionally blank.*



**Non-Collusion and Acceptance**

The undersigned attests, subject to the penalties for perjury, that the undersigned is **The County** or other party to **This Agreement**, or that the undersigned is the properly authorized representative, agent, member or officer of **The County** or other party to **This Agreement**. Further, to the undersigned's knowledge, neither the undersigned nor any other member, employee, representative, agent or officer of **The County**, directly or indirectly, has entered into or been offered any sum of money or other consideration for the execution of **This Agreement** other than that which appears upon the face hereof. Furthermore, if the undersigned has knowledge that a state officer, employee, or special state appointee, as those terms are defined in IC § 4-2-6-1, has a financial interest in **This Agreement**, **The County** or other party attests to compliance with the disclosure requirements in IC § 4-2-6-10.5.

In Witness Whereof, **The County** and **The State** have, through their duly authorized representatives, entered into **This Agreement**. The parties, having read and understood the foregoing terms of **This Agreement** do by their respective signatures dated below agree to the terms thereof.

Clark County [The Contractor]  
By: [Signature]  
JACK COFFMAN PRES CCC  
Name and Title, Printed  
Date: 11-14-19

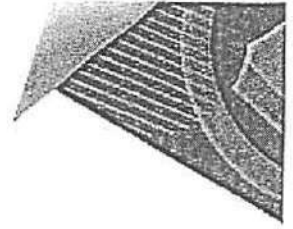
Indiana Secretary of State [The State]

By: \_\_\_\_\_  
Brandon Clifton, Deputy Secretary of State

Date: \_\_\_\_\_

**List of Attachments:**

Attachment A – IT and Cyber Security Services SOW - FireEye Inc. SOW  
Attachment B – Incident Response Services SOW– FireEye, Inc., DBA “Mandiant”  
Attachment C – Responsibilities of The County  
Attachment D – Responsibilities of The State  
Attachment E – Federal Funds Recipient Requirements



## Attachment A

### IT and Cyber Security Services available to Counties

#### STATEMENT OF WORK – US DEPLOYMENT

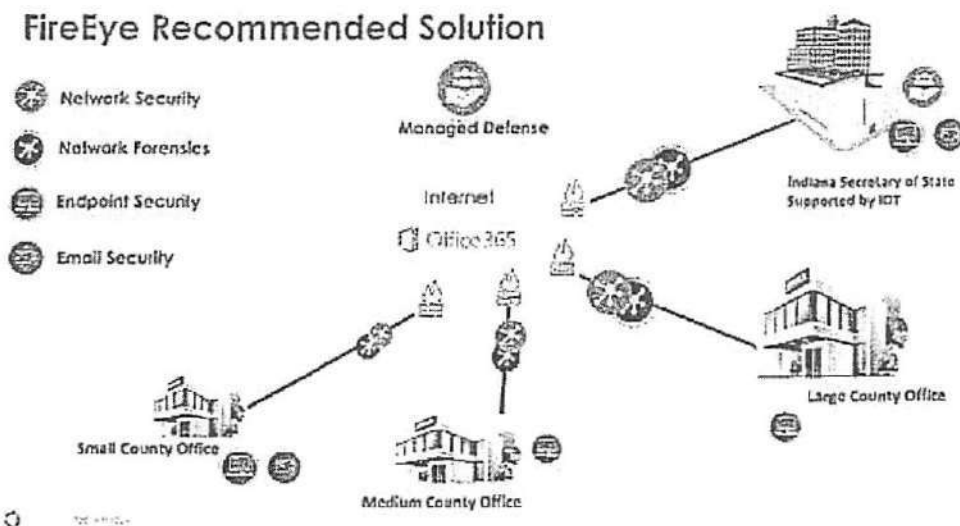
This Statement of Work ("SOW") is effective as of the date of Customer's purchase order \_\_\_\_\_ to the applicable reseller/distributor: Carahsoft Technology Corp. ("Carahsoft"), for the services described in this SOW ("SOW Effective Date"). FireEye, Inc., ("FireEye") will provide the Services described in this SOW to the INDIANA SECRETARY OF STATE ("Customer"). This SOW is governed by the Carahsoft - Customer agreement and the Carahsoft-FireEye Distributor Agreement; the latter incorporating terms at <https://www.fireeye.com/company/legal> for the applicable FireEye Offerings specified in the above-referenced Customer Carahsoft purchase order.

#### 1 DESCRIPTION OF SERVICES:

FireEye will plan, deploy, and integrate the proposed FireEye Security solution to the 92 in-scope State of Indiana County Election Office networks according to FireEye's best practices methodology designed to achieve the best use of the technology. The proposed solution consists of:

- FireEye Central Manager (one cloud management instance across all County Office networks)
- FireEye EndPoint Security (one cloud management console instance across all County Office networks with local software agents deployed on endpoints within each County Office network)
- FireEye Network Security (one physical appliance per County Office network)
- (Optional) FireEye Email Threat Prevention (one cloud management instance across all County Office networks with O365 integration for each County Office email domain)
- FireEye Managed Defense Service (above systems will be provisioned for FireEye Managed Defense Service to provide on-going advanced threat protection for County Office networks).

#### FireEye Recommended Solution





This project will consist of the following activities:

**Project Management**

**During Deployment:**

- FireEye will provide a designated Project Manager for the duration of the installation through the Planning and Design, Installation and Configuration, Configuration and Deployment Testing, and Knowledge Transfer and Operational Handoff phases. The FireEye Project Manager will function as a single point of contact for the FireEye deployment team and will work closely with the Customer Project Manager to schedule and manage the deployment.

**Post Deployment:**

- FireEye will provide a designated Project Manager for the duration of the SOW following the phases listed above. The FireEye Project Manager will coordinate with the Customer and provide project oversight to help ensure deliverables meet mutually agreed timelines and SOW specifications.

**Planning and Design**

FireEye will participate in planning to cover the following:

- Review program objectives, high-level list of activities, and milestones
- Develop detailed project plan listing the activities, dependencies, duration and resources for the deployment activities
- Review County Office network architecture diagrams, change control processes, other business processes, and security goals to determine the appropriate design and configuration plan for the FireEye solution
- Develop policy to be applied across all FireEye Endpoint Security agents and reach agreement on the policy with Customer
- Develop common configuration to be applied for each FireEye Network Security appliance and reach agreement on the configuration with Customer
- Develop configuration to be applied for the FireEye Email Security solution
- Work with Customer PM to gather information from each County Office needed for planning each deployment
- Work with Customer PM to plan the deployment for each County Office

**Installation and Configuration**

To ensure successful installation and configuration, FireEye will assist Customer's EOC with the deployment of the FireEye solution components in their networks. The installation will consist of an initial set up approximately eight pilot County Office networks. Installation of additional County Office networks will be scheduled after the pilot set is complete and lessons learned are incorporated into the plans for remaining deployments. All components for a given County Office /network are to be installed within a single onsite visit up to two days in length.

The deployment services will consist of a combination of tasks and knowledge transfer, including:

**FireEye Central Manager (cloud instance)**

- Provision one FireEye Central Manager (CM) cloud instance to be shared across all COUNTY offices
- Validate access to cloud CM instance
- Configure users and permission sets
- Configure notification settings

FireEye, Inc. | 801 McCarthy Blvd, Milpitas, CA 95035 | 408.331.6300 | 877.FIREEYE (347.3393) | [info@fireeye.com](mailto:info@fireeye.com) | [www.fireeye.com](http://www.fireeye.com)

© 2015 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WFO EH-AJS 022010



#### **FireEye EndPoint Security (cloud instance with local agents)**

- Provision one FireEye Endpoint Security management console cloud instance to be shared across all COUNTY offices
- Configure the agreed upon FireEye EndPoint Security policy to be applied across in-scope endpoints
- Configure the FireEye Endpoint Security management console per FireEye recommended best practices and Customer's requirements
- Integrate the FireEye Endpoint Security management console with the FireEye Central Manager
- Integrate the FireEye Endpoint Security management console with the FireEye Managed Defense service
- For each County Office network, deploy the FireEye Endpoint Security agent on up to five endpoints and verify connectivity and network communications with the Endpoint Security management console
- For each County Office network, provide the FireEye Endpoint Security agent deployment package and instructions for deploying Endpoint Security agents on up to 100 endpoints for devices running supported versions of Microsoft Windows, Linux, or macOS

#### **FireEye Network Security (physical appliance)**

- For each County Office network, deploy one FireEye Network Security physical appliance. For County Office networks where a customer resource is not available to rack and cable the appliance, FireEye will rack and cable the appliance with Customer's guidance on rack location, physical network connections, etc.
- Configure network settings for management port and IPMI port (IP address, subnet mask, and gateway)
- Verify network connectivity for management port and remote accessibility
- Apply latest operating system and security content updates
- Configure network monitoring ports for inline or SPAN/TAP mode per Customer requirements
- Configure the FireEye Network Security appliance according to the common configuration
- Review network traffic statistics for capture ports to verify deployment and configuration
- Integrate the FireEye Network Security appliance with the FireEye Central Manager
- Integrate the FireEye Network Security management console with the FireEye Managed Defense service
- Validate connectivity to Managed Defense
- Test alerting capability and verify alert flow

#### **Optional – Email Threat Prevention (ETP)**

- Provision one FireEye Email Security management console cloud instance to be shared across all County Office
- Integrate FireEye Email Security with Customer's O365 email solution
- Apply the agreed upon configuration for Email Security to detect and prevent email-based threats
- Customer will perform MX record changes to support inline operation of ETP
- Integrate the FireEye Email Security management console with the FireEye Central Manager
- Integrate FireEye Email Security with the FireEye Managed Defense service
- Validate connectivity to Managed Defense



#### **Managed Defense Integration**

- Ensure all components are integrated with FireEye's Managed Defense
- Validate Managed Defense access for all components
- Verify Managed Defense reporting and alerting

#### **Configuration and Deployment Testing**

FireEye will review the architecture, processes, testing, and steps required to validate the proper function and configuration of the FireEye solution within Customer's environment. The mutually agreed upon test plan will include connectivity, configuration, and operational and integration test use cases. FireEye will work with Customer to test the appropriate configurations throughout the deployment to meet their business requirements.

#### **Knowledge Transfer and Operational Handoff**

FireEye will provide up to three knowledge transfer sessions for designated points of contact for Customer Network / Security administrators to cover the installation process, configurations for each product type, and on-going administration and responsibilities for the FireEye security solution. Knowledge transfer sessions will include Managed Defense roles and responsibilities and the operational handoff to Managed Defense.

#### **FireEye Security Engineer – First Year Post Implementation Support and Management**

A FireEye Security Engineer will work as an integral part of Customer's team onsite and remotely to sustain Customer's FireEye solution. Tasks that may be performed by the FireEye Security Engineer include:

- Perform regular status checks on the FireEye solution to ensure the FireEye Network Security, FireEye Endpoint Security, and FireEye Central Manager components are up to date on patches, security content, and guest images and perform updates as needed
- Perform regular health checks on the FireEye solution to ensure components are operating properly and within the expected performance range
- Document health and status checks and any updates made to the FireEye products
- Provide guidance on and assist with additional FireEye appliance deployments as needed
- Time permitting during the FireEye Security Engineer's normal working hours, assist Indiana Secretary of State in following-up on published Managed Defense Investigations within Customer's networks, up to ten investigations per day. This task would consist of attributing the investigation to a county based on affected hostname for an endpoint alert or network sensor name for a network alert and communicating the alert to the county POC
- Provide weekly written status updates

#### **Cyber Security Analyst**

FireEye will provide an on-site resource (Consultant) to support a twelve (12) month period to the executive leadership of Customer to help develop and implement remediation strategies associated with the proposed Security solution activities and initiatives. Consultant will be responsible for interfacing with FireEye Managed Defense resources on behalf of Customer in the event that Rapid Response is required in order to ensure actions are executed in a timely and appropriate manner and addressing or coordinating remediation activities with the counties under the purview of Customer, if needed. Consultant may provide professional services to perform proactive breach detection (hunting) and incident triage. Consultant will work side-by-side with the Security Operations Center (SOC) staff, or Customer Security staff, to assist with



detection, response and containment, at the discretion of SOC leadership, and can also lead Incident Response efforts as required. Consultant will also be available for special projects and will continue efforts to mature the SOC staff by providing on-the-job training during day-to-day operations.

#### Digital Threat Assessments

FireEye will provide six (6) one-time assessments over a thirty-six (36) month period, each assessment will be conducted over thirty (30) days (unless otherwise agreed in writing) (the "Assessment Period"), through which FireEye will search for Keywords to uncover evidence of threat actor activity related to these Keywords. Prior to each Assessment Period, FireEye will meet with the Customer to determine Keywords and conduct a brief quality assurance test on the keywords. FireEye will conduct at least one meeting during each Assessment Period to inform Customer on progress and answer questions about the assessment. Following the conclusion of each Assessment Period, FireEye will provide Customer with one (1) Deliverable report summarizing each applicable assessment findings.

## 2 DELIVERABLES:

The Deliverables to be produced under this SOW are as follows:

- FireEye Implementation Planning Document
- FireEye Solution Design
- Completed FireEye Deployment Checklist for each County Office network including deployment test results
- FireEye Deployment Report
- Weekly Status Updates
- Six (6) individual Digital Threat Assessment Reports

## 3 TERM AND LEVEL OF EFFORT FOR SERVICES:

Services will begin on a mutually agreeable date after the SOW Effective Date; and, except for the Digital Threat Assessment Period (36 months), are expected to take one year to complete (including approximately four months for deployment services and project management services as described above and eight months for post deployment security engineer services as described above). The Deliverables listed in this SOW will be provided during the SOW engagement. Unless otherwise agreed, Services (including FireEye Security Engineer and Cyber Security Analyst services) will be delivered during standard business hours Monday to Friday, excluding U.S. government holidays and scheduled time off. Except for the Digital Threat Assessment Period, all other SOW Services must be used within one year of the SOW Effective Date; and any unused Services expire one year after the SOW Effective Date.

## 4 LOCATION OF PERFORMANCE OF SERVICES:

FireEye will use a blend of onsite and offsite resources to deliver the Services set forth in this SOW.

## 5 FEES AND EXPENSES:

In consideration of the Services to be provided, Customer agrees to pre-pay the Services Fixed Fees as quoted to the Customer by the applicable reseller. Pre-paid Services Fixed Fees will be invoiced on or about the SOW Effective Date and Customer will pay in accordance to the terms of the Agreement (Upfront Billing). Pre-paid Services Fixed Fees are non-cancellable and non-refundable. Quoted Services Fixed Fees include travel expenses for the deployment services specified above for one onsite visit up to two days in length per County Office and for travel to County Offices by the FireEye Security Engineer and/or the Cyber Security Analyst, if required for the performance of the post deployment services.

FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | [info@fireeye.com](mailto:info@fireeye.com) | [www.fireeye.com](http://www.fireeye.com)

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks of their respective owners. WFD-EN-US-022019



## 6 CUSTOMER RESPONSIBILITIES:

The tasks for which Customer is responsible under this SOW are:

- Customer will appoint a primary Project Manager and a secondary Project Manager for FireEye to work with throughout the engagement to schedule deployment activities, knowledge transfer sessions, weekly updates, and follow-up discussions as necessary. Customer Project Manager will act as a single point of contact for Customer throughout the engagement and will facilitate Customer action items to prevent delays in the agreed upon deployment schedule.
- For work performed at Customer's facilities (e.g. each County Office /network), Customer will provide access to the necessary systems, workspace, and Internet access for FireEye's employees including necessary access tokens and ID badges as required for this project.
- For County Office networks where Customer has onsite staff to rack and cable the FireEye appliances, Customer will ensure all FireEye appliances are unboxed, racked, and cabled prior to FireEye's arrival onsite for the installation.
- For County Office networks where Customer does not have onsite staff to rack and cable the FireEye appliances, Customer will inspect FireEye appliances for any sign of physical damage due to shipping and will alert FireEye of such damage prior to FireEye's arrival onsite for the installation. Customer will provide detailed instructions on the placement of the FireEye appliances in the network rack and on the cabling of the appliances. Customer will provide power cables compatible with the available rack, a power source with two outlets for each appliance, and the appropriate network cables for monitoring and management ports for each FireEye appliance.
- Customer will deploy FireEye Endpoint Security agents to in-scope endpoints beyond the initial five endpoints within each County Office Office/network that are deployed by FireEye. FireEye will provide the Endpoint Security agent installation package and instructions.
- Throughout the course of this engagement, Customer will make available key individuals within its organization and information that can best help plan and execute the Services described in this SOW, including:
  - Customer staff members will be available to provide infrastructure support during the installation / configuration
  - Customer will provide FireEye with relevant network diagrams and other relevant documentation to facilitate proper deployment of FireEye systems
  - Customer will make available staff members for knowledge transfer during the scheduled services delivery period

## 7 CONTACT INFORMATION:

Customer will provide contact information to FireEye for those Customer personnel who are designated as Customer's points of contact for the Services.



**Attachment B**  
**Optional Incident Response Services**



Statement of Work

SOW#

This Statement of Work ("SOW") is effective as of the date of Customer's purchase order 1959569-02 to the applicable reseller/distributor: Carahsoft Technology Corp. ("Carahsoft"), for the Services described in this SOW ("SOW Effective Date"). FireEye, Inc., ("FireEye") will provide the Services described in this SOW to the INDIANA SECRETARY OF STATE ("Customer"). This SOW is governed by the Carahsoft - Customer agreement and the Carahsoft-FireEye Distributor Agreement, the latter incorporating terms at <https://www.fireeye.com/company/legal> for the applicable FireEye Offerings specified in the above-referenced Customer - Carahsoft purchase order.

Mandiant agrees to provide services ("Services") as set forth below. The Services will consist of the following:

Mandiant agrees to provide incident response services ("Incident Response Services") during the forty (40) month period from the SOW Effective Date (the "Covered Period"). Each request for Incident Response Services that is confirmed under this SOW, will consume a minimum of forty (40) hours. During the Covered Period Mandiant will provide Incident Response Services as requested by Customer in the following areas:

- Computer security incident response support
- Digital forensics, log, and malware analysis support
- Incident remediation assistance

Upon SOW execution, Customer will receive a welcome letter that describes the Mandiant Incident Response Service Declaration Process, 24/7 contact information and email address for requesting Incident Response Services. Customer is provided access to Mandiant's toll-free hotline, which is available twenty-four (24) hours a day and seven (7) days a week.

Following Customer's request for Incident Response Services, Mandiant will engage with Customer to determine if Incident Response Services are required or if Mandiant is able to effectively assist based on the situation. Mandiant will respond to Customer's request within a maximum of four (4) hours following the initial request. If Mandiant and Customer agree that Incident Response Services are necessary, Mandiant will assign a Mandiant Incident Response Lead ("IR Lead") within twenty-four (24) hours of the Customer's request for Incident Response Services. The time frames to respond to Customer's request for Incident Response Services and assign an IR Lead, as described above, are collectively called the "IR Service Levels."

Upon engagement for Incident Response Services as described above, the IR Lead will determine the appropriate next steps with Customer. This may include one of the following common scenarios: 1) Customer provides Mandiant evidence (e.g., logs, malware samples, forensic images or live response datasets) to analyze, 2) Customer leverages Mandiant's endpoint technology, either remote or on premise, to enable Mandiant to perform analysis of a system of interest or a large number of systems. During this discussion, Customer and Mandiant will determine the appropriate technology stack, if any, required to complete the analysis.

If Mandiant and Customer determine that the requested Incident Response Services can be performed using Mandiant's technology stack, Mandiant will provide the required components to Customer for installation on the Customer endpoints

to be analyzed (each, an "Endpoint"). Mandiant may also provide network equipment to Customer for installation to facilitate Mandiant's network monitoring procedures.

Customer acknowledges that Mandiant may use other tools, including cloud-based analytics tools and cloud-email monitoring tools, in the course of performing Services, and agrees that Mandiant may use all such tools in its discretion. Customer will cooperate with Mandiant to facilitate Mandiant's use of any such tools. Any charges for such tools are set forth in the Technology Fees section of this SOW (Section 5) or will be agreed upon between the parties jointly in writing.

Mandiant and Customer will coordinate the delivery of the Incident Response Preparedness Service one time during the first twelve (12) months of the SOW Covered Period. This service is an essential part of the Incident Response Retainer Service and should be completed as early as possible to ensure Mandiant's ability to respond effectively to your Incident Response needs. The objective is to complete this activity within ninety (90) days from the SOW Effective Date. The Incident Response Preparedness Service is designed to provide Mandiant with an understanding of Customer's current capabilities to support a Mandiant Incident Response engagement. This activity will be conducted at a single Customer location and will include the following:

- Mandiant will conduct up to four (4) workshops with key managers, team members, and technical leaders within the organization to better understand Customer's environment, ability to quickly deploy Mandiant technology, and to immediately provide Mandiant first responders with the critical information. These workshops will review existing Customer incident response plans, technologies deployed and log sources in place to detect, analyze, and respond to a breach.
- Mandiant will provide recommendations on necessary play books for Customer to develop and maintain, to ensure:
  - Proper procedures and points of contact are known for technology (software and hardware) deployment.
  - Customer can quickly provide critical information to enable the incident response team to investigate a breach.

In addition to the Mandiant Services described in Section 1.1 and 1.2 of this SOW, during the Covered Period, Mandiant may provide additional consulting services on a per-request basis, as described below. The activities to be performed may be more explicitly defined and approved as mutually agreed upon "Work Orders" under this SOW or, in some cases where a Work Order is not necessary, may be described on informational quotes accepted by Customer. For purposes of clarity, this SOW does not obligate Customer to any additional fees unless and until both parties execute a Work Order as set forth below, or, if no Work Order is necessary, until the Customer has accepted FireEye's informational quote. Customer's receipt of Services will constitute acceptance of the quote. The following services can be requested via a Work Order:

- Mandiant Strategic Consulting Services
  - Security Program Assessment
  - Security Program Transformation
  - Response Readiness Assessments
  - Table Top Exercises
- Mandiant Technical Services
  - Compromise Assessments
  - Investigative Support, Forensics, Litigation Support, and Advisory Services (other than Incident Response Services)
- Mandiant Proactive Services
  - Vulnerability Assessments
  - Penetration Testing
  - Red Team Assessments
  - Red Team Operations

For each Work Order under this SOW, Mandiant and Customer will agree on a defined scope and any Deliverables that are unique to each Work Order, and the number of hours to be drawn from the total purchased as set forth in Section 4. Each Work Order will be a separate document governed by this SOW.

#### Work Order Process

During the Covered Period, Customer may request Services under this Section 1.3 of this SOW, and if mutually agreed, Mandiant and Customer may enter into a separate, mutually agreed-upon work order ("Work Order") with respect to such Services. All such Work Orders will incorporate and be governed by the terms of the Agreement and this SOW.

Each Work Order under this SOW will contain the following sections:

- Detailed description of requested work
- Estimate of requested effort including hours and duration
- Work Order Deliverables
- Estimated expenses and fees (including technology fees, if applicable)

Process for execution of a Work Order:

- Customer will request a Work Order estimate from Mandiant
- Mandiant will develop at no cost to Customer a Work Order containing the sections as described above.
- Mandiant will then send the Work Order to the Customer for review and approvals.
- A Work Order shall be deemed accepted only if executed by authorized signatories of each party.

All work under specific Work Orders will be performed in accordance with the hourly rate quoted by the applicable reseller. Services under a Work Order will not commence until the Work Order has been executed. Customer will pay all invoices as agreed between Customer and the applicable reseller. Unless otherwise agreed upon in the Work Order, invoices for the fees and expenses will be issued on a monthly basis in arrears. Actual expenses will be invoiced as set forth in Section 6 and technology fees will be invoiced as set forth in Section 5.

Below are Deliverables that may be produced. Additional Deliverables may be defined as part of Work Orders as described in Section 1.3.

Any other reports (including intelligence reports), presentations, materials or other written information provided by Mandiant as a result of the Services are Mandiant IP and will not be considered "Deliverables" as defined in the Agreement.

The following Deliverables may be produced for Incident Response Services:

- **Incident Response Status Reporting** – During a declared Incident Response engagement, Mandiant will provide weekly status reporting that will summarize activities completed, key engagement statistics, issues requiring attention and plans for the next reporting period.
- **Incident Response Final Report** – Upon completion of any declared Incident Response engagement, Mandiant will provide a detailed final report covering the engagement activities, results and recommendations for remediation in a written detailed technical document.

– Upon completion of any declared Incident Response Service engagement and as required to inform senior executives or board level members, Mandiant will provide an executive brief that summarizes engagement results and recommendations in executive format.

– Upon completion of the Incident Response Preparedness Service, Mandiant will provide an executive-level brief detailing Mandiant's recommendations to improve Customer's incident preparedness capabilities. The report will include an inventory of existing Customer incident response plans, technologies deployed, and log sources in place to detect, analyze, and respond to a breach.

All parties will mutually agree to the scheduling of Services under this SOW and each Work Order, as applicable. Any Services described in Section 1.3 must commence within the Covered Period, and must be requested no later than forty-five (45) days prior to the end of the Covered Period to allow for scheduling so that Services may commence prior to the end of the Covered Period.

Customer agrees to pay the fees incurred as quoted to Customer by the applicable reseller and any applicable expenses incurred. Customer will pay the pre-paid fees quoted by the applicable reseller ("Pre-Paid Fees"), which will include fees for the IR Service Levels, Incident Preparedness Service and 570 Pre-Paid Hours ("Pre-Paid Hours"). Pre-Paid Fees are non-cancelable and non-refundable. Any hours incurred for Services that exceed the Pre-Paid Hours ("Additional Hours") will be invoiced monthly in arrears, as they are incurred, according to the Additional Hours rate quoted by the reseller. Pre-Paid Fees do not include Additional Hours, travel time, technology fees, expenses, or long-term evidence storage. All such fees and costs will be invoiced monthly in arrears, as they are incurred.

When Customer has requested Services under this SOW and Mandiant has been engaged, Mandiant and Customer will determine the appropriate technology components required. In addition to professional services fees in Section 4, Customer agrees to pay technology fees in support of Services as quoted to Customer by the applicable reseller.

Customer shall reimburse Mandiant for the following expense categories that are directly attributable to work performed under this SOW:

- Travel and living expenses.
- Mileage in company or personal vehicles
- Computer storage media.
- Postage and courier services.
- Shipping, freight, import duties, and tariffs.
- Printing, reproduction, and binding.
- Any other expenses resulting from the work performed under this SOW.

Upon request, Mandiant will provide electronic copies of expense receipts for all expense related items greater than \$25. Expenses will be invoiced monthly in arrears as incurred.

1. Mandiant will provide Deliverables to Customer throughout this engagement. Draft Deliverables are considered final upon confirmation from Customer (written or oral) or ten (10) business days after their submission date from Mandiant to Customer, whichever is earlier.
2. When Mandiant's personnel are performing Services on site at Customer's premises, Customer will allocate appropriate working space and physical access for all Mandiant assigned personnel. To accomplish the work described in this SOW or a Work Order, Mandiant may use both onsite or off-site personnel, depending on the tasks desired by Customer and agreed upon by Mandiant.
3. Customer will make available key individuals that can best help plan operations around security event monitoring, analysis, threat intelligence, and incident response.
4. Estimated professional fees do not include any hardware, software, licensing, maintenance, or support costs of any Mandiant or other third-party product or service suggested by Mandiant as we conduct the activities outlined within this SOW.
5. All parties will mutually agree upon any changes to this SOW in writing.

Customer will provide Mandiant with points of contact information in the following table:

Technical Point of Contact	
Name:	
Title:	
Email:	
Phone:	
Street:	
City:	
State:	
Zip:	

The below terms will apply to any Proactive Service (including penetration testing and red team engagements) requested under this SOW or any Work Orders.

1. As a part of any penetration testing that may be part of this SOW, Mandiant may, among other things, (a) scan Customer's network and systems for ports, services and other entry points that can be exploited; and (b) probe those entry points in an effort to gain access to Customer's network and systems in an effort to determine the severity of the vulnerability.
2. CUSTOMER UNDERSTANDS THAT, ALTHOUGH MANDIANT TAKES PRECAUTIONS TO AVOID DAMAGE TO CUSTOMER'S NETWORK AND SYSTEMS, DISRUPTIONS, OUTAGES AND/OR DATA LOSS MAY OCCUR AS A RESULT OF ANY PENETRATION TESTING. Customer represents and warrants that all systems

on its network or otherwise accessible during the penetration test have been backed up, and that any data loss or other damage caused by the penetration testing can be easily and quickly reversed.

3. If appropriate, Customer will provide to Mandiant certain information required for performing its tests, including a description and location (e.g., an IP address) of the systems and networks to be tested. Customer represents and warrants that all information provided is true and accurate and that Customer owns or is authorized to represent the owners of the systems and networks described in connection with the penetration testing.
4. If appropriate, Customer may inform all or a selected group of its employees, contractors, and other third parties about any penetration testing to be undertaken by Mandiant. In the event that Customer decides not to inform anyone of the penetration testing, Customer understands that people may spend time and money on behalf of Customer in detecting, blocking, investigating or responding to activities of Mandiant. IN LIGHT OF THE POSSIBILITY THAT SUCH ACTIONS MAY BE TAKEN AND EXPENDITURES MAY OCCUR, CUSTOMER SHOULD CONSULT WITH CUSTOMER'S LEGAL COUNSEL AND/OR A MEMBER OF EXECUTIVE MANAGEMENT PRIOR TO ANY SUCH ZERO KNOWLEDGE ENGAGEMENTS. Customer may also want to consider contacting such third-party service providers as Customer's telecommunications carrier to alert them to the testing.
5. If appropriate, user data contained on systems that are tested may be accessible to Mandiant and Mandiant may download portions of such data (e.g., as proof of access).
6. If appropriate, at any point during the testing, either party may pause or stop the test. Should the testing be terminated, a rationale for such termination shall be provided by the party requesting such termination and such rationale shall be clearly documented.

## **Attachment C**

### **Responsibilities of the County**

The tasks for which The County is responsible under This Agreement are:

- The County will provide and authorize an appropriate primary representative and points of contact for coordination, scheduling, technical information, deployment and local management of the IT and cyber security services as detailed in Attachment A.
- The County will authorize appropriate employees and contractors to facilitate The Contractors deployment and provision of IT and cyber security services detailed in Attachment A.
- The County will provide a primary representative, employees and contractors as-needed during The Contractors installation and configuration of network security appliances (up to 2.5 days) as detailed in Attachment A.
- The County will provide feedback and status reports on an as-needed basis to The State to confirm The Contractors satisfactory installation and deployment of network security appliance and provision of IT and cyber security services detailed in Attachment A.
- In the event of an applicable IT or cybersecurity incident, The County will follow the *"IT or cyber security incident notification protocol"* provided by The State, which will include prompt notification of designated parties as soon as possible, or in no event later than 24 hours, of an applicable IT or cyber security incident.
- In the event of an applicable IT or cyber security incident, The County may apply to The State for *Incident Responses Services* which may be provided at the discretion of The State. Utilization of *Incident Response Services* by The County may obligate The County to incidental expenses as detailed in Attachment B.
- In the event of an applicable IT or cyber security incident, The County will use its best efforts to preserve forensic evidence and facilitate investigation and response by The Contractors and law enforcement agencies.
- The County will, throughout the term of This Agreement be responsible for its own efforts and incidental expenses associated with deployment and provision of IT and cyber security services and optional *Incident Response Services*.
- At the end of the term of The Contractors provision services, The County will accommodate removal of provided security appliances and cessation of services.



## **Attachment D**

### **Responsibilities of The State**

Tasks for which The State are responsible under This Agreement are:

- The State will coordinate contracting, administration and funding The Contractor's activities and provision of IT and cyber security services detailed in Attachment A and optional provision *Incident Response Services* if needed and approved, as detailed in Attachment B. The State is *not* obligated to incur or reimburse on behalf of The County, incidental *Incident Response Services* expenses detailed in Attachment B.
- The State will coordinate the business relationship between points of contact for The County and The Contractors.
- On an as-needed basis, The State will coordinate discussion and planning, kick-off meetings, network infrastructure analysis, configuration workshops, and status updates with, and between, representatives of the The County and The Contractors.
- The State will provide points of contact for The County and "*IT or cyber security incident notification protocol*" for notification of security incidents and technical issues pertaining to IT and cyber security services and optional *Incident Response Services* provided by The Contractors.

## Attachment E

### FEDERAL REQUIREMENTS

Reference to "Contractor" shall mean the County. References to "this Contract" shall mean the Data Exchange Agreement.

#### 1. AUDITS AND ACCESS TO RECORDS:

A. The Contractor acknowledges that some or all of the funds for this Contract are from a U.S. Department of Commerce ("DOC") grant. The Indiana Department of Technology, the U.S. Department of Commerce, the Comptroller General of the United States, or any of their duly authorized representatives shall have access to any books, documents, papers, and records that are pertinent to this Contract for the purpose of making an audit, examination, excerpts, and transcriptions. Unless a longer retention period is required by 44 CFR 13.42; these materials shall be maintained by the Contractor and made available at their respective offices at all reasonable times until January 27, 2018. Copies thereof shall be furnished at no cost. The rights of access in this provision are not limited to the required retention period but shall last as long as the records are retained.

B. The Contractor shall comply with the OMB Circulars A-87 (Cost Principles for State, Local and Tribal Governments) and 15 CFR 24 (UNIFORM ADMINISTRATIVE REQUIREMENTS FOR GRANTS AND COOPERATIVE AGREEMENTS TO STATE AND LOCAL GOVERNMENTS).

#### 2. INTELLECTUAL PROPERTY RIGHTS

A. Data, Databases, and Software. The rights to any work produced or purchased under a DOC Federal financial assistance award are determined by 15 CFR § 24.34 and 15 CFR § 14.36. Such works may include data, databases or software. The recipient owns any work produced or purchased under a DOC Federal financial assistance award subject to DOC's right to obtain, reproduce, publish or otherwise use the work or authorize others to receive, reproduce, publish or otherwise use the data for Government purposes.

B. Copyright. The recipient may copyright any work produced under a DOC Federal financial assistance award subject to DOC's royalty-free nonexclusive and irrevocable right to reproduce, publish or otherwise use the work or authorize others to do so for Government purposes. Works jointly authored by DOC and recipient employees may be copyrighted but only the part authored by the recipient is protected because, under 17 U.S.C. § 105, works produced by Government employees are not copyrightable in the United States. On occasion, DOC may ask the recipient to transfer to DOC its copyright in a particular work when DOC is undertaking the primary dissemination of the work. Ownership of copyright by the Government through assignment is permitted by 17 U.S.C. § 105.

#### 3. DEBARMENT AND SUSPENSION. As required by 2 CFR 3000.332, the Contractor shall:

- A. Comply with Subpart C of the OMB guidance in 2 CFR part 180; and
- B. Include a similar term or condition in any covered transaction into which it enters at the next lower tier.

#### 4. LOBBYING CERTIFICATION

A. The Contractor acknowledges that a Federal grant is the source of payments under this Contract and as required by Section 1352, Title 31 of the U.S. Code, and implemented at 44 CFR Part 18, the Contractor certifies that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of a federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any Federal grant, the making of any federal loan, the entering of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form - LLL, "Disclosure of Lobbying Activities," in accordance with its instructions;

(3) The Contractor shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, contracts under grants loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

B. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

#### 6. TRAFFICKING IN PERSONS

A. Provisions applicable to a recipient other than a private entity. The Federal Awarding Agency may unilaterally terminate this award, without penalty, if a subrecipient that is a private entity:

- i. Is determined to have violated an applicable prohibition in paragraph A.i., above; or
- ii. Has an employee who is determined by the agency official authorized to terminate the award to have violated an applicable prohibition in paragraph A.i, above, through conduct that is either:
  - a. Associated with performance under this award; or
  - b. Imputed to the subrecipient using the standards and due process for imputing the conduct of an individual to an organization that are provided in 2 CFR part 180, "OMB Guidelines to Agencies on Government-wide Debarment and Suspension (Non-procurement)," as implemented by the Federal Awarding Agency at 2 CFR part 3000.

B. Provisions applicable to any recipient.

i. You must inform the Federal Awarding Agency and the State immediately of any information you receive from any source alleging a violation of a prohibition in paragraph A.i, above.

ii. The Federal Awarding Agency's right to terminate unilaterally that is described in paragraph A.ii or B, above:

a. Implements section 106(g) of the Trafficking Victims Protection Act of 2000 (TVPA), as amended (22 U.S.C. 7104(g)), and

b. Is in addition to all other remedies for noncompliance that are available to the Federal Awarding Agency under this award.

iii. You must include the requirements of paragraph A.i., above, in any subaward you make to a private entity.

C. Definitions. For purposes of this award term:

i. "Employee" means either:

a. An individual employed by you or a subrecipient who is engaged in the performance of the project or program under this award; or

b. Another person engaged in the performance of the project or program under this award and not compensated by you including, but not limited to, a volunteer or individual whose services are contributed by a third party as an in-kind contribution toward cost sharing or matching requirements.

ii. "Forced labor" means labor obtained by any of the following methods: the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

iii. "Private entity" means:

a. Any entity other than a State, local government, Indian tribe, or foreign public entity, as those terms are defined in 2 CFR 175.25.

---



---

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION**  
Washington, DC 20549

---

**FORM 8-K**

---

**CURRENT REPORT**  
**Pursuant to Section 13 or 15(d) of**  
**The Securities Exchange Act of 1934**

**Date of Report (Date of earliest event reported): December 8, 2020**

---

**FireEye, Inc.**  
(Exact name of registrant as specified in its charter)

---

**Delaware**  
(State or other jurisdiction  
of incorporation)

**001-36067**  
(Commission  
File Number)

**20-1548921**  
(IRS Employer  
Identification No.)

**601 McCarthy Blvd.**  
**Milpitas, CA 95035**  
(Address of principal executive offices, including zip code)

**(408) 321-6300**  
(Registrant's telephone number, including area code)

**Not Applicable**  
(Former name or former address, if changed since last report.)

---

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

- ☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
- ☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- ☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- ☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

<u>Title of each class</u>	<u>Trading Symbol(s)</u>	<u>Name of each exchange on which registered</u>
<b>Common Stock, par value \$0.0001 per share</b>	<b>FEYE</b>	<b>The NASDAQ Global Select Market</b>

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

---

---

## Item 8.01 Other Events.

On December 8, 2020, concurrently with the filing of this Current Report on Form 8-K, FireEye, Inc. ("FireEye", "we", "our" or "us") is announcing on our corporate blog that FireEye recently was attacked by a highly sophisticated cyber threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Based on his 25 years in cyber security and responding to incidents, Kevin Mandia, our Chief Executive Officer, concluded we are witnessing an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past. We are actively investigating in coordination with the Federal Bureau of Investigation and other key partners, including Microsoft. Their initial analysis supports our conclusion that this was the work of a highly sophisticated state-sponsored attacker utilizing novel techniques.

During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers' security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the tools contain zero-day exploits. Consistent with our goal to protect the community, we are proactively releasing methods and means to detect the use of our stolen Red Team tools. We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools. We have seen no evidence to date that any attacker has used the stolen Red Team tools. We, as well as others in the security community, will continue to monitor for any such activity. At this time, we want to ensure that the entire security community is both aware and protected against the attempted use of these Red Team tools.

Consistent with a nation-state cyber-espionage effort, the attacker primarily sought information related to certain government customers. While the attacker was able to access some of our internal systems, at this point in our investigation, we have seen no evidence that the attacker exfiltrated data from our primary systems that store customer information from our incident response or consulting engagements or the metadata collected by our products in our dynamic threat intelligence systems. If we discover that customer information was taken, we will contact them directly.

For additional information, please see FireEye's corporate blog at [fireeye.com/blog](https://fireeye.com/blog). We currently intend that any further announcements regarding the security incident will be disclosed on our corporate blog at [fireeye.com/blog](https://fireeye.com/blog) or social media ([twitter.com/fireeye](https://twitter.com/fireeye); [twitter.com/mandiant](https://twitter.com/mandiant); [facebook.com/FireEye/](https://facebook.com/FireEye/); and/or [linkedin.com/company/fireeye](https://linkedin.com/company/fireeye)).

## Forward Looking Statements

Certain statements contained in this Current Report on Form 8-K constitute "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These forward-looking statements are based on our current beliefs, understanding and expectations and may relate to, among other things, statements regarding our current beliefs and understanding regarding the impact and scale of the disclosed event and our understanding of what occurred. Forward-looking statements are based on currently available information and our current beliefs, expectations and understanding, which may change as the investigation proceeds and more is learned, including what was targeted and accessed by the attacker. These statements are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to FireEye. These risks and uncertainties include but are not limited to our ongoing investigation, including the potential discovery of new information related to the incident.

Forward-looking statements speak only as of the date they are made, and while we intend to provide additional information regarding the attack, FireEye does not undertake to update these statements other than as required by law and specifically disclaims any duty to do so.

**SIGNATURES**

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

**FIREEYE, INC.**

Date: December 8, 2020

By: /s/ Alexa King

Alexa King

*Executive Vice President, General Counsel and Secretary*



**State of Indiana (/)** > **IDOH Calendar (https://events.in.gov/idoh)** >

STATE NOTIFYING HOOSIERS ABOUT IMPROPER ACCESS OF CONTACT TRACING INFORMATION

## STATE NOTIFYING HOOSIERS ABOUT IMPROPER ACCESS OF CONTACT TRACING INFORMATION



📅 Tuesday, August 17, 2021 10:30am



### ABOUT THIS EVENT

**Add to calendar** 📅

INDIANAPOLIS — The Indiana Department of Health (IDOH) is notifying nearly 750,000 Hoosiers that data from the state's COVID-19 online contact tracing survey was improperly accessed. The data included name, address, email, gender, ethnicity and race, and date of birth.

The state was notified of the unauthorized access on July 2. Last week, the state and the company that accessed the data signed a “certificate of destruction” to confirm that the data was not released to any other entity and was destroyed by the company.

When the state was notified of the unauthorized access, the Indiana Office of Technology and IDOH immediately corrected a software configuration issue and requested the records that had been accessed. Those records were returned on Aug. 4.

“We believe the risk to Hoosiers whose information was accessed is low. We do not collect Social Security information as a part of our contact tracing program, and no medical information was obtained,” said State Health Commissioner Kris Box, M.D., FACOG. “We will provide appropriate protections for anyone impacted.”

The state Department of Health will send letters to affected Hoosiers to notify them that the state will provide one year of free credit monitoring and is partnering with Experian to open a call center to answer questions from those impacted. In addition, the Indiana Office of Technology will continue its regular scans to ensure information was not transferred to another party.

“We take the security and integrity of our data very seriously,” said Tracy Barnes, chief information officer for the state. “The company that accessed the data is one that intentionally looks for software vulnerabilities, then reaches out to seek business. We have corrected the software configuration and will aggressively follow up to ensure no records were transferred.”

###

EVENT DETAILS

EVENT TYPE	CALENDAR
------------	----------

**PRESS RELEASES****(HTTPS://EVENTS.IN.GOV/SEARCH/EVENTS?****EVENT\_TYPES%5B%5D=34006056633355).****AGENCY****(HTTPS://EVENTS.IN.GOV/SEARCH/EVENTS?****EVENT\_TYPES%5B%5D=34731297000171).****IDOH****(HTTPS://EVENTS.IN.GOV/SEARCH/EVENTS?****EVENT\_TYPES%5B%5D=34733410550388).****GROUP****Department of Health****(/group/idoh).****CONTACT EMAIL**media@isdh.in.gov(mailto:media@isdh.in.gov).



# Voter Portal



## Election Security

In Indiana, we take great care to prepare for each election. The security of our election systems is of the utmost importance, and in addition, to physical and cyber security, information is a powerful defense. In partnership with counties, other states, and the federal government, we are developing new answers to security concerns and election policy. Some of the tools and precautions being taken in Indiana to ensure secure voting include:

## Our Partners

- **Voting System Technical Oversight Program (VSTOP)**

Hosted by Ball State University, this program tests all of the election equipment used in Indiana for an added layer of safety and security. After VSTOP reviews the system to ensure its compliance with the law, their recommendation is presented to the bi-partisan Indiana Election Commission, the body responsible for certifying voting systems for use in Indiana.

- **IU Center for Applied Cybersecurity Research (CACR)**

The Indiana Secretary of State's Office has partnered with Indiana University to review and improve the state's election cybersecurity incident response plan and will help prepare election officials in all 92 Indiana counties for cybersecurity incidents related to the 2020 General Election and beyond.

The project will have three parts:

1. Creation and delivery of a suite of materials and table-top training events prior to the 2020 elections, including a series of regional "boot camps" with county clerk offices to train election officials about how to respond to different forms of cyberattacks, such as phishing, phone scams and impersonation calls.
2. Ongoing consulting with Indiana's Secretary of State and county clerks during the 2020 election season
3. Post-election documentation of lessons learned and recommendations for the future

- **FireEye**

FireEye provides intrusion detection and prevention systems at the state and county level. They monitor internet traffic accessing websites and databases to prevent bad actors from accessing critical election information. This partnership not only prevents and blocks cyber threat, in the event of an incident, FireEye will provide resources to remove the threat.

- **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**

An independent entity that partners with the U.S. Department of Homeland Security, this allows us access to 24/7 security information, threat notifications, and security advisories.

- **U.S. Department of Homeland Security**

The Federal Government has conducted risk and vulnerability testing to secure Indiana's electronic information such as the Statewide Voter Registration System and the state election website.

## **Our Tools**

- **Multifactor Authentication Protocol for County Election Offices**

The Statewide Voter Registration System is used by the state and the counties to maintain voter registration list. We are investing in security at all levels by implementing validation requirements to ensure only authorized users can access the system.

- **Multifactor Authentication Protocol for all Voters**

Hoosiers utilize IndianaVoters.com to register to vote, update their voter information, find their polling location and much more. The state is investing in security at all levels by implementing validation requirements to enhance security for public online access of voter registration information on indianavoters.com, if the voter chooses to do so.

- **Voter Verifiable Paper Audit Trail**

A voter verifiable paper audit trail (VVPAT) is a security measure that allows voters to independently verify their vote was correctly recorded. Further, Indiana law allows for county election boards to select the voting equipment used in their counties, as long as those systems are certified for use in Indiana. Currently, state law allows for the use of an optical scan ballot card system (OpScan) or direct record electronic system (DRE).

OpScan voting systems employ a voter verifiable paper audit trail (VVPAT) by nature of its design – using ballot card marked by the voter or a ballot marking device that is then tabulated by an optical scan component. All DRE systems must contain a VVPAT component not later than December 31, 2019. The bi-partisan Indiana Election Commission has certified a VVPAT component for use on one vendor's voting system, and currently awaits applications from other DRE vendors. During the 2019 Municipal General Election, four counties piloted the VVPAT attachments to provide voters with a paper trail. The pilot was a success and more counties will be adding paper trails in 2020. By 2030, all counties must use a voting system – DRE and OpScan – that has a voter verifiable paper trail.

- **Penetration Testing**

Penetration testing, also called ethical hacking, is a practice of testing a computer system, network, or web applications to find security vulnerabilities that could be exploited. The State periodically conducts penetration testing to identify potential security vulnerabilities. Once vulnerabilities have been identified steps will be taken to address identified security vulnerabilities and strengthen the security of the Indiana elections infrastructure.

- **Cloudflare**

Distributed denial of service attacks known as DDOS attacks are used to take down websites. To prevent this, the State has implemented a distributed denial of service content filter called Cloudflare to protect indianavoters.com.

- **Cyber Best Practice Training**

Each year the Voting System Technical Oversight Program (VSTOP) team provides Indiana counties with best practices for the operation of election equipment and cybersecurity. Best practices are updated each year as cyber threats evolve and the election landscape changes.

- **Risk Limiting Audits**

A risk limiting audit or RLA is a post-election audit of ballots. A RLA requires manually reviewing a sample of ballot cards of a VVPAT component to a DRE to ensure election results are interpreted and tallied correctly.

- **Security Protocol**

State law establishes physical security standards for election equipment. Many county election boards adopt customized security resolutions above and beyond what is required by law.

It's also important to know that no piece of Indiana's voting equipment is online. The machines and tabulators are not connected to the internet. Public tests of voting systems are conducted in all counties prior to an election, and are open to the public. If you would like to attend, contact your county administrators for times and locations.

We take the security of our elections process very seriously and are working diligently to ensure that every available defense is utilized. Indiana has taken many steps to secure our elections, but let's be clear: there will always be new recommendations, new technology, and new best practices where cybersecurity is concerned. The way we administer elections must continue to evolve, because this is a race without a finish line. We are fully committed to ensuring that we continue to move forward, using every tool at our disposal to maintain safe and secure voting for all Hoosiers.

### **How to Report a Problem at the Polls**

Call 1-866-IN-1-VOTE (1-866-461-8683) or email [havaadministrator@sos.in.gov](mailto:havaadministrator@sos.in.gov).

Scroll for more options.



## ACCESSIBILITY

### Site Contrast

✓ **DEFAULT**

**DARK**

BrowseAloud Text Reader

Adobe Acrobat Reader

IndianaVoters.com has been built with the accessibility of all people in mind. It was checked against best practices and standards as defined by Section 508 of the U.S. Rehabilitation Act and the Web Content Accessibility Guidelines, WCAG 2.0, of the World Wide Web Consortium Web Accessibility Initiative and all pages under the domain of IndianaVoters.com meets AAA WCAG criteria.

This includes:

- Skip links, landmarks, and headings are defined to aid in navigation.
- Alternative text details (ALT tags) for appropriate images and other non-text elements.
- Additional markup is used where appropriate to indicate various page elements and other media.
- Form labels are programmatically associated with form fields.
- JavaScript and style sheets are used to enhance the appearance and functionality of the site. Care and caution has been used to ensure contrast and resolution remain high across devices, and that if these elements are unavailable to users, that the site degrades gracefully with minimal negative impact on user experience.
- Embedded documents and media have been made accessible to whatever extent possible.
- Higher contrast toggle option to view IndianaVoters.com pages.

If you are having issues with a part of our site, or are unable access specific content or functions, please call us at 800-622-4941 (toll free in Indiana) or share your concern by emailing at [elections@iec.in.gov](mailto:elections@iec.in.gov).





Indiana Election Registration Turnout VS Eligible Voting Population																					
Year	Election Type	*Pop of Indiana	Pop Under 18 Census shows 22.3%	Pop of Voting Age Census shows 77.7%	Number of Registered Voters	Vote Age Pop vs Registered	Total Voters Voting	Percent of Participation	"In Person" Votes	Percentage of "In Person" Votes	"Absentee/Mail" Votes	Percentage of "Absentee/Mail" Votes	Number of Residents who participated in Census Ineligible: VISA, Foreign, Incarcerated, Died Within 30 days before or after of Election, Turned 18 within 30 days After Election, Moved within 30 days before after Election		Voting Age Pop minus % Migrant Est (Census Data )	Percent of Voting Age Pop Minus Ineligible Voters	Difference of Voting Age Pop / Migrant Voter Est.				
													Migrants	Incarcerated	Died 30 days before	Turned 18 After Election	Moved/ Registered elsewhere				
1990	Primary General	5555097	1238787	4316310	2764768	64%	1567532	57%	1477927	94%	89605	6%	199983	3.60%	UNKNOWN/UNREPORTED DATA AS PER THE STATE OF INDIANA AND SHOULD HAVE BEEN UPDATED IN THE VOTER ROLL			4116327	95.4%	199983	
1992	Primary General	5,648,649	1259649	4389000	3180157	72%	2347912	74%	2182694	93%	165218	7%	203351	3.60%				4185649	95.4%	203351	
1994	Primary General	5,745,626	1281275	4464351	2976255	67%	1610082	54%	1499688	93%	106154	7%	206843	3.60%				4257509	95.4%	206843	
1996	Primary General	5,834,908	1301184	4533724	3488088	77%	2195224	63%	2031595	93%	162068	7%	210057	3.60%				4323667	95.4%	210057	
1998	Primary	5,907,617	1317399	4590218	3939103	86%	861560	22%	804174	93%	57023	7%	212674	3.60%				4377544	95.4%	212674	
2000	Primary General	5,942,901	1325267	4617634	3994910	87%	2232851	56%	2027746	91%	188019	8%	213944	3.60%				4403690	95.4%	213944	
2002	Primary General	6,155,967	1372781	4783186	3939103	82%	861560	22%	804174	93%	57023	7%	221615	3.60%				4561572	95.4%	221615	
2004	Primary General	6,233,007	1389961	4843046	4,162,606	86%	887592	21%	831017	94%	56521	6%	224388	3.60%				4618658	95.4%	224388	
2006	General				MISSING GENERAL ELECTION DATA FROM INDIANA ELECTION DIVISION																
2008	Primary	6,424,806	1432732	4992074	4,162,606	83%	887592	21%	831017	94%	56521	6%	231293	3.60%				4760781	95.4%	231293	
(2-conflicting 2008 General Election	General	6,424,806	1432732	4992074	4514759	90%	2805986	62%	2143813	76%	662443	24%	231293	3.60%			4760781	95.4%	231293		
	GENERAL	6,424,806	1432732	4992074	4514804	90%	2805374	62%	2143831	76%	662443	24%	231293	3.60%			4760781	95.4%	231293		
2002-2008														MISSING AND/OR CONFLICTING GENERAL ELECTION DATA FROM INDIANA ELECTION DIVISION							
2010	Primary	6,490,555	1447394	5043161	4277762	85%	892403	21%	797718	89%	94673	11%	233660	3.60%			4809501	95.4%	233660		
2011	General	6,490,555	1447394	5043161	4329153	86%	1786213	41%	1528293	86%	258320	14%	233660	3.60%			4809501	95.4%	233660		
2012	Primary	6,538,989	1458195	5080794	4409890	87%	957510	22%	837871	88%	119639	12%	235404	3.60%			4845391	95.4%	235404		
	General	6,538,989	1458195	5080794	4555257	90%	2663368	58%	2072974	78%	590445	22%	235404	3.60%			4845391	95.4%	235404		
2014	Primary	6,596,019	1470912	5125107	4571744	89%	617156	13%	518168	84%	98969	16%	237457	3.60%			4887650	95.4%	237457		
	General	6,596,019	1470912	5125107	4593222	90%	1388965	30%	1163054	84%	228932	16%	237457	3.60%			4887650	95.4%	237457		
2016	Primary	6,637,898	1480251	5157647	4715292	91%	1771753	38%	1489365	84%	282288	16%	238964	3.60%			4918682	95.4%	238964		
	General	6,637,898	1480251	5157647	4829243	94%	2807676	58%	1873281	67%	934403	33%	238964	3.60%			4918682	95.4%	238964		
2018	Primary	6,698,481	1493761	5204720	4406549	85%	861767	20%	690841	80%	171926	20%	241145	3.60%			4963574	95.4%	241145		
	General	6,698,481	1493761	5204720	4526663	87%	2308258	51%	1560152	68%	748106	32%	241145	3.60%			4963574	95.4%	241145		
2019	Primary	6,732,219	1501285	5230934	2647099	51%	345620	13%	265989	77%	79631	23%	242360	3.60%			4988574	95.4%	242360		
	General	6,732,219	1501285	5230934	2851245	55%	645458	23%	491940	76%	153518	24%	242360	3.60%			4988574	95.4%	242360		
2020	Primary	6,732,219	1501285	5230934	4585024	88%	1084558	24%	531392	49%	553166	51%	242360	3.60%			4988574	95.4%	242360		
	General	6,732,219	1501285	5230934	4751370	91%	3068625	65%	1201003	39%	1867577	61%	242360	3.60%			4988574	95.4%	242360		
Difference between 1990 to 2020		17.5%	17.5%	17.5%	41.8%	29.5%	48.9%	12.2%	-23.1%	-140.9%	95.2%	90.6%	*ineligible migrants	*est by Census 3.6% migrants				17.5%	0.0%	17.5%	
Average Change over 16 Elections		6242185	1392007	4850178	3962244	81%	1877429	47%	1480845	82%	395336	18%	224719	3.60%				4625459	95%	224719	
(these estimates are only from Migrants who participated in the Census as per the Indiana Census website)																(only subtracting 3.6% migrant est per Indiana Census and Clark Co Growth Reports)					

All data derived from Indiana Census, Secretary of State's and Clark County websites  
\*Population of Clark County Numbers are from Indiana Census (2010 & 2020) and Clark County Reports of annual population growth  
\*Percentage Difference from 1990 to 2020 as per the Indiana Census, Secretary of States and Clark County reports

This example puts into question the potential Algorithms used on reported numbers with a failure of clean Voter Rolls since 2008

<sup>1</sup> The April 1, 2000 Population Estimates base reflects changes to the Census 2000 population from the Count Question Resolution program,  
<sup>2</sup> The data source for April 1, 2010 is the 2010 Census count.  
<sup>3</sup> The values for July 1, 2010 were produced by applying estimates of change in the population between April 1 and July 1 of 2010 to the 2010 Census counts. Further details on this methodology are available at [http://www.census.gov/popest/methodology/intercensal\\_nat\\_meth.pdf](http://www.census.gov/popest/methodology/intercensal_nat_meth.pdf).  
Note: All geographic boundaries for the 2000-2010 intercensal estimates are defined as of January 1, 2010.

Source: U.S. Census Bureau, Population Division  
Release Date: September 2011

Clark County Election Registration Turnout VS Eligible Voting Population																				
Year	Election Type	*Pop of Clark Co.	Pop Under 18 Census shows 22.3%	Pop of Voting Age Census shows 77.7%	Number of Registered Voters	Vote Age Pop vs Registered	Total Voters Voting	Percent of Participation	"In Person" Votes	Percentage of "In Person" Votes	"Absentee/Mail" Votes	Percentage of "Absentee/Mail" Votes	Number of Residents who participated in Census Ineligible: VISA, Foreign, Incarcerated, Died Within 30 days before or after of Election, Turned 18 within 30 days After Election, Moved within 30 days before after Election				Voting Age Pop minus % Migrant Est (Census Data )	Percent of Voting Age Pop Minus Ineligible Voters	Difference of Voting Age Pop / Migrant Voter Est.	
													Migrants	Incarcerated	Died 30 days before	Turned 18 After Election	Moved/ Registered elsewhere			
1990	Primary												0							
	General	87,703	19558	68145	39120	57%	19841	51%	19079	96%	762	4%	3157	3.60%				64988	95.4%	3157
1992	Primary												0							
	General	89,278	19909	69369	50144	72%	36691	73%	34409	94%	2282	6%	3214	3.60%				66155	95.4%	3214
1994	Primary												0							
	General	90,654	20216	70438	57583	82%	36295	63%	33814	93%	2481	7%	3264	3.60%				67175	95.4%	3264
1996	Primary												0							
	General	92,358	20596	71762	57583	80%	36295	63%	33814	93%	2481	7%	3325	3.60%				68437	95.4%	3325
1998	Primary												0							
	General	93,991	20960	73031	62431	85%	26852	43%	unreported	unreported	unreported	unreported	3384	3.60%				69647	95.4%	3384
2000	Primary												0							
	General	96,446	21507	74939	68760	92%	37894	55%	34826	92%	3068	8%	3472	3.60%				71466	95.4%	3472
2002	Primary	97,935	21840	76095	68,942	91%	10457	15%	9756	93%	701	7%	3526	3.60%				72570	95.4%	3526
2004	Primary	100435	22397	78038	65388	84%	15512	24%	14019	90%	1493	10%	3616	3.60%				74422	95.4%	3616
	General	100,435	22397	78038	83698	107%	33535	40%	30018	90%	3517	10%	3616	3.60%				74422	95.4%	3616
2008	General	107,406	23952	83454	80,521	96%	55958	69%	48479	87%	7479	13%	3867	3.60%				79588	95.4%	3867
2010	Primary	110,232	24582	85650	82525	96%	16388	20%	14931	91%	1457	9%	3968	3.60%				81682	95.4%	3968
	General	110,232	24582	85650	83698	98%	33535	40%	30018	90%	3517	10%	3968	3.60%				81682	95.4%	3968
2012	Primary	111,879	24949	86930	86456	99%	13001	15%	11944	92%	1057	8%	4028	3.60%				82902	95.4%	4028
	General	111,879	24949	86930	88632	102%	47867	54%	41144	86%	6723	14%	4028	3.60%				82902	95.4%	4028
2014	Primary	114,082	25440	88642	87014	98%	11651	13%	10477	90%	1174	10%	4107	3.60%				84535	95.4%	4107
	General	114,082	25440	88642	88601	100%	31228	35%	27173	87%	4055	13%	4107	3.60%				84535	95.4%	4107
2016	Primary	115,660	25792	89868	92182	103%	29757	32%	27599	93%	2158	7%	4164	3.60%				85704	95.4%	4164
	General	115,660	25792	89868	94446	105%	52204	55%	42620	82%	9584	18%	4164	3.60%				85704	95.4%	4164
2018	Primary	117,287	26155	91132	87121	96%	13991	16%	12627	90%	1364	10%	4222	3.60%				86910	95.4%	4222
	General	117,287	26155	91132	89470	98%	49383	55%	40678	82%	8705	18%	4222	3.60%				86910	95.4%	4222
2019	Primary	118,191	26357	91834	66846	73%	8709	13%	8100	93%	609	7%	4255	3.60%				87580	95.4%	4255
	General	118,191	26357	91834	67870	74%	20365	30%	17079	84%	3286	16%	4255	3.60%				87580	95.4%	4255
2020	Primary	121093	27004	94089	91624	97%	21610	24%	13856	64%	7754	36%	4359	3.60%				89730	95.4%	4359
	General	121093	27004	94089	94856	101%	58298	61%	29632	51%	28666	49%	4359	3.60%				89730	95.4%	4359
Change from 1990 to 2020		27.6%	27.6%	27.6%	58.8%	43.1%	66.0%	17.5%	35.6%	-89.2%	97.3%	92.2%	*ineligible migrants	*est by Census 3.6% migrants				27.6%	0.0%	27.6%
Average Change over 16 Elections		104039	23201	80839	73522	90%	36669	50%	31503	87%	5820	13%	4121	3.60%				84829	95%	4121

All data derived from Indiana Census, Secretary of State's and Clark County websites

\*Population of Clark County Numbers are from Indiana Census (2010 & 2020) and Clark County Reports of annual population growth

\*Percentage Difference from 2010 to 2020 as per the Indiana Census, Secretary of States and Clark County reports

\*\*Over 100% of Voting Age Population as Registered Voters

(these estimates are only from Migrants who participated in the Census as per the Indiana Census website)

(only subtracting 3.6% migrant est per Indiana Census and Clark Co Growth Reports)

This example puts into question the potential Algorithms used on reported numbers with a failure of clean Voter Rolls.

\*Population of Clark County beyond 2010 and 2020 Census

<sup>1</sup> The April 1, 2000 Population Estimates base reflects changes to the Census 2000 population from the Count Question Resolution program,

<sup>2</sup> The data source for April 1, 2010 is the 2010 Census count.

<sup>3</sup> The values for July 1, 2010 were produced by applying estimates of change in the population between April 1 and July 1 of 2010 to the 2010 Census counts. Further details on this methodology are available at [http://www.census.gov/popest/methodology/intercensal\\_nat\\_meth.pdf](http://www.census.gov/popest/methodology/intercensal_nat_meth.pdf).

Note: All geographic boundaries for the 2000-2010 intercensal estimates are defined as of January 1, 2010.

Source: U.S. Census Bureau, Population Division

Release Date: September 2011

## Indiana Election Statistics

The following information and statistics Cited by [www.state.in.us/sos/election/iec](http://www.state.in.us/sos/election/iec), <http://clerkweb.house.gov/elections/elections.htm> , in some cases utilizing the Way Back Machine as the current Secretary of State's website fails to provide all data today.

Between 1964 and 1996, prior to electronic voting systems the average participation in elections through the paper ballot and paper pollbook was **73% of Registered Voters**. Indicating the confidence in the election system was substantially higher than it is today with only 58% participation in 2016 and 65% in 2020, even with the increase in population, percentages tell a story.

In less than 20 years of the Elections Participation and Confidence in the Indiana Electronic Election Systems declined by an average of 15%, however the Absentee Votes increased by 54%.

A severe distrust with the government, elected officials, election system companies and lobbyist. The electronic systems fail to provide the necessary information for Audits, as even today there are still 52 counties in Indiana without Paper Trails.

Whereas, paper ballots and paper Poll Books ensure a Paper Trail for audits and are recyclable after 5 years. Paper ballots and Paper Poll Books ensured privacy, free and fair elections.

**In 1980**, Voters cast their votes using the Paper Ballots and Paper Poll Books. While the number of Registered Voters was not recorded, the total number of **Ballots cast was 2,242,033**

**In 1984**, Voters cast their votes using the Paper Ballots and Paper Poll Books. While the number of Registered Voters was not recorded, the total number of **Ballots cast was 2,233,069**.

**In 1988**, Voters cast their votes using the Paper Ballots and Paper Poll Books. While the number of Registered Voters was not recorded, the total number of **Ballots cast was 2,168,621**.

**In 1990**, 73% of Registered Voters cast their vote into the Paper Ballot, Paper Pollbook voting system. Only 5.7% of the voters were Absentee Ballots.

Registered 2,764,768 **Ballots Cast 1,567,532** /56.7% Participation  
Vote at Poll 1,477,927 Absentee Vote 89,605 /5.7%

**In 1992**, 73% of Registered Voters cast their vote into the Paper Ballot, Paper Pollbook voting system. Only 7% of the votes were Absentee Ballots.

Registered 3,180,157 **Ballots Cast 2,347,912** /73.8% Participation  
Vote at Poll 2,182,694 Absentee Vote 165,218/7.0%

**In 1994**, 54% of Registered Voters cast their vote into the Paper Ballot, Paper Pollbook voting system.  
Only 6% of the votes were Absentee Ballots

**In 1996** 62% of Registered Voters cast their vote into the Paper Ballot, Paper Pollbook voting system.  
Only 7.3% of the votes were Absentee Ballots

Registered 3,488,088      **Ballots Cast 2,195,224** /62.93% Participation  
Vote at Poll 2,031,595      Absentee Vote 162,068/7.3%  
*HOWEVER: According to the STATISTICS OF THE PRESIDENTIAL AND  
CONGRESSIONAL ELECTION OF NOVEMBER 7, 2000 a total of Indiana Ballots  
cast was 2,199,302  
\*According the records the Vote at Poll plus the Absentee Vote (2,193,663)  
did not equal the Total Ballots cast (2,195,224) leaving out 1561 votes?*

**In 2000**, 56% of Registered Voters cast their vote according to the Secretary of State website, however the website did not disclose the same data sets from all previous elections. It wasn't until 2006 the data updated to a spreadsheet that mirrored previous Voter Turnout statistics.

In 2006, the **2000 Election data** from the Secretary of State's website was updated and reflected the following:

Registered 3,994,910      **Ballots Cast 2,232,851** /55% Participation  
Vote at Poll 2027746      Absentee Vote 188019 /8%

*In 2002 the data from the Secretary of State's website reflected the following Vote total snapshot:*

*Total Presidential Votes Cast 2,180,305  
Total Governor Votes Cast 2,179,268  
Total US Senator Votes Cast 2,145,209  
Total House Representative Votes Cast 2,156,743  
Total Attorney General Votes Cast 2,102,164*

**In 2004**, only 58% of Registered Voters chose to cast their vote with only 9% of the voters casting Absentee Ballots.

Registered 4,294,196      **Ballots Cast 2,511,319/** 58% Participation  
Vote at Poll 1,892,237      Absentee Votes 215,372 /9%

*In \*2006 the Secretary of State's website showed different election results from the 2004 Election  
Registered 4,296,602      Ballots Cast 2,512,142 / 58 % Participation  
Vote at Poll 2,251,193      Absentee Votes 260,550 /10%*

**In 2008**, 62% of Registered Voters chose to cast their votes, however in 2008 a record increase in **Absentee Ballots jumped to a whopping 24% from the previous decades average of less than 10%.**

Registered 4,514,804      **Ballots Cast 2,805,986** / 62% Participation  
Vote at Poll 2,143,813      **Absentee Votes 662,443 /24%**

**In 2012**, only 58% of Registered Voters chose to cast their votes. The use of Absentee ballots lowered by only 2%, however still remained high at 22%

Registered 4,555,257      **Ballots Cast 2,663,368** / 58% Participation  
Vote at Poll 2,072,974      **Absentee Vote 590,445 /22%**

**In 2016**, only 58% of registered voters chose to cast their vote into the electronic voting system. However the Absentee Votes in less than 10 years went from 10% in 2006 to a whopping 33% in 2016.

Registered 4,829,243      **Ballots Cast 2,807,676** /58 % Participation  
Vote at Poll 1,873,281      **Absentee Vote 934,403 / 33%**

**In 2020**, participation grew to 65% although still not at the levels prior to the digital age, with less Registered voters, in 2020 the most Ballots cast in History. However, with the fear propagated onto the public with Covid 19 concerns, the Absentee Votes nearly doubled to a staggering 61%.

Registered 4,751,370      **Ballot Cast 3,068,625** /65% Participation  
Vote at Poll 1,201,033      **Absentee Vote 1,867,577 /61%**



**An Investigation of Issues Regarding  
Election Systems & Software, LLC Electronic Poll Books  
Used During the 2018 Primary and General Elections**

**Conducted by  
The Voting System Technical Oversight Program (VSTOP)**

**April 10, 2019**



## **Executive Summary**

The Indiana Voting System Technical Oversight Program (VSTOP) conducted an investigation of issues related to a significant increase in voter check-in times in Johnson County, Indiana during the General Election on November 6, 2018. A preliminary report based on the investigation, was submitted to Secretary Lawson on December 31, 2018. During the investigation it was discovered that there were electronic poll book (ePB) malfunctions and problems in several Indiana counties using ES&S ePBs during both the Primary Election in May 2018 and the General Election in November 2018. Secretary Lawson asked VSTOP to carry out a comprehensive investigation of these issues.

This comprehensive report describes the follow-up investigation of ePB problems in ES&S counties in Indiana. This report incorporates by reference the preliminary report submitted to Secretary Lawson on December 31, 2018. See Appendix A for a copy of this preliminary report.

ES&S's ePB problems during the 2018 Primary and General Elections included delays with voter check-ins, which was caused by slow access and response times through the Microsoft Azure Web Application Firewall (WAF). A WAF is a feature of an Application Gateway that provides centralized protection to Web Applications. It has configuration rules to allow, block and monitor the requests based on customizable rules and definitions. WAF was not properly scaled out due to the configuration chosen by ES&S personnel. As a result, this limited the number of WAF instances available caused serious widespread problems. There were additional problems with ePB bases and related connectivity issues.

VSTOP conducted interviews with ES&S and with eight ES&S counties. VSTOP also conducted a technical analysis of server and client transaction logs provided by ES&S.

This report includes VSTOP's findings and recommendations based on the follow-up investigation. The findings of the preliminary report are also included as summaries.

VSTOP's findings include the extent of the November 2018 Election Day problems and their impact, analysis of the technical logs that explain the slow check-in times, problems with retention of logs, issues with filing of anomaly reports, inability to replicate errors, and lack of contingency planning.

VSTOP's recommendations include suggestions for a review of ES&S's internal quality control processes, failsafe methods to prevent recurrence of problems, a review of anomaly reporting processes, and communication protocols to ensure technical support to ES&S's customers.





## Introduction

VSTOP conducted an investigation of issues related to a significant increase in voter check-in times in Johnson County during the General Election on November 6, 2018. A preliminary report based on the investigation was submitted to Secretary Lawson on December 31, 2018. During the investigation, it was discovered that there were ePB malfunctions and problems in several other Indiana counties using ES&S during both the Primary Election in May 2018 and the General Election in November 2018. Secretary Lawson asked VSTOP to carry out a comprehensive investigation of these issues.

ES&S's ePB problems during the 2018 Primary and General Elections included delays with voter check-ins, which was caused by slow access and response times through the Web Application Firewall (WAF). WAF was not properly scaled out due to the configuration chosen by ES&S personnel. As a result, this limited the number of WAF *instances*<sup>1</sup> available caused serious widespread problems. There were additional problems with ePB bases and related connectivity issues.

VSTOP conducted interviews with ES&S and with eight ES&S counties. VSTOP also conducted a technical analysis of server and client transaction logs provided by ES&S.

This report includes VSTOP's findings and recommendations based on the follow-up investigation.

## Scope of the Comprehensive Investigation

The comprehensive investigation included the following activities:

- a. Conducting further interviews and gathering information from ES&S and the involved counties;
- b. Contracting with a technical expert to assist with the investigation;
- c. Conducting reviews of responses from ES&S and the involved counties;
- d. Reviewing and analyzing logs submitted by ES&S;
- e. Reviewing documentation;
- f. Drawing conclusions regarding the findings and engaging in a risk management assessment to advise ES&S and the Secretary of potential ways to avoid such problems in the future; and
- g. Providing recommendations related to these issues.

## ES&S Electronic Poll Book Systems Used in Indiana

---

<sup>1</sup> An "instance" is a resource (virtual server) that validates the https or http request from the client. For more information, please visit <https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview>



In 2018, ES&S's ePBs were used in the following eight Indiana counties: Brown, Carroll, Elkhart, Hancock, Howard, Johnson, Monroe, and Porter.

All ES&S ePB counties in Indiana used the EZRoster 3.2.2.1 in the 2018 elections. For a complete description of the components, please see the preliminary report (Appendix A).

### **Timeline of Events**

#### **2018:**

For a timeline of events in 2018, please see the preliminary report (Appendix A).

Additionally, on December 27, 2018, VSTOP sent a second email to Elkhart County asking for a description of ePB issues. At the same time, VSTOP began preparing follow-up questions for ES&S.

#### **2019:**

January 3: Stephen Berger (VSTOP Technical Consultant) compiled a list of potential problems uncovered in the investigation, as described in the preliminary report.

January 22: ES&S filed anomaly reports for Brown, Elkhart, and Hancock Counties (see Appendix B)

February 7: VSTOP communicated with Ms. Kathy Rogers, ES&S Senior Vice President of Government Affairs, to discuss progress on ES&S's internal research and follow-up questions.

February 8: VSTOP sent the third set of questions to ES&S (see Appendix C).

February 14: VSTOP sent a third email to Elkhart County asking for a description of ePB problems. VSTOP spoke on the phone with Ms. Carol Smith in the Elkhart County Clerk's office. VSTOP received an email with responses from Elkhart County Circuit Court Clerk Christopher Anderson.

February 15: VSTOP received responses to the third set of questions from ES&S.

February 18: ES&S uploaded county client log files to a secure Ball State University box account.

February 21: VSTOP sent a set of fourth set questions to ES&S.

February 25: After an analysis of client logs from counties, VSTOP sent a fifth set of questions to ES&S and requested a phone call with ES&S; VSTOP received responses from Johnson and Monroe Counties.



February 26: VSTOP received responses to questions about the client logs from ES&S.

February 27: VSTOP called ES&S to seek further clarification on the client logs.

February 28: VSTOP submitted a draft report to Secretary Lawson.

March 6: VSTOP received written responses from ES&S following the February 27<sup>th</sup> phone call.

### **Description of the Issues**

Based on reports, the following issues occurred in the May 8, 2018 Primary Election, the November 6, 2018 General Election, or both:

- a. Delays in checking-in voters significantly impacted the 2018 General Election.
- b. Although ES&S had performed system load testing, the methods ES&S used failed to predict the problems experienced. Since the election, ES&S has been unable to reproduce the problems through simulations or additional testing.
- c. Similar issues were experienced during the 2018 Primary Election, but they were not effectively documented and the potential for these problems to become much worse in the General Election went unrecognized.
- d. Johnson County experienced significantly longer access and response times through the Microsoft Azure WAF. These delays continued for several hours.
- e. Some county election administrators reported that they were unable to receive information and responses from ES&S, even as delays became more significant.
- f. ES&S had no immediate contingency plan for the problems that manifested. This resulted in counties using different work-arounds, some of which were ineffective and not compliant with Indiana law.
- g. There was a failure of communication and coordination among those involved. This resulted in county election administrators wasting time and effort duplicating unsuccessful workarounds.
- h. The WAF was not and could not be scaled sufficiently to meet demands due to the limited capacity contracted for by ES&S on Election Day. Their contract did not allow for rapid response to meet voter demands on Election Day and as a result impeded access to voters at the polls.
- i. Many voters in Indiana counties using this ES&S equipment on Election Day were affected by the malfunctions. The ES&S ePB in Indiana uses two components: CentralPoint (a web application) and SyncPoint (a web service). ES&S refers to the combination of CentralPoint and SyncPoint as “CentralPoint.”
- j. There were problems with ePB bases and related connectivity issues.

### **ES&S’s Responses to Questions**



During February of 2019, ES&S and VSTOP had numerous discussions regarding the matters addressed in this preliminary report. The following is a summary of the responses from ES&S to questions from VSTOP, regarding these topics:

Retention of Logs: ES&S stated that their WAF and firewall logs were not retained due to a configuration problem. In other words, the configuration did not appear to have been properly set. This is a point of serious concern. Logs are “election materials”, for which retention requirements are governed by Indiana and federal law. It is the position of ES&S that they did not have the understanding that logs were election materials, and therefore did not provide for retention of those records. In the ‘recommendations’ section in the latter part of this report, VSTOP recommends appropriate corrective actions for ES&S to come into compliance for proper retention with Indiana law.

Reporting of Issues and Anomalies: Johnson County reported an issue during the May 2018 Primary Election, which was similar to the check-in delays that occurred later during the November 2018 General Election. Johnson County confirmed the occurrence of this issue in correspondence to VSTOP on February 26<sup>th</sup>. Johnson County also stated that it reported the issue to ES&S’s local staff. In their response to Question 3-5, ES&S stated “...it is possible that site support personnel may have been notified of an issue, we cannot provide a copy of any communication for this reason.” This raises a concern about ES&S’s reporting practices and procedures and a potential noncompliance with Indiana’s anomaly reporting requirements.

Additionally, Porter County and Brown County reported problems with ePB stands that arose during the Primary Election. In response to Question 3-8, Item #3, “ES&S was made aware of the stand [the stand is the base on which the ePB is mounted] issues that occurred during the Primary Election. As stated above, after the Primary Election, Brown County’s stands were sent back to our Omaha facility for testing and repair.” VSTOP has no record that ES&S filed anomaly reports regarding this problem, as required by Indiana law.

ES&S’s Internal Research Procedure on Replication/Reproducing Errors: During the call on Friday, December 21, 2018, ES&S staff mentioned that they were conducting internal research on the status code 500 internal server issues. This was also mentioned in ES&S’s response to Questions 2-13. In the preliminary report, it was stated “VSTOP expects that ES&S will share the results of its research with the State as soon as those are available.” In response to Questions 3-6, ES&S stated “ES&S has not been able to reproduce the 500 internal server issue encountered and research to date has not indicated why the 500 internal server issue was indicated in the log file. ES&S continues to monitor for any application exceptions as a result of it, but currently there is no clear indicator of the cause of the message.” During the call on February 27<sup>th</sup>, ES&S stated that the HTTP Status Code 500 issues might be caused by validating the client certificate from Azure Certificate Revocation List (CRL). In the response received on March 6<sup>th</sup>, ES&S stated “The reason [for the 500 internal server issue] was due to the server making a call to another TLS [Transport Layer Security] secured service and not being able to completely negotiate the secure channel.” This does not strengthen VSTOP’s confidence that such complications can be avoided in the future.



ES&S's Replication/Reproducing of Performance Issues: In response to Questions 3-7, ES&S stated "ES&S has not been able to reproduce or replicate the performance issue related to the web application firewall issue that occurred in the General Election. ES&S has made several changes to allow for further diagnostics and logs to be collected if issues arise in the future. In addition, ES&S has also made configuration changes allowing for greater scalability without interruption, such as using the ability to scale up to more instances of the web application firewall instead of the previous limitation of 7." Without ES&S being able to replicate or reproduce the performance malfunctions, and without testing, VSTOP is concerned by ES&S's confidence that the stated configuration changes will resolve the problems. In a follow-up response, ES&S stated that the scaling up of WAF instances is an interim step and it will not be utilized long-term in ES&S's hosting environment. Without any testing data and other evidence, VSTOP remains skeptical that scaling up of WAF instances will completely avoid a recurrence of the glitches and malfunctions.

Change in ES&S's infrastructure and hosting environment: In response to Questions 3-9, ES&S stated, "After additional research of the issues and to further reduce its dependency on third parties, ES&S will be transitioning its e-poll book server infrastructure to ES&S' hosting environment. ES&S expects the transition will be completed in advance of the November 2019 Elections. Further notification will be provided to the State in subsequent communications by ES&S." VSTOP requested further information regarding ES&S's plans for testing, including load and performance testing of the server infrastructure before its expected use in November 2019. In response, ES&S stated, "Our load and performance test plan is similar to what was previously shared with VSTOP in prior communications. We are prepared to share the results of those tests when completed."

In the written response received on March 6<sup>th</sup> ES&S stated, "due to commitments to support its customers throughout the months of March, April, and May with scheduled elections, [we] will not be able to migrate off of the Azure environment until after the May 2019 Municipal Elections. Consequently, ES&S will continue to service Indiana ePB customers within the current Azure environment until after the May Municipal Elections." ES&S has also stated, "The issue experienced on Election Day was an unexplained slowdown in the performance of the Azure WAF component, and a configuration that did not allow scale-out of this component. This component is being removed from the ePB architecture and being replaced with equivalent technology that has been proven successful through numerous elections and daily use by ES&S customers." However, VSTOP's concerns regarding the replication of the problem with WAF instances remains the same.

Please see the 'findings' section below for VSTOP's findings based on its analysis of ES&S's responses.



## Responses from Counties

VSTOP contacted all eight ES&S counties in Indiana and sought descriptions of any issues with ePBs in the Primary or General Elections in 2018. Below are the responses by the counties.

### **Brown (Responses received December 27, 2018):**

*During the 2018 Primary, we had issues with the power supply on 3 pollbook bases. The bases were changed out and voting continued. I sent all the stands back to ES&S and they tested and corrected all the stands.*

*During the 2018 General, we did have issues with the poll books connecting to the internet. However, the Election Board informed the polling locations not to wait on the host, therefore, voting continued.*

### **Carroll (Responses received December 20, 2018):**

Question 1: On Election Day, November 6, 2018, did you encounter any delays with the check-in of voters at your voting locations that were related to electronic poll book performance? If yes, please explain in detail.

Response 1: *Yes, at times it took up to 5 mins to pull up a voter in the electronic poll book to check them in.*

Question 2: During Early Voting for the 2018 General Election, did you encounter delays with the check-in process related to electronic poll book performance? If yes, please explain in detail.

Response 2: *No*

Question 3: If the answer to either of the questions above is yes, please list all ES&S personnel by name who assisted with resolving this issue and how the problem or problems were resolved. Do you believe the ES&S personnel were appropriately trained to handle the issues? Were the problems resolved to your satisfaction?

Response 3: *The ES&S help desk, I did not log names, the first time I called I was told there were no issues, then I called Jeremy Burton and he contacted someone, eventually I was told that they were having this problem nationwide. The Secretary of State called and said that ES&S had a temporary solution and that I would be hearing from ES&S soon. I was called by ES&S and given steps to bypass Central Point, I had to call each vote center and walk them through the steps. About an hour or so later, they called back and said they had the problem fixed and that we need to reverse the steps on each poll book. I would not say that everyone I spoke with was trained to handle this situation, but my problem was solved, but my first issue happened around 8:00am and the problem was not fixed until early afternoon. This resulted in long lines for a good portion of the day.*





Question 4: Did you experience any similar issues in relation to your electronic poll books during the 2018 Primary period? If so, please explain in detail.

Response 4: *No*

**Elkhart (Responses received February 14, 2019):**

Question 1: On Election Day November 6, 2018, did you encounter any delays with the check in of voters at your voting locations that were related to electronic poll book performance? If yes, please explain in detail.

Response 1: *Elkhart County did experience a “slow down” in our E-poll book check-in process on Election Day, November 2018. We were never “shut down” in regard to processing voters! It did back up the check-in process, maybe adding, at max 30 minutes to process voters. It is very hard to say for sure due to the fact that it was a busier than usual election.*

Question 2: During Early Voting for the 2018 General Election, did you encounter delays with the check in process related to electronic poll book performance? If yes, please explain in detail.

Response 2: *We did not experience any type of problems or issues during early voting in the E-poll book process.*

Question 3: If the answer to either of the questions above is yes, please list all ES&S personnel by name who assisted with resolving this issue and how the problem or problems were resolved. Do you believe the ES&S personnel were appropriately trained to handle the issues? Were the problems resolved to your satisfaction?

Response 3: *Elkhart County were supplied with two very good technicians from ES & S. Between Kyle and Deepti from ES & S, and our own voter registration manager Chad Clingerman, they were more than qualified to deal with the “slow down” issues we experienced once we were made aware of them from our vote center staff.*

*We feel that things were handled in a professional manner and we were quite satisfied.*

Question 4: Did you experience any similar issues in relation to your electronic poll books during the 2018 Primary Period? If so, please explain in detail.

Response 4: *We did not experience any type of problems or issues during the 2018 Primary election season.*



**Hancock (Responses received December 14, 2018):**

Question 1: On Election Day November 6, 2018, did you encounter any delays with the check in of voters at your voting locations that were related to electronic poll book performance? If yes, please explain in detail.

Response 1: *Hancock County received a “host error” message on our poll books. We instructed poll workers to enter the Supervisor Password and to issue regular ballots – no real delay except to call the Inspectors and direct them to use the Supervisor Password so they could move on to issue the ballots*

Question 2: During Early Voting for the 2018 General Election, did you encounter delays with the check in process related to electronic poll book performance? If yes, please explain in detail.

Response 2: *No*

Question 3: If the answer to either of the questions above is yes, please list all ES&S personnel by name who assisted with resolving this issue and how the problem or problems were resolved. Do you believe the ES&S personnel were appropriately trained to handle the issues? Were the problems resolved to your satisfaction?

Response 3: *Susan Casey, Project Manager; Sara Mahon, Site Support. Yes, we called in a ticket to ES&S help Desk to alert them of the issue. Yes, system was back up and from what I could see running properly by around 1:30 or 2:00 (incident regarding Host Error occurred around 10:00 a.m. if I recall) The Host Error problem was only intermittent from 10 – until it came back up – some of our polling locations never experienced a problem at all. CentralPoint had a delay in showing a status report earlier in the day around 6:00 a.m. but looked alright by 7:00 a.m. a ticket for this issue was also submitted.*

Question 4: Did you experience any similar issues in relation to your electronic poll books during the 2018 Primary period? If so, please explain in detail.

Response 4: *I do not recall any Host Error problems with the Primary*

**Howard (Responses received December 27, 2018):**

Question 1: On Election Day November 6, 2018, did you encounter any delays with the check in of voters at your voting locations that were related to electronic poll book performance? If yes, please explain in detail.

Response 1: *Yes. It was an insignificant amount of time. It was a “wait” error. We could still issue ballots. No one was turned away. We just had to click on “host error, issue ballot” and retype the name of the voter.*





Question 2: During Early Voting for the 2018 General Election, did you encounter delays with the check in process related to electronic poll book performance? If yes, please explain in detail.

Response 2: *Same as issue as above. Only happened 2 different days.*

Question 3: If the answer to either of the questions above is yes, please list all ES&S personnel by name who assisted with resolving this issue and how the problem or problems were resolved. Do you believe the ES&S personnel were appropriately trained to handle the issues? Were the problems resolved to your satisfaction?

Response 3: *Mike Manna, Sarah Mahon. They thought they knew but made a phone call to main office to verify. They were correct*

Question 4: Did you experience any similar issues in relation to your electronic poll books during the 2018 Primary period? If so, please explain in detail.

Response 4: *During the Primary it happened at one poll location. It didn't last very long. The ESS team called the main office to verify and then educated us on how to handle.*

**Johnson:** See detailed responses in the preliminary report. Additional responses were received on February 26<sup>th</sup>.

In its initial set of questions to Johnson County, VSTOP asked the following:

Question 5: Were there similar issues encountered during the Primary Election period in 2018?

Johnson County's Response: *Yes. We had a similar (but not as severe) problem during the 2018 Primary Election. If memory serves, the delays were not quite as long, nor was it quite as widespread. So we are not sure if the issues in the Primary were also related to a problem with Microsoft Azure or something completely different. This was reported to ES&S at the time, but we never received an explanation for the underlying cause.*

VSTOP asked for more details on February 20, 2019 and received the following responses.

Question 6: Do you have more information about the nature of the problem and the delays that occurred during the Primary 2018 election?

Response: *The issue that occurred in the 2018 Primary Election was similar to the issue experienced in the 2018 General Election in that the electronic poll books at several locations were giving the yellow "Host Wait" messages. My recollection is that the delays to bring up the voters were between 5 and 10 seconds or so. The problem was not as widespread as it was in the 2018 General Election. I want to say that only a handful of sites (perhaps 5 or so) reported the slowdown.*



Do you have the name or names of the ES&S personnel to whom this problem was reported? On what date?

*Response: I made a call to ES&S on election day when the problem was actually occurring. Unfortunately I do not recall the name of the person I spoke to at that time. Our on-site project manager, Su Clark, recommended the person that I spoke with. Initially, this person said they did not think there was an issue on their end. Then, during a second phone call, they said they looked into it more deeply and found something that perhaps needed to change, and they supposedly made that change. I do not recall what they said they changed, but I know I had never heard of it before. At the time I was just pleased that they seemed to have found something. The problem eventually seemed to clear up after a couple hours. I do not know if it was the result of the change they made or something else entirely. I know we did not make any changes on our end to get it working better.*

*On June 20, 2018, our clerk at the time, Susie Misiniec, received an email from our ES&S Sales Manager, Jeremy Burton, in which he admitted that ES&S still did not know the cause of the connectivity problems on election day but that they were still researching it. It was admitted that it was known that the problem was not on Johnson County's end.*

**Monroe (Responses received February 25, 2019):**

Question 1: On Election Day November 6, 2018, did you encounter any delays with the check in of voters at your voting locations that were related to electronic poll book performance? If yes, please explain in detail.

*Response 1: We did have delays on Election Day. The poll worker would have to wait for the host errors from Central Point to go away. But it was possible to force it through. It slowed down our voting process. It continued all day and it was never fixed. To our knowledge, it still hasn't been fixed.*

Question 2: During Early Voting for the 2018 General Election, did you encounter delays with the check in process related to electronic poll book performance? If yes, please explain in detail.

*Response 2: Early Voting did not have delays.*

Question 3: If the answer to either of the questions above is yes, please list all ES&S personnel by name who assisted with resolving this issue and how the problem or problems were resolved. Do you believe the ES&S personnel were appropriately trained to handle the issues? Were the problems resolved to your satisfaction?

*Response 3: Susan Casey from ES&S was contacted. She knew the right person to contact within ES&S. Also our IT personnel contacted Central Point directly but does not know the name of that person.*



Question 4: Did you experience any similar issues in relation to your electronic poll books during the 2018 Primary period? If so, please explain in detail.

Response 4: *Yes, it was the same problem.*

**Porter:** See detailed responses in the preliminary report. In its responses Porter County had identified issues with the ePB bases and connectivity issues. In a February 22, 2019 response to a follow-up question from VSTOP, former Clerk Karen Martin explained that the connectivity issues were related to the issues with bases:

*“It is my understanding that most of the connectivity issues were due to the bases at the Portage and Chesterton locations. After the bases were exchanged the system seemed to function properly.*

*Although a majority of the issues were at the Portage location which also has internet issues.*

*Sorry I can't be more specific.”*

Please see the ‘findings’ section below for VSTOP’s findings from the county responses.



### Technical analysis of Client Logs provided by ES&S

The VSTOP team and Mr. Stephen Berger conducted a detailed investigation of the logs provided by ES&S. In the preliminary report, VSTOP provided a technical analysis of the Internet Information Services Server (IIS) logs. IIS is a web application server used for storing, processing, and serving web pages to a requesting client.

On February 18<sup>th</sup>, ES&S provided client logs (EZRoster Tablet Logs) to VSTOP, which contain logs of transactions occurring in the EZRoster Tablets. These logs provided November 2018 Election Day transactions of ePBs in seven counties (Brown, Carroll, Elkhart, Hancock, Howard, Johnson, and Monroe). Porter County used ePBs only for early voting.

Client transactions include time-stamps for each of the following: login and logout information, communication with the server, and power status. The communication transactions include ballot transactions and error transactions. A “ballot transaction” records an issuance of a ballot, that is, a successful check-in. An “error transaction” records errors, such as printer and network issues.

Using the time-stamp values provided with the transactions, VSTOP computed several parameters. Table 1 shows the total number of ballots issued and errors that occurred by hour in Indiana on Election Day. We observed that counties began having more errors at 8:00 AM.

**Table 1: Client Logs (EZRoster Tablet Logs)**

<b>Date/Start Time (1 Hour) (ET)</b>	<b>Client Logs (7 Indiana Counties)</b>	
	<b>Ballots Issued</b>	<b>Errors</b>
11/6/2018 6:00	11960	280
11/6/2018 7:00	11446	352
11/6/2018 8:00	10854	1098
11/6/2018 9:00	9858	2087
11/6/2018 10:00	9511	2876
11/6/2018 11:00	10074	3095
11/6/2018 12:00	9460	1401
11/6/2018 1:00	10360	1113
11/6/2018 2:00	10189	1273
11/6/2018 3:00	10580	7689
11/6/2018 4:00	11971	1024
11/6/2018 5:00	10506	873

Note: Only non-printer errors were included in VSTOP’s error calculations.

Table 2 shows “Ballots per Unit by Hour” and “Errors per Unit by Hour.” These are averages of overall units with over 2-hour or 4-hour periods in each county. The table shows that most counties experienced the most errors during the 10:00 AM to 12:00 PM time period. In comparison, Johnson County consistently had less errors than any other county until 2:00 PM. Despite fewer errors, Johnson County’s ballot rate was lower compared to other counties during



the 10:00 AM to 12:00 PM timeframe. Johnson County stated in the preliminary report that the workaround was approved by the County Election Board after 12:00 PM.

The number of errors per unit by hour was larger in Brown, Elkhart, and Howard Counties than in Johnson County. However, Brown, Elkhart, and Howard continued to have consistent volumes of ballot transactions. During the same time period, Johnson County's ballot rate decreased to about 12 ballots compared to rates of 35 and 34 ballots in the periods before and after. This confirms the slowdown in reported check-ins.

The error rate was high for Elkhart County during the 2:00 PM to 6:00 PM timeframe, but these issues were limited to eight of 133 units in operation on Election Day.

**Table 2: County Client Logs Hourly Information**

County	6:00 AM to 10:00 AM (ET)		10:00AM to 12:00 PM (ET)		12:00 PM to 2:00 PM (ET)		2:00 PM to 6:00 PM (ET)	
	Ballots per Unit by Hour	Errors per Unit by Hour	Ballots per Unit by Hour	Errors per Unit by Hour	Ballots per Unit by Hour	Errors per Unit by Hour	Ballots per Unit by Hour	Errors per Unit by Hour
Brown	27.20	1.08	28.47	14.43	20.13	2.67	21.10	0.05
Carroll	31.40	0.71	24.58	6.75	26.13	1.25	30.52	0.00
Elkhart	24.95	3.58	22.89	7.00	25.29	6.65	26.91	19.47
Hancock	29.20	1.07	26.93	5.70	20.58	1.20	25.37	0.15
Howard	42.32	8.64	44.27	38.07	46.09	3.77	46.32	0.03
Johnson	34.58	0.56	11.94	5.21	33.72	1.19	39.28	0.13
Monroe	28.23	0.99	27.40	6.44	20.39	0.92	22.15	0.41

Note: Only non-printer errors were included in VSTOP's error calculations.

Table 3 shows the average wait time (mm:ss) between ballot transactions per unit (overall units) for each hour on Election Day. To obtain the average wait time, the difference between timestamps from successive ballot transactions for each unit were calculated, then averaged for each hour. The average wait time by county drastically increased during the 10:00 AM to 12:00 PM timeframe for Johnson County (shown in bold).

In comparison with the Table 2 and 3, Howard County maintained average ballot issue rate even with the increased error rate (see Question 1 of Howard County's responses received December 27, 2018). Whereas, Johnson County retained the average ballot issue rate during 12:00 PM to 2:00 PM by following the workaround approved by the Johnson County Election Board.



**Table 3: Average wait time by County**

	<b>Average wait time between ballots by unit per County (mm:ss)</b>						
	<b>Brown</b>	<b>Carroll</b>	<b>Elkhart</b>	<b>Johnson</b>	<b>Hancock</b>	<b>Howard</b>	<b>Monroe</b>
<b>6 AM</b>	01:44	01:39	02:08	01:11	01:46	01:19	01:18
<b>7 AM</b>	01:58	01:55	02:06	01:15	02:04	01:19	01:22
<b>8 AM</b>	01:44	01:58	02:24	01:29	02:12	01:21	01:23
<b>9 AM</b>	02:01	02:10	02:49	01:52	02:21	01:26	01:26
<b>10 AM</b>	01:45	02:32	03:13	<b>03:48</b>	02:03	01:15	01:08
<b>11 AM</b>	01:43	02:24	02:03	<b>04:12</b>	02:33	01:32	01:16
<b>12 PM</b>	02:25	02:51	02:18	01:39	03:06	01:13	02:02
<b>1 PM</b>	02:39	01:54	02:18	01:15	02:55	01:09	01:50
<b>2 PM</b>	02:52	02:12	02:14	01:16	02:48	01:20	01:52
<b>3 PM</b>	02:30	01:58	02:05	01:15	02:30	01:22	01:49
<b>4 PM</b>	01:57	01:31	01:58	01:12	02:04	01:06	01:32
<b>5 PM</b>	02:17	02:07	01:59	01:11	02:09	01:09	02:12

Table 4 shows the number of requests made to the Microsoft IIS Server and the number of successfully processed requests. We observe that the server was a shared resource for all ES&S client jurisdictions in the U.S. Other ES&S client jurisdictions include Arizona, Arkansas, Illinois, Mississippi, and Texas where the polls opened later than in Indiana. The polls opened in these jurisdictions at the following times:

	<b>Eastern Time</b>	<b>Central Time</b>	<b>Mountain Time</b>	<b>Eastern Time</b>
<b>Indiana</b>	6:00 AM	6:00 AM		6:00 AM , 7:00 AM
<b>Illinois</b>		6:00 AM		7:00 AM
<b>Mississippi</b>		7:00 AM		8:00 AM
<b>Texas</b>		7:00 AM		8:00 AM
<b>Arizona</b>			6:00 AM	8:00 AM
<b>Arkansas</b>		7:30 AM		8:30 AM

Except for Porter County, the Indiana counties that reported problems are located in the Eastern Time zone. The opening of additional polls for voting in these states is reflected in the increase in the number of requests from Indiana between 6:00 AM to 9:00 AM, which was particularly noticeable beginning at 8:00 AM eastern time.

However, during the 9:00 AM to 1:00 PM eastern timeframe, the server was not receiving all the client requests. This may be related to the reported delay in check-in times. This highlights the significance of WAF logs which are not available. Later in the day, the number of requests appeared to stabilize.



**Table 4: Server Logs (IIS Logs)**

	Server Logs	
<b>Date/Start Time (1 Hour) (ET)</b>	<b>Total Number of Requests Per Hour</b>	<b>Successfully Processed Requests (HTTP Status Code 200)</b>
11/6/2018 6:00	454757	454739
11/6/2018 7:00	1162376	1162219
11/6/2018 8:00	1245095	1244889
11/6/2018 9:00	1055019	1054740
11/6/2018 10:00	620515	619206
11/6/2018 11:00	627907	626395
11/6/2018 12:00	702375	701713
11/6/2018 1:00	1548724	1548272
11/6/2018 2:00	1435399	1435301
11/6/2018 3:00	1464816	1464684
11/6/2018 4:00	1665515	1665362
11/6/2018 5:00	1928387	1928240

Please see the ‘findings’ section below for VSTOP’s findings from the analysis of logs.

### **VSTOP’s Findings**

Our findings include those of Mr. Stephen Berger’s. Please see Appendix D for a complete copy of his report. Some of his finding are included below.

**Findings in the Report:** VSTOP’s follow-up investigation is a continuation of the investigation for Johnson County and other counties. The findings of this report include all the findings from the preliminary report (see Appendix A). Below are summaries of the findings from the preliminary report.

#### The extent of the problem in the field and its impact:

The problem on Election Day, November 6, 2018, involved technical issues with ePB performance resulting in longer than expected wait times at Johnson County vote centers. The Johnson County election officials first began to see slow ePB performance at around 8:00 AM on November 6<sup>th</sup>. The slow ePB performance seriously disrupted the voting process in Johnson County. Additionally, this problem extended beyond Johnson County to several other counties across Indiana. Please see the preliminary report for more details.

#### The technical configuration that caused the problem:

The *ExpressPoll EZRoster 3.2.2.1* deployed in Johnson County was used in conjunction with the CentralPoint and SyncPoint servers. The *ExpressPoll EZRoster 3.2.2.1* used Microsoft Azure as its web application gateway. According to information provided by ES&S, “*CentralPoint is the web application that overlays the data transmitted by the pollbooks, and is used primarily by election administrators to monitor turnout. Syncpoint is the web service utilized by the pollbooks*





*to communicate limited data about voter check-ins from the polling places.” Please see the preliminary report for more details.*

VSTOP’s technical analysis of IIS Server logs provided by ES&S:

Retention of logs: In response to a VSTOP request for any activity logs, diagnostic logs, firewall request logs, access and performance logs, ES&S stated, *“Any logs that would reflect activity, diagnostics, requests, access or performance were not saved and, thus, not available for the WAF functionality used on Election Day.”*

Load tests: The logs provided by ES&S included results of load tests conducted in the summer and fall of 2018. In response to a VSTOP question about the timing and frequency of load tests, ES&S responded that *“ES&S is certain load tests were performed prior to the May Primary, however those results are not retained. Load tests are performed at specific times when elections are not occurring. Load testing will continue to be part of ES&S’ toolset in order to ensure environments are ready for election days in the future, and will undoubtedly evolve further as a result of this.”*

VSTOP is concerned that the results for the May Primary Election load tests were not retained.

Please see the preliminary report for more details on other findings.

**Additional Findings:** VSTOP’s follow-up investigation led to several additional findings. Each of the headings below represents a key area investigated by VSTOP.

**Retention of logs:** As part of this investigation, VSTOP analyzed two sets of logs provided by ES&S. Another set of logs were not available and these were the WAF logs. ES&S indicated that “the logs weren’t retained due to a configuration issue. This configuration issue was corrected in December and firewall logs have been configured to be retained for 365 days.” VSTOP communicated to ES&S that Indiana law (IC 3-10-1-31.1) and the United States Code (52 USC 20701) require a 22-month retention of election materials. In response, ES&S stated, “it is ES&S’s understanding that the retention of election records is the duty of the election entity charged with conduct of the election. Please note that once logs are received via SFT [Secure File Transfer] for data conversion post-election processes they are retained in our storage location for at least 22 months unless state law dictates they are to be deleted sooner. To ensure that the State of Indiana and ES&S are in full compliance with retention requirements, ES&S is happy to review and discuss current and required retention requirements during our in-person meeting.” VSTOP is concerned that the WAF logs were not saved. See VSTOP’s recommendations in the next section in this regard.

**Findings from ES&S counties in Indiana:** In response to the first set of questions and the lack of anomaly reports, ES&S stated that performance issues similar to those that occurred in Johnson County in the November 2018 election “...were not encountered during the primary election period in 2018.” However, since that time, three counties (Howard, Johnson, and Monroe) reported similar problems in the 2018 Primary Election.





Howard County stated, “During the Primary it happened at one poll location. It didn’t last very long. The ES&S team called the main office to verify and then educated us on how to handle.” Monroe County stated, “Yes, it was the same problem.”

Johnson County provided a detailed response to VSTOP on February 20<sup>th</sup>. See Johnson County’s response in the ‘responses from counties’ section above. VSTOP found that Johnson County experienced similar issues in the Primary Election, but the delay times were not as severe as those in the General Election. Johnson County reported the problem to ES&S. According to the county, ES&S may have made some changes and the problem seemed to have been resolved after some time. In a June 20, 2018 email communication between Clerk Susie Misiniec and ES&S’s Sales Manager, Jeremy Burton, he “admitted that ES&S still did not know the cause of the connectivity problems on Election Day but that they were still researching it. It was admitted that it was known that the problem was not on Johnson County’s end.” VSTOP has no record of these problems being filed as anomalies per IC 3-11-18.1-14(b). It is also a concern that a cause had not been discovered by ES&S until June 20, 2018.

**ES&S Workarounds regarding Host Issues:** In the phone call on February 27<sup>th</sup>, ES&S stated that there are two workarounds. The first involves disabling the host on the client and the second bypasses the host to continue voter check-in. In the response received on March 6<sup>th</sup>, ES&S provided the following details.

“There was only one workaround that was sent out to counties in an email approved by the IN SOS office. This involved the following steps which were outlined in the PDF attachment to the email to the counties:

- a. From the main screen, go to the Manage System Tab
- b. Select the System Setup Tab on this screen
- c. At the bottom of the screen click on Manage Devices
- d. You may need to enter the supervisor password to proceed
- e. Select the Network Tab
- f. Uncheck the box in front of the Enable Remote Host Network
- g. Click OK Save Changes
- h. Return to the Issue Ballots Tab

While other counties or polling locations may have taken an alternate approach, we do not have have [sic] any evidence that another approach was taken.”

However, on December 19, 2018, Johnson County stated the following:

“Shortly after 11 AM ET, ES&S Support representative Tim King suggested to Ms. Clark that the host wait issue could be bypassed by having poll workers enter a 4-digit supervisor code. This was tested at one of the vote centers, and it was successful. The County Election Board then met about 12 PM ET to discuss whether to instruct each vote center to utilize the supervisor code



to speed up the check-in process. Of concern was the fact that implementing such a bypass would theoretically allow a voter to be issued a ballot at more than one location. The election board and Johnson County Clerk Susie Misiniec decided that this risk was not great enough to override the need to move the voters through the lines and voted unanimously to implement the workaround. Voter Registration employees were immediately directed to contact inspectors at the vote centers to implement the workaround. The workaround was very effective, and the vote centers once again began to process voters at a good rate.

At 12:30 PM ET, ES&S Support Representative Larry Kennell called Mr. Henry to say that ES&S had come up with a change that could be made to the ePB to disable the ability to check for network connectivity. The result would be that it would not get delayed waiting for a network connection and would allow ballots to be issued without the need for a supervisor code. However, it would also not continue to attempt to connect to the network, thus it would not be known when or if the ES&S servers had begun working again. Because of this and the fact that an effective workaround was in place already, this suggestion was not implemented.”

VSTOP’s analysis of the logs shows that three counties (Carroll, Hancock and Monroe) followed the process sent out to the counties by ES&S (HostEnabled option set to FALSE (0)). For Carroll and Hancock this occurred around 2:00 PM, while for Monroe this occurred around 5:00 PM. For all other counties (including Johnson), the HostEnabled option remained TRUE (1) showing that ePB were connected to the host throughout.

VSTOP is alarmed that there is an apparent discrepancy in the above statements provided by ES&S and Johnson County.

**Failure to File Anomaly Reports:** ES&S submitted several anomaly reports of ePB problems in 2018 (see Appendix B). However, in addition to the Primary Election performance problems in Howard, Johnson, and Monroe that were not reported, VSTOP has no record of the malfunctions with ePB bases that occurred in Brown County (Primary and General election 2018) and Porter County (early voting General Election 2018).

**Late Filing of Anomaly Reports:** During the first week of January 2019, in a review of November 2018 vote history records, GCR discovered a large number of Hancock County voters flagged as “Absentee.” These should have been Election Day voters. An anomaly report was submitted by ES&S on January 22<sup>nd</sup> for Brown, Elkhart, and Hancock Counties. In a report ES&S submitted on January 22<sup>nd</sup>, it was determined that “The root cause was an error in our conversion process that determines when to set this True or False based on a value stored for the date of the Election. This date was incorrect.” In the same report, ES&S also reported anomalies for Brown and Elkhart Counties concerning incorrect date encoded for provisional ballots. VSTOP is concerned that: 1. ES&S internal testing processes did not catch the incorrect encoding of dates and 2. The problem was not discovered by ES&S during its post-elections review.



## **Findings from the Analysis of Logs**

The data in the tables above led to several findings.

- a. Johnson County's greatly decreased Ballot rate confirms the reported slow check-in times. For other counties the Ballot rate stayed largely consistent.
- b. Johnson County's average wait times went up during the 10:00 AM to 12:00 PM time period. For other counties the average wait time stayed largely consistent.
- c. In the absence of WAF logs, a correlation between server and client values cannot be established. However, the client requests are consistent throughout the day whereas, the server requests showed a drop from 10:00 AM to 1:00 PM. This is in agreement with the reported delays in check-in times during that period.

## **ES&S's internal Research into the 2018 General Election Issues**

In ES&S's responses for the preliminary report, ES&S had stated that it was conducting internal tests. In response to VSTOP's third set of questions, ES&S stated, "ES&S has not been able to re-produce the 500 internal server issue encountered and research to date has not indicated why the 500 internal server issue was indicated in the log file. ES&S continues to monitor for any application exceptions as a result of it, but currently there is no clear indicator of the cause of the message."

Further, ES&S stated, "ES&S has not been able to reproduce or replicate the performance issue related to the web application firewall issue that occurred in the general election."

During the call on February 27<sup>th</sup>, ES&S stated that the HTTP Status Code 500 issues might be caused by validating the client certificate from Azure Certificate Revocation List (CRL).

In the response received on March 6<sup>th</sup>, ES&S stated, "The reason [for the 500 internal server issue] was due to the server making a call to another TLS [Transport Layer Security] secured service and not being able to completely negotiate the secure channel."

VSTOP is concerned that lack of such testing results (a) does not help improve quality control and improvement and (b) limits the degree of confidence that future performance issues can be avoided.

## **ES&S's Corrective Action for the Short-Term and Long-Term**

**Short-term:** In response to VSTOP's third set of questions, follow-up questions, and a phone call on February 27<sup>th</sup>, ES&S described corrective actions to the Azure configuration and a long-term plan for transitioning to ES&S's hosting environment.

According to ES&S, "ES&S has made several changes to allow for further diagnostics and logs to be collected if issues arise in the future. In addition, ES&S has also made configuration



changes allowing for greater scalability without interruption, such as using the ability to scale up to more instances of the web application firewall instead of the previous limitation of 7.”

ES&S stated further that “ES&S is confident this will prevent this happening in the future as the source of the issue is being completely removed. The issue that occurred in November was a slow-down of the performance of the WAF component of the CentralPoint architecture as it exists with the Azure environment. In the interim, ES&S has reconfigured this component within the Azure infrastructure in order to allow it to scale further than it did in November. This specific component will no longer be utilized long-term with the transition to ES&S’ hosting environment.”

On March 6<sup>th</sup>, ES&S stated, “The issue experienced on Election Day was an unexplained slowdown in the performance of the Azure WAF component and a configuration that did not allow scale-out of this component.”

Given ES&S stated on two occasions that there was unexplained slow-down in the performance of the Microsoft Azure WAF component and configuration, VSTOP is alarmed that in the absence of ES&S internal research not being able to reproduce or replicate the performance issues, and unavailability of WAF logs, there is a lack of conclusive evidence that this scaling up will resolve and prevent further occurrence of performance issues.

**Long-Term:** According to ES&S, “After additional research of the issues and to further reduce its dependency on third parties, ES&S will be transitioning its e-poll book server infrastructure to ES&S’ hosting environment. ES&S expects the transition will be completed in advance of the May [2019] municipal elections. Further notification will be provided to the State in subsequent communications by ES&S.”

ES&S stated further that “Our load/performance test plan is similar to what was previously shared with VSTOP in prior communications. We are prepared to share the results of the tests when completed.”

In the phone call on February 27<sup>th</sup>, ES&S explained that the ES&S hosting environment has been in existence since 2013. However, in the last two years, it has not been used to host ePB server infrastructure. In response to a question, ES&S did not provide names of any jurisdictions where the ES&S hosting environment was used in the past to host ePB server infrastructure.

In the written responses received on March 6<sup>th</sup>, ES&S stated, “Due to commitments to support its customers throughout the months of March, April, and May with scheduled elections, we don’t expect the migration off of the Azure environment to be completed until May [2019]. Consequently, ES&S is likely to continue to service Indiana e-pollbook customers within the current Azure environment until after the May municipal elections.”

VSTOP’s concerns regarding the replication of the issue with WAF instances remains the same for May 2019 Municipal Primary Elections.



Regarding ES&S migration to their internal hosting environment, ES&S provided the following details in the responses received on March 6<sup>th</sup>:

“ES&S’ hosting environments are housed in two disparate co-location facilities connected by multi-gigabit connections. Each environment contains telecommunications redundancy, network firewalls, application firewalls, host-based intrusion detection and prevention, anti-malware and power/electrical redundancy, and are located 125+miles apart.”

“Equivalent security is provided by default within ES&S’ hosting environment. This includes but is not limited to telecommunications provider redundancy, built-in DDoS protection, network firewalls, application firewalls, host-based intrusion detection and prevention, anti-malware. ES&S’ hosting environment also leverages two-factor authentication and geo-ip filtering on all internet-facing assets, as well as IP and domain-based reputation services to assist in filtering all unneeded traffic.”

“The issue experienced on Election Day was an unexplained slowdown in the performance of the Azure WAF component and a configuration that did not allow scale-out of this component. ES&S’ hosting environment does not depend on this component and employs equivalent technology that can be scaled and adjusted more easily if the need arises. As a comparison, to make any adjustment to the Azure WAF component can take up to 30 minutes to take effect. Conversely, in ES&S’ hosting environment, an equivalent change could be performed in under 5 minutes conservatively. The move to ES&S’ hosting environment will allow quicker reaction time to unforeseen events in the future. This is just one of the many strengths of the environment to which ES&S is migrating.”

However, ES&S also stated, “There are no past testing reports available for ES&S’ hosting environment with e-pollbooks.” The absence of such test reports remains a concern.

In this regard, see VSTOP’s recommendations in the next section.

### **Summary of conclusions from Stephen Berger’s Report**

- a. Although the hypotheses proposed about the cause of the delays experience during the 2018 Midterm Election may be correct, they must be held as tentative until they can be reproduced in load testing.
- b. The failure of the current methods of system and load testing to replicate those failures raise grave doubts about the ability of the current methods to give early warning of the same or new problems.
- c. Because system changes are still being planned by ES&S, evaluating the sufficiency of those changes is not yet possible. It is important that the change approval process be clarified and agreed to by all parties. ES&S will do its own testing of the modifications it makes to its system. It is recommended that independent tests of the modified system be performed under the supervision of election officials as part of their independent due-diligence before using the new version of the system.



- d. Given the uncertainty in these areas, the lack of contingency planning is particularly troubling. Should the same or a different problem arise in the future, there is no reviewed and practiced contingency plan to deal with it or commitment by ES&S to communicate any plan to its county customers in advance of any similar problem occurring.

Please see Appendix D for the full report by Mr. Berger.

### **Recommendations**

The findings in the last section are a cause for concern. VSTOP recommends the following corrective actions and best practices. Some of the recommendations below also appeared in the preliminary report and those are included herein with revisions based on the findings of this follow-up investigation.

- a) ES&S should carefully review its internal quality control and testing processes to implement failsafe methods to prevent recurrence of the problems that occurred in Indiana counties in the 2018 Primary and General Elections. Testing and simulation procedures should be reviewed to ensure that the load test results are closely aligned with the actual Election Day results. When issues are encountered, plans for replication/reproduction of such errors should be in place.
- b) ES&S shall revise and improve anomaly reporting processes so that anomalies and problems are reported to SOS and VSTOP within the legally required 48-hour period after discovery. Review internal communication processes so that anomalies or problems that are reported to local or on-site personnel are properly recorded and reported in the ES&S's reporting repositories.
- c) ES&S must comply with state and federal laws concerning the 22-month retention period for election related materials as identified by the Indiana Election Division and the Office of the Indiana Secretary of State including logs and test results. Implement as a standard practice saving all logs and making copies available to client jurisdictions and the state after each election. This will help jurisdictions comply with the twenty-two-month retention requirement of all materials.
- d) ES&S must inform the State and jurisdictions in a timely manner when modifications in the front-end or the back-end infrastructure changes planned and executed.
- e) ES&S must thoroughly assess its pre-election and ongoing risk management and mitigation strategies to appropriately serve electronic poll book clients within the Indiana.
- f) ES&S should carefully evaluate its deployment of alternative solutions with ample time for testing and simulation.
- g) ES&S must provide prompt, clear, and consistent service that meets their contractual obligations to their county customers when counties encounter issues.





- h) ES&S must review and improve internal ES&S communication protocols to ensure that employees are responding to both customers and to ES&S supervisors regarding issues. ES&S support personnel should work in close collaboration with the ES&S technical and troubleshooting personnel for resolutions and mitigation of issues and reports results to client jurisdictions in a timely manner.
- i) ES&S should respond with project and test results by a date specified by the Secretary.
- j) Anomalies in Brown, Hancock, and Elkhart Counties were caused by incorrect settings of dates. This should be entirely avoidable with proper quality control best practices which can be set in place and to monitor for compliance.

### **The Investigation Team**

The following individuals formed the investigation team for the present inquiry.

- a. Dr. Jay Bagga and Dr. Bryan Byers, VSTOP Co-Directors
- b. Ms. Jessica Martin, VSTOP Project Manager
- c. Mr. Mani Kilaru, VSTOP IT Specialist
- d. Mr. Isaac Walling, VSTOP Computer Science Graduate Assistant
- e. Mr. Stephen Berger, Technical Consultant, TEM

### **For media questions regarding this report, please contact:**

Valerie Warycha  
Deputy Chief of Staff and Communications Director  
Indiana Secretary of State Connie Lawson  
201 Statehouse  
Indianapolis, IN 46204  
Email: VWarycha@sos.IN.gov  
Phone Number: 317-233-8655

Or

Ian Hauer  
Deputy Communications Director  
Indiana Secretary of State Connie Lawson  
200 W. Washington St.  
Indianapolis, IN 46204  
Email: IaHauer@sos.IN.gov  
Phone Number: 317-234-9682

# ELECTION SYSTEMS AND SOFTWARE (ES&S) CORRUPTION DOC

## TABLE OF CONTENTS

*Updated as of 7/16/2019, Previous Update 7/10/2019, New Bullets in Red*

- **THEME 1: ES&S Pay-For-Play Schemes Run Rampant Across U.S. As Election Officials Trade Million Dollar Voter Machine Contracts for Donations and Gifts**
  - **Topic 1:** In Georgia—The Chief of Staff to the former Secretary of State, the Deputy Chief of Staff to the Governor, the head of Legislative Affairs for the former Governor, the former Secretary of State, and the former State Election Director—were all either ES&S lobbyists or accepted large donations/gifts from ES&S (PAGE 3)
  - **Topic 2:** In order to pass bill to purchase \$150 million of new, unsafe voting equipment (likely from ES&S), GA lawmakers repeatedly lied and produced data conservative groups deemed “profoundly misleading.” (PAGE 4)
  - **Topic 3:** On February 8, 2018, Georgia Secretary of State awarded ES&S with \$450,000 sole source contract—giving a private corporation direct access to and/or responsibility over voter registration, ballot access, and ballot counting until Dec 31<sup>st</sup>, 2019. (PAGE 8)
  - **Topic 4:** Massive conflicts of interest uncovered with ES&S and elections officials in New York, Arkansas, South Carolina, Pennsylvania, Texas, Louisiana, North Carolina, Ohio, and Florida (PAGE 12)
  - **Topic 5:** South Carolina republicans to reassess voter machine procurement after ES&S corruption uncovered during process to pick vendor for \$60 million contract (PAGE 16)
  - **Topic 6:** Pennsylvania state auditor warned of nationwide ES&S vendor corruption “If it’s happening here, it must be happening elsewhere.” (PAGE 18)
- **THEME 2: ES&S Lied to Federal Lawmakers Regarding Data Security and Consistently Demonstrated a Dangerous Lack of Competence in Creating Secure and Reliable Machines. Their “Criminally Negligent” Software Caused Election Altering Undervotes, Exposed the Personal Data of Millions, and Violated State Laws**
  - **Topic 1:** ES&S machines are directly tied to significant undervotes at every level in Georgia, Florida, Texas, Arizona, Pennsylvania, and North Carolina (PAGE 20)



- **Topic 2:** Ohio software called “highly dangerous,” “criminally negligent from the standpoint of data security” and “insanely risky” by election security experts. (PAGE 23)
- **Topic 3:** ES&S has consistently demonstrated a systematic disregard for basic security best practices and a complete lack of competence in the manufacturing of reliable voting machines (PAGE 25)
- **Topic 4:** ES&S large-scale negligence exposed personal data of millions of voters, left tens of thousands of names off rolls and led to massive delays in vote counts across the country (PAGE 25)
- **Topic 5:** US Senators express national security concerns after ES&S lied to federal lawmakers, refused to reveal which states were sent critically flawed machines, and vigorously fought attempts to reveal reliability information (PAGE 31)
- **Topic 6:** ES&S Indiana contract terminated after investigation reveals ES&S violated state law, lied to election officials, and were responsible for errors resulting in long wait times, voter anxiety, discouraged voters, and embarrassment. (PAGE 35)
- **Appendix:**
  - **A:** 2017 ES&S Security Test Report: Missing Operating Systems & Patches (PAGE 38)
  - **B:** Georgia Vendor RFI Analysis: Statewide Voting Machine Contracts (PAGE 39)
  - **C:** Map of Voting Systems Across the U.S.—Pew Research Center/Verified Voting Foundation (PAGE 40)

## **ES&S PAY-FOR-PLAY SCHEMES RUN RAMPANT ACROSS U.S. AS ELECTION OFFICIALS TRADE MILLION DOLLAR VOTER MACHINE CONTRACTS FOR DONATIONS AND GIFTS**

IN GEORGIA—THE CHIEF OF STAFF TO THE FORMER SECRETARY OF STATE, THE DEPUTY CHIEF OF STAFF TO THE GOVERNOR, THE HEAD OF LEGISLATIVE AFFAIRS FOR THE FORMER GOVERNOR, THE FORMER SECRETARY OF STATE, AND THE FORMER STATE ELECTION DIRECTOR WERE ALL EITHER ES&S LOBBYISTS OR ACCEPTED LARGE DONATIONS/GIFTS

**David Dove, Chief of Staff to former Secretary of State Brian Kemp, Accepted Las Vegas Trips From ES&S While His Office Was In The Market For New Voter Machines.** In March of 2017, when Dove attended an E.S. & S. junket in Las Vegas, Kemp's office was in the market to replace the state's entire inventory of voting machines. "It's highly inappropriate for any election official to be accepting anything of value from a primary contractor," Virginia Canter, the chief ethics officer at Citizens for Responsibility and Ethics in Washington, told McClatchy. "It shocks the conscience." ([The New Yorker](#), 1/22/2019)

**Kathy Rogers, Georgia's Former State Elections Director Who Opposed Paper Ballot Records, Is Now an ES&S Lobbyist and ES&S's Senior Vice President for Government Affairs.** "Kathy Rogers, E.S. & S.'s senior vice-president for governmental affairs, told McClatchy that there was nothing untoward about the advisory board, which she said has been "immensely valuable in providing customer feedback."...In 2006, a bill requiring a verifiable paper record of each ballot, introduced in the Georgia legislature at the urging of election-integrity advocates, failed after the state's elections director, Kathy Rogers, opposed it. Rogers, of course, later went to work for E.S. & S. Election-integrity advocates sued in response, challenging the legality of the state's voting equipment." ([The New Yorker](#), 1/22/2019)

**Karen Handel, Georgia's former Secretary of State, Received \$25,000 in Contributions From Voting Machine Lobbying Firm.** "In the three years that the case wended its way through the courts, where it was eventually dismissed by the Georgia Supreme Court, the new secretary of state, Karen Handel, was found to have received twenty-five thousand dollars in campaign contributions from employees and family members associated with Massey and Bowers' lobbying firm." ([The New Yorker](#), 1/22/2019)

**Charles Harper, Brian Kemp's current Deputy Chief of Staff and former Legislative Director, Was a Lobbyist for ES&S as Recently as June 2018.** "In 2012, Charles Harper, a sod farmer who had been elected to the Georgia House of Representative a decade earlier, became a registered lobbyist in the office of the Georgia secretary of state, Brian Kemp, where he served as legislative director. At the end of 2017, as Kemp was ramping up his campaign for governor, Harper did not renew his lobbying credentials with the secretary of state. Instead, he registered to lobby for E.S. & S...After Kemp won the governor's race, in November, he named Harper, whose contract with E.S. & S. ended in June, 2018, to his transition team. Harper is now Kemp's deputy chief of staff." ([The New Yorker](#), 1/22/2019)

**John Bozeman, the Head of Legislative Affairs for Former Governor Sonny Perdue, Has Been a Registered Lobbyist with ES&S Since 2017.** “At the end of 2017, as Kemp was ramping up his campaign for governor, Harper did not renew his lobbying credentials with the secretary of state. Instead, he registered to lobby for E.S. & S. Around the same time, John Bozeman, then the head of legislative affairs for Georgia’s former governor, Sonny Perdue (who is now the Secretary of Agriculture in the Trump Administration), also registered to lobby on behalf of E.S. & S.” ([The New Yorker](#), 1/22/2019)

**IN ORDER TO PASS BILL TO PURCHASE \$150 MILLION OF NEW, UNSAFE VOTING EQUIPMENT (LIKELY FROM ES&S), GA LAWMAKERS REPEATEDLY LIED AND PRODUCED ANALYSIS CONSERVATIVE GROUPS DEEMED “PROFOUNDLY MISLEADING”**

**Georgia Lawmakers Chose New Voting Equipment that Shared “Similar Risks” to Machines a Federal Judge Deemed a Constitutional Risk.** “The new equipment would replace the state’s paperless, electronic machines — technology so risky that a federal judge said last year that its continued use threatened Georgians’ “constitutional interests.” But security researchers say similar risks exist in the new electronic machines that the GOP-led legislature has chosen, which would embed the voter’s choice in a barcode on a slip of paper.” ([Politico](#), 3/28/2019)

**Cybersecurity Experts Said Georgia Lawmakers Made “False and Misleading” Statements that Flatly Contradicted Objective Evidence in Support of Bad Voting Machine Bill.** “The bill’s sponsors made false and misleading statements during the entire legislative session in hearings leading up to the vote, often flatly contradicting objective evidence or mischaracterizing scientific writing,” said Georgia Institute of Technology computer science professor Rich DeMillo, who testified throughout the process.” ([Politico](#), 3/28/2019)

**Two Conservative Groups Called GOP Sec. of State’s Brad Raffensperger’s Hand-Marked Ballot vs Machine Marked Analysis “Profoundly Misleading.”** “Two conservative groups, the National Election Defense Coalition and FreedomWorks, called the voting-machine deal a “boondoggle” in a letter last week to state Senate Republicans. “The Secretary of State is circulating a cost analysis that is profoundly misleading and wildly inflates the costs of conducting elections with hand-marked paper ballots,” they wrote.” ([The New Republic](#), 3/06/2019)

**GOP State Senator William Ligon Repeatedly Demonstrated a Lack of Understanding of Cyber Security and Ignored Warnings from Experts During Debate.** “Ligon, who praised ballot-marking devices as “the technology of today built upon the experience of the past,” repeatedly demonstrated what experts called a lack of understanding about the cybersecurity implications of using computers to generate ballots, based on his comments during the Senate debate on the bill. “If there is any discrepancy discovered in an audit between what the machine says and what the paper says,” he assured his colleagues, “the paper will control.” But the paper ballot is generated by the machine and can thus be corrupted at the source, rendering a meaningful audit impossible. Stark, who invented the widely recommended audit technique known as a risk-limiting audit, warned Georgia lawmakers about this, but “they ignored his warning,” DeMillo said.” ([Politico](#), 3/28/2019)

**State Sen. Ligon Falsely Stated that Barcode Devices and Hand-Marked Paper Ballots Posed Equal Hacking Risk.** “State Sen. William Ligon, the bill’s chief defender in the chamber, said the barcode devices and hand-marked paper ballots were equally at risk of hacking. That’s just not the case, researchers said. “Hacking and configuration errors cannot cause pens to put the wrong votes on hand-marked paper ballots, but they can cause ballot-marking devices to print the wrong votes on the paper record,” Philip Stark, a statistics professor and voting security expert at the University of California at Berkeley, said in an email.” ([Politico](#), 3/28/2019)

**State Sen. Ligon Falsely Stated that Optical Scanners Had Not Changed in 20 Years.** “Ligon said the technology of optical scanners was “pretty much the same” as it was in 2000, even though, as DeMillo noted, “imaging capabilities have increased by orders of magnitude in the last twenty years.” ([Politico](#), 3/28/2019)

**State Sen. Ligon Falsely Denied that Hand-Marked Paper Ballots Eliminated Need for Voter Verification.** “During a colloquy with Parent, Ligon also denied (wrongly, experts said) that removing the ballot-generating computer — as hand-marked ballots do — eliminated the need for a voter to verify his or her ballot, despite this being one of the chief advantages of not using computers to mark ballots. (Research shows that voters using ballot-marking devices do not check to make sure the computer marked their ballot properly.)” ([Politico](#), 3/28/2019)

**HB316 Bill Sponsor, Georgia State. Sen. Ligon, Later Claimed He Was Not Familiar with Recommendations Provided by Election Experts on the GA [SAFE] Commission.** “Georgia state Senator William T. Ligon Jr. doesn’t agree that touchscreens are a less reliable method for casting votes. He was a sponsor of the bill, now signed into law, overhauling Georgia’s election system... Ligon said he wasn’t familiar with Lee and his advice to the commission.” ([Quartz](#), 7/9/2019)

**GOP State Senator Greg Dolezal Falsely Stated that “Hackability” of Various Voting System Was Uniform.** “Republican Sen. Greg Dolezal, too, said the “hackability” of various voting systems was “uniform,” despite the widespread consensus from technical experts that it’s not.” ([Politico](#), 3/28/2019)

**GOP State Senator P.K. Martin IV Claimed, Without Evidence, that There Were No Instances of Hackers Breaching GA Voting Systems.** “Sen. P.K. Martin IV, another Republican, said there had been “zero” instances of hackers breaching Georgia’s current voting machines. But there’s no evidence that hackers haven’t tampered with Georgia’s current voting system — paperless machines can be hacked to prevent any signs of tampering — and the machines have previously generated results that prompted questions about their reliability.” ([Politico](#), 3/28/2019)

**Despite the National Academies Recommending Against Barcode Technology in Voting Systems Last Year, GOP State Rep Barry Fleming Claimed the Technology Would Bring GA Into the 21<sup>st</sup> Century.** “Republicans largely hailed the [barcode] technology. “We can put our voters first in Georgia and bring us into the 21st century,” Republican state Rep. Barry Fleming said after the vote, according to The Atlanta Journal-Constitution... In a landmark report published last year, the National Academies recommended against voting devices that tally barcodes. “Electronic voting systems that do not produce a human-readable paper ballot of record raise security and verifiability concerns,” it said. “Additional research on ballots produced by BMDs will be necessary to understand the effectiveness of such ballots.” ([Politico](#), 3/01/2019)

**GA State Senator, Elena Parent, Said the Relationship Between ES&S and GA Officials “Reeks of Corruption” and There is “No Good Reason” to Buy ES&S Machines.** “Democratic state Sen. Elena Parent, who opposes the type of equipment the state is preparing to purchase — which includes an electronic marking device that produces a paper ballot — condemned the close ties between the company [ES&S] and the state. “I’ve been given absolutely no good reason why we should buy these things. There’s not one good reason. So therefore it just reeks of corruption, that we’re prioritizing vendors over voters,” Parent said on the Senate floor during a debate in March.” ([NPR](#), 5/2/2019)

**ES&S Repeatedly Told Georgia State Officials That Its Machines Were Not Connected to the Internet, Despite Strong Disagreement from Cyber Security Experts.** Quotes from ES&S Request For Information Response: “Furthermore, the EMS [Election Management System] system is closed (air-gapped) and therefore has no connection to the internet.” (pg. 17) “Standalone hardened system that is not connected to the Internet or any other network.” (pg. 17) “The data is accessed by the database server through a service account, thereby protecting the data files from being directly accessed. The EMS is isolated from any connection to the internet or other networks.” (pg. 18) ([ES&S GA RFI](#), 8/24/2018)

**National Election Defense Coalition Said the Assertion Voting Machines Are “Not Connected to the Internet” is a Damaging Myth Preventing Election Officials from Using Paper Ballots.** “The incorrect assertion that voting machines or voting systems can’t be hacked by remote attackers because they are ‘not connected to the internet’ is not just wrong, it’s damaging,” says Susan Greenhalgh, a spokeswoman for the National Election Defense Coalition, an elections integrity group. “This oft-repeated myth instills a false sense of security that is inhibiting officials and lawmakers from urgently requiring that all voting systems use paper ballots and that all elections be robustly audited.” ([NYT](#), 2/21/2018)

**Cybersecurity Experts Explain Election Data Transmitted Via Phone Lines Are Still Connected to the Internet.** “Election officials and vendors insist that the modem transmissions are safe because the connections go over phone lines and not the internet. But as security experts point out, many of the modems are cellular... These routers are technically part of the internet.” ([NYT](#), 2/21/2018)

**Cybersecurity Experts Detail How Election Results Can Still Be Intercepted Since Phone Lines Are Part of the Internet.** “Because of this, attackers could theoretically intercept unofficial results as they’re transmitted on election night — or, worse, use the modem connections to reach back into election machines at either end and install malware or alter election software and official results. “Almost any phone call, whether on a cellular network or a so-called landline, goes through a part of the internet,” says Andrew Appel, a computer-science professor at Princeton University and longtime voting-machine security expert.” ([NYT](#), 2/21/2018)



**Georgia's SAFE Commission Ignored Security Measures Directly Recommended by Georgia Tech, Stanford, Yale, Princeton, MIT & Google Election Experts.** "Earlier this year, Georgia's [SAFE] Commission held a public meeting at the state capitol to answer a pressing question: What should Georgia do to replace its aging, touchscreen voting machines, as well as other parts of its election system?... Computer scientists and elections experts from around the country had weighed in during the seven months of the commission's deliberations on the issue... **Despite this, the commission ultimately did not recommend measures backed by Lee and his colleagues** at places like Stanford, Yale, Princeton, MIT, and Google—including the recommendation that the state return to a system of paper ballots filled out by hand, combined with what scientists call risk-limiting audits." ([Quartz](#), 7/9/2019)

**Elections Experts Fear Georgia's Ignorance of Election Security Issues Will be Copied by Other States & Cause Nationwide Erosion of Election Integrity.** "Georgia's decision has computer scientists and election experts worried that lessons learned over nearly two decades of computerized voting are being woefully ignored. Indeed, hundreds of millions of dollars have been or will soon be spent in these and other states on technology that experts say decreases election security and erodes election integrity." ([Quartz](#), 7/9/2019)

**Including Georgia, Only 33% of Counties Nationwide Use Machines with No Paper Trail or Machines that "Print" Ballots.** "With its decision, Georgia's counties remain among the 33% of counties nationwide that use either machines with no paper trail or machines that print paper ballots, which are then scanned on separate machines. The vast majority of the rest of the counties use paper ballots filled out by hand, which are then scanned or counted by hand." ([Quartz](#), 7/9/2019)

**Georgia New Machines May Run On Unsupported Software.** "The AP surveyed all 50 states, the District of Columbia and territories, and **found multiple battleground states affected by the end of Windows 7 support**, including Pennsylvania, Wisconsin, Florida, Iowa, Indiana, Arizona and North Carolina. Also affected are Michigan, which recently acquired a new system, and Georgia, which will announce its new system soon. ([AP](#), 7/13/2019)

**It Is Unclear Whether Georgia Counties Will Be Forced to Pay for Windows 10 Software Update.** "Critics say the situation is an example of what happens when private companies ultimately determine the security level of election systems with a lack of federal requirements or oversight. Vendors say they have been making consistent improvements in election systems. And many state officials say they are wary of federal involvement in state and local elections. It's unclear whether the often hefty expense of security updates would be paid by vendors operating on razor-thin profit margins or cash-strapped jurisdictions." ([AP](#), 7/13/2019)

**ES&S Implied "Jurisdictions" May Ultimately be Responsible for Updating Software Expenses.** "ES&S said it expects by the fall to be able to offer customers an election system running on Microsoft's current operating system, Windows 10. It's now being tested by a federally accredited lab. For jurisdictions that have already purchased systems running on Windows 7, ES&S said it will be working with Microsoft to provide support until jurisdictions can update. Windows 10 came out in 2015. ([AP](#), 7/13/2019)

**GA Sec of State Failed to Follow Federal Judge Orders to Preserve FBI Election Data Evidence**

**After Secretly Deleting Data on State Server.** “Nearly two years ago, state lawyers in a closely watched election integrity lawsuit told the judge they intended to subpoena the FBI for the forensic image, or digital snapshot, the agency made of a crucial server before state election officials quietly wiped it clean. Election watchdogs want to examine the data to see if there might have been tampering, given that the server was left exposed by a gaping security hole for more than half a year. A new email obtained by The Associated Press says state officials never did issue the subpoena, even though the judge had ordered that evidence be preserved, including from the FBI.” ([AP](#), 7/3/2019)

**Brian Kemp Denied Ordering Election Data Destruction in 2017, Called Destruction “Reckless, Inexcusable, and Inept.”** Technicians at the Center for Elections Systems at Kennesaw State University, which then ran the state’s election system, erased the server’s data on July 7, 2017, less than a week after the voting integrity suit was filed. **After the AP reported on it three months later, Kemp denied ordering the data destruction or knowing about it in advance** and called it reckless, inexcusable and inept. ([AP](#), 7/3/2019)

**Georgia Officials Failed to Disclose that the Department of Homeland Security Warned them that the State May Be a Cyber Target.** “As lawyers for Georgia’s secretary of state argued vehemently last fall that the state’s obsolete electronic voting infrastructure was secure from hackers, **they failed to mention a warning from the U.S. Department of Homeland Security that Georgia might already be a cyber target.** “Foreign governments may engage in cyber operations targeting the election infrastructure and political organizations in Georgia and engage in influence operations that aim to interfere with the 2018 U.S. elections,” according to a memo by the U.S. Department of Homeland Security Southeast region addressing “a Georgia Perspective on Threats to the 2018 U.S. Elections.” ([Law.com](#), 7/15/2019)

**The Department of Homeland Security Warned Georgia Election Officials That Foreign Actors May Attempt to Enter Polling Places, Hack Voter Registration Systems, and Access Information Technology.** “The DHS memo warned Georgia election officials that the agency’s Office of Intelligence and Analysis was particularly concerned that foreign actors would employ at least 10 different methods in **efforts to interfere with the 2018 election in Georgia.** They included: Unauthorized entry to polling places...Attempts to hack voter registration systems...Attempts to access information technology infrastructure used to manage elections, display results, or for counting or certifying votes...Efforts to compromise networks or election-related systems...” ([Law.com](#), 7/15/2019)

**IN FEBURARY 2018, GEORGIA SECRETARY OF STATE AWARED ES&S WITH \$450,000 SOLE SOURCE CONTRACT – GIVING PRIVATE CORPORATION DIRECT ACCESS TO AND/OR RESPONSIBILITY OVER VOTER REGISTRATION, BALLOT ACCESS, AND BALLOT COUNTING THROUGH DECEMBER 31, 2019**

**In 2019 RFP, GASOS Said Their Office Was Responsible for Maintaining Voter Registration System, Building Ballots, and Creating Poll Book Files.** “Election Structure: State law provides for a uniform voting system where every county uses the same type of voting equipment...The GASOS

maintains the Voter Registration System (“eNet”), builds ballots for each federal, state, and county election, and creates Electronic Poll Book (“EPoll”) files. ([GASOS RFP](#), 3/15/19)

**In 2018, GASOS Transferred Georgia Election Data Preparation Services—Previously Performed by State Entity, Center for Election Systems—to Private Corporation, ES&S.**

“Exclusive Capability: ...Assistance in data preparation requires a license to utilize both pieces of software. These services were previously provided by the Center for Election System, which, as a state entity, was able to utilize the license purchased by the State of Georgia from ES&S...Now that the functions of the Center for Election Systems have been moved to the State Entity, State Entity requires a vendor who has licenses to both components of the voting system to assist in the data preparation. State Entity also requires a vendor...who knows the specific processes utilized by the Center for Election Systems in how they built their data sets.” ([CGG Subpoena](#), page 15, 7/5/2019)

**In 2018, GASOS Paid Private Corporation-ES&S \$300,000 to Prepare Data Necessary for the Entire Georgia Election Management System (GEMS) & for All Voter Rolls.**

“Scope of Work: State Entity seeks to enter into a contract to provide assistance in data preparation for ExpressPoll 4000 and 5000 running EZRoster version 2.1.2 and the Georgia Election Management System (GEMS) database version 1.18.22g!... The cost will be \$25,000 per month for the calendar year 2018.” ([CGG Subpoena](#), page 14, 7/5/2019)

**In 2019, GASOS Paid Private Corporation, ES&S, an Additional \$150,000 to Extend Data Preparation and Ballot Layout Services Through December 31, 2019.**

“The Agreement between Election Systems & Software (“Contractor” or “ES&S”) and Georgia Secretary of State dated February 8, 2018 for Ballot Building Support Services is hereby renewed for a term of January 1, 2019 through December 31, 2019 and amended as set forth below:...Payment Terms: 50% of total due (\$75,000) shall be payable on January 1, 2019 upon receipt of corresponding contractor invoice. The remaining 50% of total due (\$75,000) shall be payable on July 1, 2019 upon receive (sic) of corresponding contractor invoice.” ([CGG Subpoena](#), page 12, 7/5/2019)

**ES&S Prepared Election Data for All 159 Georgia Counties & for Every County, State, and**

**Federal Race in 2018.** “State Entity requires data preparation for 159 counties for all county, state, and federal races in Georgia including primary, primary runoffs, general election, general election runoffs, and any special elections. The cost will be \$25,000 per month for the calendar year 2018.” ([CGG Subpoena](#), page 14, 7/5/2019)

**GASOS Failed to Document Any Effort to Locate Other Vendors—Claimed Vendor Change Would Be “Too Costly.”**

“Market Research: Sole Source: A purchasing situation in which the procurement is available from only one source. The announcement must be posted to the GPR in accordance with the Georgia Procurement Manual, Section 2.3.3.3. Question: Identify efforts made to locate other possible sources: Answer: “Current License provider for Georgia Election Management System. Changing systems would be to (sic) costly.” ([CGG Subpoena](#), page 19, 7/5/2019)

**GASOS Claimed 2018 “Sole-Source” Award to Private Corporation, ES&S, Justified Because ES&S Was Only Company with Licenses to Work Both Components of Georgia’s Voting System.**



“Sole-Source Intent to Award Justification: Exclusive Capability: The State of Georgia utilizes ExpressPoll 4000 & 5000 running EZRoster version 2.1.2 and GEMS version 1.18.22g!. Assistance in data preparation requires a license to utilize both pieces of software....ES&S provided both systems to the state and has a license to maintain both databases... ES&S has specific knowledge that is necessary to the fulfillment of these services and is the only company that has licenses to work with both components of Georgia’s voting system.” ([CGG Subpoena](#), page 15, 7/5/2019)

**Election Expert Disputed GASOS Sole-Source Argument Claim—Said GASOS Awards Licenses, Not the Vendor/ES&S.** “Vendors are in the business of providing software licenses for a fee, so election administrators should be the ones to get a license to use the necessary software. In the U.S., our federalist system says that election officials administer elections –not private corporations. ([Twitter](#), @eddiepereztx, 7/5/2019)

**Election Expert Said GASOS Claim that Only ES&S Could Provide Election Administration Services “Exceptional” and Uncommon.** “NOT common (exceptional): D) Assertions by a state or county authority that no one other than the vendor can provide election administration services, because no one other than the vendor has a license to use voting system software.” ([Twitter](#), @eddiepereztx, 7/5/2019)

**Election Expert Said Georgia Sec. of State’s Decision to Pay ES&S to Maintain Election Databases Was “Atypical” & “NOT common.”** “NOT common (atypical): C) Paying a vendor to \*maintain\* ballot programming databases. (Once the vendor’s ballot programming is complete, the databases are typically turned over to state or county election officials, so they can run the election under their own auspices).” ([Twitter](#), @eddiepereztx, 7/5/2019)

**Election Expert Said Georgia’s 2018 Contract with ES&S “Robbed” State & County Officials Power to Run their Own Elections.** Vendors are in the business of providing software licenses for a fee, so election administrators should be the ones to get a license to use the necessary software. In the U.S., our federalist system says that election officials administer elections — not private corporations. 6/ Saying “Only the vendor that holds the license has the license to use election software” is tautological, and it robs both the state and county officials from having the wherewithal to run their own elections.” ([Twitter](#), @eddiepereztx, 7/5/2019)

**Contract Said ES&S is Responsible for All Ballot Layout, Coding & Voice File Services in Georgia.** “1. BALLOT LAYOUT, CODING, AND VOICE FILE SERVICES – Scope of Services includes the data entry and maintenance of County level databases in the State of Georgia for all county (including municipal elections that are administered by counties), state and federal elections in Georgia in calendar year 2019, including primary, primary runoffs, general election, general election runoffs, and special elections. ES&S will receive the data required to facilitate the creation of paper and electronic ballots as well as audio file recording to the State of Georgia for review and approval.” ([CGG Subpoena](#), page 12, 7/5/2019)

**Election Expert Said Counting of Votes Should “Never, Ever” be Done by the Vendor.** “If a state or local official outsources programming, that’s one thing; but the actual tabulation function, i.e. insertion of memory cards into the tabulation computer, and the counting of the votes, should be done solely by election officials, and never, ever by the vendor.” ([Twitter](#), 7/5/2019)

**Texas Secretary of State’s Office Said ES&S Ballots Failed to Present Candidates Consistently or Separate Races Properly During Initial Examination.** “The full-face ballot layout used during the examination was less than ideal. Too much of the available screen real estate was unused. Also, the candidates were not presented consistently for each race. Sometimes the candidates for a race were presented vertically and sometimes they were presented horizontally.” ([Texas Secretary of State](#), 1/22/19)

**Texas Secretary of State’s Office Said ES&S Poor Ballots Designed Caused Candidates to be “Lost in the Mix” During Initial Examination.** “Ballot layout requires consideration of how the candidates and parties are displayed. At the very least, a blank line or race separator (i.e. double line) should be between each race. This should be enforced by the layout software so the ballot isn’t presented like the test ballot which had races stacked on top of each other. With many candidates listed across the columns, and no gap before the next race, some of the candidates were “lost” in the mix due to their unfavorable location. The ES&S representative said that the poor layout was because she is not an expert in ballot design on the XL.” ([Texas Secretary of State](#), 1/22/19)

**ES&S Representative Failed to Properly Display Candidates During State Examination—Said She was “Not an Expert in Ballot Design.”** “With many candidates listed across the columns, and no gap before the next race, some of the candidates were “lost” in the mix due to their unfavorable location. The ES&S representative said that the poor layout was because she is not an expert in ballot design on the XL.” ([Texas Secretary of State](#), 1/22/19)

**ES&S is Responsible for All Data Entry & Maintenance of County Level Data Sets in Georgia.** “2. EXPRESSPOLL DATA SETS FOR ADVANCE VOTING PURPOSES – Scope of Services includes the data entry and maintenance of County level data sets in the State of Georgia for all county (including municipal elections that are administered by counties), state, and federal elections in Georgia in calendar year 2019, including primary, primary runoffs, general election, general election runoffs, and special elections. ES&S will receive the data required to facilitate the creation of ExpressPoll data sets for Advance Voting purposes to the State of Georgia for review and approval. Creation of ExpressPoll data sets does not include any handling or conversion of voter data.” ([CGG Subpoena](#), page 12, 7/5/2019)

**ES&S Provided Georgia with its Election Management System & Has License to Maintain that System.** Purpose of the Sole Source. The State of Georgia utilizes ExpressPoll 4000 & 5000 running EZRoster version 2.1.2 and GEMS version 1.18.22g!...ES&S provided both systems to the state and has a license to maintain both databases. Through contracts with all Georgia counties, ES&S has been the sole maintenance provider on the system since its purchase... ([CGG Subpoena](#), page 18, 7/5/2019)

**GASOS Stated EPoll Data Management System (EPDMS) Combines Voter Registration & Election Ballot Data into Voter Lists for Poll Books & Voter Specific Ballots.** “EPoll Data Management System (EPDMS) – Used to combine voter registration and election ballot data into an election-specific elector’s list that powers the electronic poll book (EPoll) and provides each voter with the properly assigned ballot style.” ([GASOS RFP](#), Attachment M, 3/15/19)

**GASOS Stated EPDMS Must Accept Imports of Voter Registration Data from eNet Including Voter Name, Driver License Number, Voter Status, & Voter Polling Place.**

“Confirm That Capability Exists and is Able to be Demonstrated: Capabilities: a. Accept imports of voter registration data from eNet on removable devices for the purposes of building an elector’s list for any given election. The data transferred from eNet includes but is not limited to: Voter Name...Voter Street Address, Voter City, State, Zip, Driver License number, Voter Registration ID, Voter Status, Assigned Precinct, Assigned District Combination Value, Assigned Polling Place, Polling Place Street Address, Polling Place City, State, Zip, and Absentee Status. ([GASOS RFP](#), Attachment M, 3/15/19)

**Winning Vendor of RFP Process Must Complete Pilot Program In 10 Counties During November 2019 Election.** “For the purposes of this eRFP, the Supplier’s preliminary plan and estimates for delivery are to be in a phased roll-out as a pilot project and then a full roll-out to all counties. Phase 1 will be the full inventory distribution and necessary training of up to 10 counties selected by GASOS to participate in a pilot project to be executed in November 2019. The pilot equipment will be used in any associated November 2019 election schedule for the selected counties.” ([GASOS RFP](#), Page 42, 3/15/19)

**Winning Vendor of RFP Process Must Distribute 1,272 Voting Machine Components by December 31, 2019.** “Phase 2 will be broken into two parts. Phase 2-Part 1 will be distributing a minimum of five BMD, two PPS, and 1 EMS computer to each county (159). These components will facilitate election official and poll worker training activities...Completion of Phase 2 – Part 1 will be completed by endo for the fourth quarter of 2019 (December 31<sup>st</sup> 2019).” ([GASOS RFP](#), Page 42, 3/15/19)

**GASOS Said ES&S “Knows the Specific Processes” Used by KSU’s Center for Election Systems to Build Their Data Sets.** “ES&S also worked closely with the Center for Election Systems and is most familiar with the processes it utilized to provide these data sets...State Entity also requires a vendor who best knows the Georgia voting system, who is familiar with Georgia counties, and who knows the specific processes utilized by the Center for Election Systems in how they built their data sets.” ([CGG Subpoena](#), page 15, 7/5/2019)

## MASSIVE CONFLICTS OF INTEREST UNCOVERED WITH ES&S AND ELECTIONS OFFICIALS IN NEW YORK, ARKANSAS, SOUTH CAROLINA, PENNSYLVANIA, TEXAS, LOUISIANA, NORTH CAROLINA, OHIO AND FLORIDA

**In Order to Secure \$40 Million NY Contract, ES&S Paid Anthony Mangone \$50,000 to Act as Lobbyist--Despite Mangone Being Under Federal Investigation for Corruption and Previously Pleading Guilty to Election Rigging (2010).** "While a Republican lawyer was under federal investigation in a Yonkers corruption case, he was paid nearly \$50,000 last year to help a Nebraska company win a contract to provide New York City with new voting machines. Anthony Mangone was indicted this month with Yonkers Councilwoman Sandy Annabi and former city GOP Chairman Zehy Jereis on extortion, bribery and other federal charges related to payments made to Annabi for her to change votes on city projects. Coincidentally that same day, the New York City Board of Elections voted to buy thousands of new electronic voting machines - a contract expected to be worth more than \$40 million - from Mangone's client, Election Systems & Software...Mangone was implicated in a Westchester vote-rigging scheme a decade ago, admitting that he opened about 30 sealed absentee ballots during the 2000 Green Party primary and wrote in the names of his boss, Republican state Sen. Nicholas Spano, and a judicial candidate... Mangone agreed to plead guilty to a misdemeanor in the case but was never charged." (*The Journal News*, Bandler, 1/21/2010)

**New York Board of Elections Head Resigned From ES&S Advisory Board After Conflicts of Interest Uncovered (2018).** "The head of the city's Board of Elections Michael Ryan, a native Staten Islander, abruptly resigned from his post on the advisory board of the maker of New York City's voting machines, Election Systems and Software (ES&S), earlier this week. His resignation came after a NY1 report found that ES&S had flown Ryan around the country to destinations like Las Vegas putting him up in hotels and buying him dinners. Ryan reportedly did not disclose several ES&S paid trips in his annual disclosure forms with the city's conflict of interest board." ([SI Live](#), 10/13/2018)

**Arkansas Secretary of State Bill McCuen Pleaded Guilty to Felony Charges that He Took Bribes and Accepted Kickbacks from Company that Would Become ES&S (2002).** "Arkansas. February 2002. Arkansas Secretary of State Bill McCuen pleaded guilty to felony charges that he took bribes, evaded taxes, and accepted kickbacks. Part of the case involved Business Records Corp. now merged into Election Systems & Software. The scheme also involved Tom Eschberger, an employee of BRC, but Eschberger received immunity from prosecution for his cooperation. Today, Eschberger remains employed with ES&S." ([Voters Unite](#), 7/10/2007)

**South Carolina's Director of Elections Resigned From ES&S Advisory Board Right Before State Reviewed Voting Machine Bids, Claimed No Impropriety After Conflicts of Interest Uncovered.** "For more than a decade, Marci Andino, executive director of the S.C. Election Commission, served on an advisory board formed by Elections Systems and Software, known commonly as ES&S. Andino received more than \$19,000 worth of flights, hotels and meals from ES&S since 2009 to attend regular conferences at the company's headquarters in Nebraska and other cities across the country, according to records with the South Carolina Ethics Commission...On Monday, Andino confirmed she stepped down from her advisory position with the company last year in anticipation of the state requesting bids for a new voting system. She promised her connection to ES&S would in no way impact the state's decision over which company wins the multimillion dollar contract. Andino said she will not be taking part in selecting the winning bid." ([Post & Courier](#), 1/29/2019)

**Pennsylvania County Election Director Resigned From ES&S Advisory Board Right Before County Vote To Purchase ES&S Poll Book System, Claimed No Impropriety After Undisclosed Conflicts of Interest Uncovered.** "Crispell traveled to Las Vegas and Nebraska last year for meetings of the Election Systems & Software (ES&S) customer advisory board. Her travel expenses were paid for by ES&S, which supplied the voting machines Luzerne County has used for more than 10 years, as well as an electronic poll book system the county purchased this year for \$324,802. Crispell resigned from the advisory board in October 2017, before the county requested proposals for the poll book system from vendors. She did not disclose her service on the board to county council before it voted on the poll book purchase, in April." ([Citizens' Voice](#), 12/7/2018)

**Dallas, Texas Elections Administrator Asked To Resign After "Troubling" ES&S Conflicts of Interest Uncovered.** "State ethics laws are clear when it comes to the relationship between public officials and vendors. Over the past two years, Dallas County has paid them or their subsidiaries \$3.5 million dollars for software and services. As Dallas County Elections Administrator, Toni Pippins-Poole recommends to the Commissioners Court which vendors get hired...In a June 7 email, she asks a county employee... "Have you checked with [vendor] ES&S to sponsor the Texas Delegation pins for IGO or the shirts?" The next day, a representative from ES&S emailed Pippins-Poole regarding paying for the lapel pins. He writes... "In the past we simply wrote a check to Toni..." He adds..."We can send a check made out to you (Toni) for the \$1500 amount..." "For an elections administrator to solicit contributions from a vendor is troubling," said Joe Kulhavy, a former staff attorney for the Texas Secretary of State's elections division who looked at Pippins-Poole's emails at WFAA's request." ([WFAA ABC](#), 10/19/2017)

"A candidate for Dallas County commissioner on Tuesday asked a judge to remove Elections Administrator Toni Pippins-Poole from office, alleging incompetence and official misconduct. J.J. Koch, a Republican, accused Pippins-Poole of improperly soliciting a gift from a county contractor." ([Dallas News](#), 10/2017)

**Louisiana Elections Commissioner Accepted \$3000 in Donations from ES&S Prior to Recommending ES&S for a \$4 Million Voting Machine Contract.** "Elections Commissioner Suzanne Terrell won praise for the way she selected the vendor for computerized absentee voting machines. But Legislative Auditor Daniel Kyle said he was still troubled by the selection of a company that has a top official who was allegedly involved in illegal dealings in Arkansas...Terrell was given a chance to explain how she chose Elections Systems and Software for a \$4 million contract to provide the new voting machines...Terrell said she has contributed Eschberger's \$2,000 campaign gift to a charity, later identified by staff aide Pat Bergeron as Girls' State. She said it was "naive" of her to have accepted the gift from Eschberger and another \$1,000 contribution from the Adams and Reese law firm that lobbies for ES&S." (*Daily Town Talk*, Morgan, 2/7/2002)

**North Carolina Election Directors Accepted Large Cash Donations From ES&S, Allowed Vendors to Charge Double for Ballots, After \$3 Million Statewide Voting Machine Contract.** "A group made up of election directors from across North Carolina has received large cash donations from the owner of a New Bern company that maintains the state's voting machines and prints most of its ballot...Printelect is the sole agent in the state for Election Systems & Software, a company that won a concession in 2006 to sell and maintain all of the voting machines in the state. That arrangement gives



Print elect, which also represents ES&S in South Carolina and Virginia, a big advantage in getting printing jobs. The company prints ballots for 85 of the North Carolina's 100 counties, sometimes charging double what it costs to buy from a competitor not certified by ES&S." (*The News & Observer*, Biesecker, 08/11/2010) (\$3 Million Contract [Link](#))

**North Carolina Board of Elections Delayed Certification of ES&S Machines Until Security Concerns Regarding Company Ownership Disclosed.** "The State Board of Elections said cybersecurity worries prompted a delay in certifying election system vendors to sell voting machines to counties. In her first state board meeting Thursday, June 13, new Executive Director Karen Brinson Bell urged the board to require vendors seeking certification to disclose all ownership interests of 5% or greater. After a lengthy closed executive session, the board unanimously approved Bell's proposal... The board was scheduled to certify three voting machine vendors — Massachusetts-based Clear Ballot, Nebraska-headquartered Election Systems & Software, and Hart Intercivic of Texas." (*The Daily Courier*, Way, 6/20/2019)

**Deputy Director of Franklin County, Ohio Board of Elections Lied to Board, Failed to Disclose He Was Offered a Job By ES&S, and Failed His Wife was on Board of ES&S linked Group In order to Ensure \$12.3 Million ES&S Contract Signed.** Conflict-of-interest questions surrounding Michael R. Hackett Jr.'s relationship with owners of SST Systems, a New Albany company that supplies storage carts for voting machines, concerned board members for much of last year. Those worries appeared to be resolved on Nov. 23, when elections board Director Matthew Damschroder, a co-worker and close friend of Hackett's, told the board, "We've consulted with the county prosecutor and there are no conflicts of interest." The board then approved the SST contract. But County Prosecutor Ron O'Brien said last week that he never cleared Hackett of conflict questions. (*The Columbus Dispatch*, 5/14/2006)

**Ohio Election Official Joined Board of ES&S Linked Company Despite Ohio Ethics Board finding "Significant Issues" With the Arrangement.** "In fact, when an Ohio Ethics Commission lawyer took an initial look at the relationship, she said there were "significant issues" with the arrangement. Hackett did not respond to the lawyer's questions for almost four months, and then he retired without receiving an opinion from the commission... For three or four months last year, Hackett's wife, Mary, was a one-third partner in SST. The company was incorporated in January 2005 by Mrs. Hackett; John Fike, one of Mr. Hackett's childhood friends; and Richard Prohl. On Jan. 3, five weeks after he retired from the board, Mr. Hackett became a partner of Fike and Prohl's by forming an affiliate of SST. \* For months last year, SST Systems was negotiating a sales agreement with Election Systems & Software, a Nebraska-based company that was simultaneously seeking a contract to supply Franklin County's new voting machines." (*The Columbus Dispatch*, 5/14/2006)

**Former Florida Secretary of State Profited by Acting as ES&S Lobbyist and as the Lobbyist for State Counties To Receive Vendor Recommendations.** "A former Florida secretary of state profited by being a lobbyist for both the state's counties and the company that sold some of them touchscreen voting machines used in last month's botched primary election. Sandra Mortham, who served as the state's top elections official from 1995 to 1999, is a lobbyist for both Election Systems & Software and the Florida Association of Counties, which exclusively endorsed the company's touchscreen machines

in return for a commission...After the association's June 2001 endorsement, ES&S received orders totaling more than \$70.6 million from Florida counties. That includes Miami-Dade County's \$24.5 million purchase and Broward County's \$18 million contract. The association will receive about \$300,000 in commissions, according to the agreement." (*AP News*, 10/5/2002)

**After John Bel Edwards was Elected Governor of Louisiana, He Sided With ES&S and Successfully Blocked a \$95 Million Voting Machine Contract Awarded to Their Competitor.**

"Ardoin's office had announced Aug. 9 that it had selected Dominion to replace Louisiana's current stock of voting machines, which were last purchased in 2005...The \$95 million contract was held up a few weeks after it was awarded when one of the losing bidders, Election Systems & Software, the largest U.S. manufacturer of voting equipment, objected to the contracting process." (*State Scoop*, 10/11/2018)

**Between 2014-2018, ES&S Donated \$13,250 to Louisiana Governor John Bel Edwards (D).**

"Louisiana campaign finance records show that ES&S's lobbyist in Baton Rouge, William "Bud" Courson, has donated \$13,250 to Edwards' campaigns since 2014." (*State Scoop*, 10/11/2018)

**"Independent" Voting Machine Testing Labs Accepted Thousands of Dollars in Donations From ES&S.** "The private testing system of independent labs was created in 1994 by a group of election officials who were brought together by the National Association of State Election Directors (NASED)...In 2002, the Houston-based Election Center operated on a \$462,000 budget. Executive Director Doug Lewis said Election Center's budget comes mostly from membership dues and training fees. But he acknowledges accepting up to \$10,000 a year in donations from voting-equipment manufacturers like Sequoia Voting Systems and Election Systems & Software. That doesn't sit well with California's top election official. "Where I come from, any firm regulatory or approval scheme should be conducted by entities that are entirely independent from any reliance -- financial or otherwise -- from the people that they have to oversee," Shelley said." (*San Jose Mercury News*, Ackerman, 5/30/2004)

**SOUTH CAROLINA REPUBLICANS TO REASSESS VOTER MACHINE PROCUREMENT AFTER ES&S CORRUPTION UNCOVERED DURING PROCESS TO PICK VENDOR FOR \$60 MILLION STATE CONTRACT**

**South Carolina's Election Commission Executive Director, Marci Andino, Proposed \$60M ES&S Contract After Serving on ES&S Advisory Board and Receiving Over \$19,000 Worth of Flights, Hotels Meals, and Conferences From ES&S.** "The relationship between South Carolina's director of elections and the country's largest voting equipment company has caught the attention of lawmakers as the state prepares to spend a proposed \$60 million to replace 13,000 voting machines. For more than a decade, Marci Andino, executive director of the S.C. Election Commission, served on an advisory board formed by Elections Systems and Software, known commonly as ES&S. Andino received more than \$19,000 worth of flights, hotels and meals from ES&S since 2009 to attend regular conferences at the company's headquarters in Nebraska and other cities across the country, according to records with the South Carolina Ethics Commission." (*Post & Courier*, 1/29/2019)

**S.C. Republican Lawmaker Said Conduct by ED of Election Commission May Give the Appearance of a Conflict and Urged Director to Avoid All Involvement in Solicitation Process.**

“Some of the lawmakers advocating for a new voting system in South Carolina worry Andino’s connection to ES&S could cause the public to question that relationship, especially if the company is awarded another state contract. “I think if we’re not careful it gives the appearance — and underline that, the ‘appearance’ — of a conflict,” Rep. Kirkman Finlay, R-Columbia, said. “The director should avoid any and all involvement in the solicitation of bids.” ([Post & Courier](#), 1/29/2019)

**S.C. Republicans Called for More Oversight and Transparency In the Bidding Process for Voting Machines, Move to Reassess Procurement Process, After Conflict of Interests Arise.**

“But lawmakers are working on a joint resolution to give the State Fiscal Accountability Authority — made up of top S.C. elected officials — the authority to approve or veto that decision. We feel like there needs to be some more oversight and the process needs to be a little bit more open,” said state Rep. Kirkman Finlay, a Columbia Republican on the House Ways and Means Committee. “A lot of vendors, a lot of individuals, a lot of groups have contacted us and felt it was moving a little too quickly. With something like voting machines, we need to make sure everybody is included and everybody gets a shot at it.” ([The State](#), 2/21/2019)

**S.C. Chooses to Limit the Election Commission’s Authority to Buy New Voting Machines Amid Concerns Over the Commission Director’s Relationship with ES&S.** “S.C. lawmakers are working to limit the State Election Commission’s authority to buy new voting machines, amid concerns over the projected cost and the commission director’s longtime relationship with a possible vendor [ES&S]. ([The State](#), 2/21/2019)

**South Carolina Approves \$51 Million Contract for ES&S Despite Long History of Pay-For-Play with Election Officials.** “State officials on Monday announced that a \$51 million contract had been awarded to Election Systems and Software, the nation’s largest voting equipment vendor, to provide the new voting machines which promise more security in producing a paper ballot...The company also has ties to elections officials in South Carolina and other states, an investigation by McClatchy and The State revealed...For at least nine years, ES&S invited dozens of state and local elections officials to serve on an “advisory board” that gathers twice annually for company-sponsored conferences, including at a ritzy Las Vegas resort hotel, a McClatchy investigation found. Andino was among the attendees. The State reported last June that the company had covered \$19,200 in expenses associated with those trips for Andino during her decade as an adviser for ES&S.” (*The State*, Barton, 6/10/2019)

**South Carolina League of Women Voters Criticized Decision, Said Hand Marked Paper Ballots Cost Half as Much as ES&S Machines and Are More Secure.** “Critics of the Election Commission, including the League, say the state could move toward hand-marked ballots that can’t be hacked at half the projected cost -- about \$25 million. Teague contends poorly designed ES&S software has led to problems in the past, including miscounted votes, according to League audits of South Carolina elections. She also argued hand-marked ballots have worked well in other states, and problems reading them have been exaggerated. “We are paying extra money for something that produces extra problems,” she said. (*The State*, Barton, 6/10/2019)



**PENNSYLVANIA STATE AUDITOR WARNED OF NATIONWIDE ES&S VENDOR CORRUPTION “IF IT’S HAPPENING HERE, IT MUST BE HAPPENING ELSEWHERE.”**

**Pennsylvania State Auditor Warned Auditors Nationwide to Review Potential ES&S Corruption.**

“Even if this activity was permitted under the law, county officials who are making decisions about spending taxpayer dollars should not accept anything of value from the companies that are asking for their business,” DePasquale said... Costs are expected to range from \$125 million to \$150 million...DePasquale is urging auditors general nationwide to conduct similar reviews of elections-related gifts. “If it’s happening here, it must be happening elsewhere,” he said. ([TribLive](#), 2/22/2019)

**Pennsylvania State Auditor Called For Stronger Ethics Rules to Prevent County Officials From Benefiting from Voting Machine Vendor Corruption.** “DePasquale called for updating disclosure laws and strengthening state ethics rules to encompass more public officials. He said it doesn’t matter if the gifts were large or small. He took issue with the fact that people accepted them. “Even if this activity was permitted under the law, county officials who are making decisions about spending taxpayer dollars should not accept anything of value from the companies that are asking for their business,” DePasquale said.” ([TribLive](#), 2/22/2019)

**Pennsylvania State Auditor Cited Several Counties For Accepting Gifts From ES&S That “Smacks Of Impropriety.”** Elections officials in Western Pennsylvania say they’re rethinking accepting even small gifts like coffee and doughnuts from potential vendors after state Auditor General Eugene DePasquale flagged counties around the state for behavior that “smacks of impropriety.” Westmoreland, Butler and Washington counties were among those cited for accepting gifts from voting machine vendors since 2016. ([TribLive](#), 2/22/2019)

**Pennsylvania State Auditor Was Concerned When ES&S Offered Flights to Las Vegas, Tickets to Wine Festivals, Admission to Amusement Parks, Dinners at High End Restaurants, and Open Bars at Conferences to Public Officials in 27% of Pennsylvania Counties.** “Flights to Las Vegas, tickets to wine festivals, admission to an amusement park, dinners at high-end restaurants and open bars at conferences were among gifts that companies provided to public officials in 18 of Pennsylvania’s 67 counties, DePasquale said in a report released Friday. “As Pennsylvania counties choose new voting equipment, I want them to make decisions based on the best interest of voters — and no other factors,” DePasquale said.” ([TribLive](#), 2/22/2019)

**Philadelphia City Controller Refused to Approve Payment for ES&S Voting Machines Amid Process and Legal Concerns.** “Philadelphia City Controller Rebecca Rhynhart says she will not approve payment for new voting machines that will cost the city tens of millions of dollars. “I’m deeply concerned about the legality of this process,” she said in a statement Tuesday night, “and as city controller, I will not release \$1 of payment while these questions go unanswered.” ([The Inquirer](#), 5/1/2019)

**Philadelphia Controller is Investigating Accusations Voting Machine Selection Process Biased to Favor Electronic Voting Machines Over Paper Ballots.** “Until her office completes an investigation of the voting-machine selection process, including accusations that it was biased to favor electronic voting machines over paper ones that voters fill out manually, Rhynhart said she won’t sign

off on payment. Her approval is one of several that are required along the way when the city purchases new equipment or services.” ([The Inquirer](#), 5/1/2019)

**Philadelphia Commission Approved ES&S Machines Despite Fierce Criticism from Controller, Auditor General and Hand-Marked Paper Ballot Supporters.** “The Philadelphia city commissioners chose a new voting machine system Wednesday to be used starting in November, despite criticism of the process from the city controller, the state auditor general, and a group of advocates who want hand-marked paper ballots.” ([The Inquirer](#), 2/20/19)

**Unnamed City Employees Selected ES&S Through a “Fast-Track and Secret Selection Process.”** “New voting machines were selected Feb. 20 by two of the three current commissioners, Lisa Deeley and Al Schmidt, after a fast-tracked and secret selection process in which a committee of unnamed city employees evaluated proposals from vendors and made recommendations to the commissioners. Deeley has defended that process as intentionally rushed to meet Gov. Tom Wolf’s directive to purchase new machines by next year and intentionally secretive to protect it from outside influence, in accordance with city rules.” ([The Inquirer](#), 5/1/2019)

**Commissioner Anthony Clark Voted Against the Proposal Because He Was Denied All Information Pertaining to the Selection Process as it Occurred.** “Later, he called The Inquirer to reiterate his position. He said that since he had not signed a confidentiality form that would have allowed him to receive information on the selection as it was occurring, he was essentially left out of the process. He added that he learned about the machines only at the public meetings and as advocates criticized the system. “I didn’t have enough information,” Clark said. “I didn’t even know what options were available, because I didn’t sign the confidentiality [form] and no information was coming to me.” ([The Inquirer](#), 4/10/19)

**Pennsylvania Councilwoman Called For ES&S to be Removed from Consideration of \$4M Contract Following Pay-For-Play Controversy.** “Luzerne County Councilwoman Linda McClosky Houck has called for a potential vendor of planned new voting machines to be removed from the process, based on the company’s ties to the county election director...The company, known as ES&S, became embroiled in controversy in December when it came to light that county election director Marisa Crispell had served on the ES&S advisory board in 2017, and attended advisory board meetings for which the company paid her travel expenses. The county plans to purchase new paper-trail voting machines this year, to comply with a directive from state officials. The new voting system will cost about \$4 million, county officials said. (*The Citizen’s Voice*, Mark, 6/19/2019)

**Pennsylvania Officials Say “Almost Impossible” for Voting Machines to be in Place for November Elections Given Training Required.** “McGinley said he hopes the committee will forward its recommendation to council this summer. However, it is not likely the new voting machines will be in place for the November election, as officials had hoped, according to county Manager David Pedri. Even if the machines arrive in time, the amount of training required for election officials, poll workers and voters would make that almost impossible, Pedri said.” (*The Citizen’s Voice*, Mark, 6/19/2019)

**Pennsylvania Governor Announced \$90 Million Bond Issue to Fund State Mandated Voting Machines.** “Pennsylvania Gov. Tom Wolf announced a \$90 million bond issue Tuesday to fund a statewide voting machine upgrade effort that he ordered more than a year ago to ensure that every

vote cast creates a paper trail that can be checked by voters and audited ... The statewide voting machine upgrade requires all counties to use new systems with paper trails that voters can verify in plain text before casting their votes, allowing for audits and manual recounts. While some counties have used paper-based systems for years, **most Pennsylvania voters have used insecure systems that store votes electronically.**" ([The Philadelphia Inquirer](#), 7/9/2019)

**ES&S LIED TO FEDERAL LAWMAKERS REGARDING DATA SECURITY AND CONSISTENTLY DEMONSTRATED A DANGEROUS LACK OF COMPETENCE IN CREATING SECURE AND RELIABLE MACHINES. "CRIMINALLY NEGLIGENT" SOFTWARE CAUSED ELECTION ALTERING UNDERVOTES, EXPOSED PERSONAL DATA OF MILLIONS, AND VIOLATED STATE LAWS.**

ES&S MACHINES ARE DIRECTLY TIED TO SIGNIFICANT UNDERVOTES AT EVERY LEVEL IN GEORGIA, FLORIDA, TEXAS, ARIZONA, PENNSYLVANIA, AND NORTH CAROLINA

**Georgia's ES&S Unreliable Machines Led to an Undervote In the Lieutenant Governor's Race of over 60,000 votes (2018).** "The conduct of the election "was so defective and marred by material irregularities as to place in doubt the result of the election under Georgia law. This court should therefore declare the contested election invalid and set the date for a second election between the same candidates," the lawsuit states... "Citizens must not permit flawed elections to stand," said Bruce Brown, an Atlanta-based attorney representing the plaintiffs... **The lawsuit notes the lieutenant governor's race reported only 3,780,034 votes, while every other statewide race tally exceeded 3.843 million votes.** The plaintiffs allege that "this high under-vote rate is a likely result of the touchscreen voting system malfunctions, and that the un-auditable system does not permit a reliable determination of the vote count." ([AP News](#), 11/24/2018) (Note: GA signed a [\\$54 million voting machines deal](#) with Diebold Election Systems in 2002, Diebold sold Election System [business to ES&S](#) after Antitrust lawsuit in 2009.)

**In 2015, Georgia Officials Said State Protocol Required Every Precinct in Every County to Compare Tabulated Results with Physical Poll Tape to Avoid ES&S Software Bug that Causes Undervote.** "Some counties in Virginia and Georgia still use the problem software, as well. But they employ special protocols to make sure that votes aren't dropped, officials in both states say. In Georgia, that includes comparing tabulated precinct results with each physical poll tape—essentially replicating Smith's experiment, but for every precinct in every county." ([Bloomberg](#), 9/29/2016)

**ES&S General Election Software "Dropped" Over 1000 Votes from Black Precincts in Memphis—Some Were Incorrectly Labeled "Double Votes" By the System.** "Not all of the precincts are named in the e-mail, but **a master record for the voting machines shows missing uploads at four polling places on election night, all in areas with large concentrations of black voters.** Three are **located at black churches.**... The weird thing is, the GEMS system recognized at least some of the missing votes—stored on the memory cards of seven voting machines—as already counted when officials tried to reload them on Oct. 19, according to an e-mail exchange between Young and operations manager Darral Brown. But it was clear from Smith's poll tape and other data dug up by

Young that they hadn't been. In all, 1,001 votes had been dropped from the election night count, according to the master record, including almost 400 from an early voting center at Mt. Zion, the most from any single polling place." ([Bloomberg](#), 9/29/2016)

**2015 Memphis Undervote Caused by Software Bug ES&S [Diebold] Aware of Since 2008.** "Among the documents released to Chumney is a user's manual for the county's version of GEMS. It shows they're using a version of the software that contains the bug known to drop votes, the subject of that 10-month investigation in Ohio in 2008. The software flaw creates exactly the situation described in the e-mails by Young and other officials, one that has been well-known for eight years. Diebold didn't replace the flawed versions outside of Ohio, and for counties to do so on their own was expensive." ([Bloomberg](#), 9/29/2016)

**In 2008, ES&S [Diebold] Lied to Ohio Secretary of State About Software Bug That Caused Primary Undervote in 11 Counties.** "Ohio Secretary of State Jennifer Brunner sued Diebold following the 2008 primaries after 11 counties using the company's AccuVote-TSX voting machines and GEMS tabulator dropped votes. The company claimed the problem was the result of the antivirus program the counties were using. After a 10-month fight, Diebold conceded the lost votes were the result of a software bug. The bug was fixed in later versions, and more than half of Ohio counties received free or discounted voting machines and software as part of the settlement." ([Bloomberg](#), 9/29/2016)

**In Florida, a Major Congressional Race in Florida Imploded After 18,000 Votes From Paperless ES&S iVotronic Machines Went Missing in a Race Decided By Less Than 400 Votes (2006).** "But the tipping point came in 2006, when a major congressional race between Vern Buchanan and Christine Jennings in Florida's 13 th District imploded over the vote counts in Sarasota County—where 18,000 votes from paperless machines essentially went missing (technically deemed an "undervote") in a race decided by less than 400 votes. Felten drew an immediate connection to the primary suspect: The ES&S iVotronic machine..." ([Politico](#), 8/5/2016)

**A 2002 ES&S Software Error Caused 103,222 Votes to Not Be Counted in The Original Tally in Broward County, Florida.** "CNN reported that a software error caused 103,222 votes, cast with ES&S iVotronic paperless machines, to be left uncounted in the original tally. The error was discovered the morning after Election Day. When the missing votes were added, voter turnout for the county was adjusted from 35% to 45%." ([Brennan Center For Justice](#), 2010)

**In 2007, Florida's ES&S Machines Were Responsible for a 5% Undervote of Absentee Ballots in the US Senate and US Governor's Race.** "In 2007, the Florida Division of Elections listed Orange County as experiencing the highest undervote rates in the state on absentee ballots cast in the 2006 general election for both the U.S. Senate race and the state Governor's race. Alarmed by the exceptionally high rate of undervoted ballots in a major election – nearly 5 percent – the Florida Fair Elections Center's Associate Director contacted the Orange County Elections Administrator, who promised to investigate the issue. According to the Center, Orange County officials responded to the inquiry by stating that their manual inspection of the ballots confirmed that some legitimately cast ballots had not been counted... Bill Cowles, Supervisor of Elections for Orange County noted in an interview with us that the county switched to a different model of ES&S scanner after the 2006 general election." ([Brennan Center For Justice](#), 2010)

**An ES&S Software Glitch Led to 32,000 Votes to Not Be Counted on Certain Florida State Amendments.** “Two days after Election Day in November 2004, Broward County election officials double-checked election results and discovered that tens of thousands of votes on certain state amendments were not counted. The problem: a “software glitch” in the system used to count the county’s absentee ballots.<sup>91</sup> According to the Palm Beach Post, the software started counting backward after it logged 32,000 votes in a race. Once officials identified the problem and obtained correct vote totals, the newfound votes contributed to a changed result for a statewide gambling amendment and sparked angry calls for a recount.” ([Brennan Center For Justice](#), 2010)

**ES&S Machines Led to Nearly 3000 Votes Disappearing in Florida 2018 Recount.** “Nearly 3,000 votes effectively disappeared during the machine recount of Florida’s midterm races, according to election records, calling into question whether officials relied on a flawed process to settle the outcome of three statewide contests. With extremely narrow gaps separating candidates in the still-undeclared races for both governor and United States Senate, the results of the machine recount of all votes cast in the Nov. 6 election, posted by the Florida secretary of state’s office, showed 900 fewer votes than those reported in the original statewide tally. The discrepancy was expected to grow by an additional 2,000 votes when updated numbers from Broward County [are added]...Teresa Paulsen, spokeswoman for ES & S, the other company, said machine recounts depend on the same number of ballots being entered into the system. Some ballots could have been torn or damaged after the election, which could have cause a different result in the recount, she said.” ([New York Times](#), 11/17/2018)

**In Dallas County, Texas ES&S Machines Failed to Count 41,000 Votes Do to Software Error (1998).** “In its maiden run almost two years ago, Dallas County’s new \$ 3.8 million computerized election system overlooked 41,000 votes, one of every eight cast. A software error made it think the votes had already been counted. Thirty elections later, in the March 14 primaries, the county released “final” totals that left out 11,000 votes...“We are concerned that it failed to operate properly in Dallas,” said Ann McGeehan, the state’s director of elections. “This election-reporting system is very clunky.” (*The Dallas Morning News*, Gillman, 4/1/2000)

**In the 2008 Presidential Primary, an ES&S Software Error Resulted in Romney Incorrectly Being Declared Winner of Cochise County, Arizona and More Votes Cast than People Registered.** “The Douglas Dispatch reported that, in Cochise County, during the 2008 primary presidential race, “a computer glitch that kept counting five polling places over and over again-for five times-caused [a] reporting error” of the election’s results...Consequently, the error resulted in Mitt Romney erroneously being declared winner of Cochise County over John McCain in news reports on the day after the election...Moreover, “the error got worse when the cumulative error went through five updates. It was then realized that the total number of ballots cast according to the wrong report was more than the people registered in the county, Schelling said.” ([Brennan Center For Justice](#), 2010)

**ES&S Coding Error Resulted in 2,452 Votes Not Counted in Lackawanna County, Pennsylvania (2009).** “The good news is, with paper, we have the ballots.” The large-scale recount was forced by the disclosure last week of a coding error in the county’s computerized vote counters. The error cost city tax collector candidate Bill Courtright and city Councilwoman Janet Evans up to 2,452 straight-party votes. The revelation prompted a flurry of requests for recounts, based partly on fears the error was more widespread, despite Director of Elections Maryann Spellman Young’s assurances to the contrary... Omaha, Neb.-based Election Systems & Software, the machine provider, will lend the



county a new, high-speed vote counter... Party secretary Lance Stange said he is skeptical about the new, high-speed machine recount because Election Systems & Software is providing the machine. "It's from the same company that made the earlier error," he said." (*The Times-Tribune*, Krawczeniuk, 11/13/2009)

**ES&S Software Error Caused 94,000 Votes to be Counted Late in North Carolina, Resulting in a Late-Night Lead Change and Complaints Regarding Accuracy (2016).** "Similarly, this round of upgrades comes on the heels of concerns regarding the technology used in the 2016 election. In North Carolina, *Durham County* faced difficulties transferring data off of the memory cards in its vote scanning machine bought from Election Systems & Software. The glitch, the result of memory limitations in the counting software, caused a late-night lead change in the gubernatorial race from then-incumbent Pat McCrory to challenger and eventual victor Roy Cooper, despite the state's website reporting that the county had already completed tallying its votes." (*The News & Observer*, Lewontin, 8/2/2018) (94,000 votes [citation](#))

**ES&S Software Error Resulted in 436 Ballots In North Carolina Not Counted (2002).** "Problems with voting machines in elections were also making headlines. In 2002 in North Carolina, for example, D.R.E.s made by ES&S failed to record 436 entire ballots during early voting in *Wake County*, a failure the company attributed to a software bug. Two years later, in *Jacksonville, N.C.*, a D.R.E. made by UniLect lost more than 4,500 ballots when its memory became full and stopped recording; it continued to let voters cast ballots, however, instead of locking up. The incidents that made headlines were disturbing enough, but the real concerns were the ones that weren't being caught." ([New York Times](#), 9/26/2018)

OHIO ES&S SOFTWARE CALLED "HIGHLY DANGEROUS," "CRIMINALLY NEGLIGENT FROM THE STANDPOINT OF DATA SECURITY" AND "INSANELY RISKY" BY ELECTION SECURITY EXPERTS

**Attorney Cliff Arnebeck Called the Installation of ES&S Software in Ohio Machines a "Flagrant Violation of the law."** His attorney, Cliff Arnebeck, has also referred the case to the Cincinnati FBI for a criminal investigation. Arnebeck says, "It's a flagrant violation of the law. Before you add new software, you need approval of a state board. They are installing an uncertified, suspect software patch that interfaces between the a county's vote tabulation equipment and state tabulators." He adds, "This may be criminal conduct. If they're not doing something wrong, why are they covering it up?" ([Huffington Post](#), 1/23/2014)

**In 2014, Free Press Editor-In-Chief Robert Fittrakis Filed a Lawsuit Against ES&S and the Ohio Secretary of State To Halt the Use of Secretly Installed, Unauthorized "Experimental" Voting Machine Software.** "Those worries about a rigged election were given new urgency today as The Ohio-based Free Press editor-in-chief Robert Fittrakis, also a Green Party candidate for Congress, announced plans to file a lawsuit later today seeking an immediate injunction against Ohio Secretary of State Jon Husted and the ES&S manufacturer to halt the use of secretly installed, unauthorized "experimental" software in 39 counties' tabulators in an alleged violation of state election law." ([Huffington Post](#), 1/23/2014)

**In Sworn Declaration, Election Security Expert Jim March Called ES&S Custom Software Update in Ohio Voting Machines “Highly Dangerous.”** “For a number of reasons, I believe that this custom software is not necessary for the conduct of elections and is in fact highly dangerous – the presence of this software significantly reduces the odds that the election results (on a county or statewide level) will be illegally and/or unconstitutionally incorrect. My analysis follows.” ([PDF](#), 11/03/2012)

**Election Security Expert Jim March Called ES&S Software “Extremely Dangerous” and Said Deliberate Tampering of Software Would Be “Child’s Play.”** “9) What ES&S has chosen to do here is extremely dangerous and exactly what you'd want to do if you wanted to plant a “cheat” onto the central tabulator. Their custom application written in a variant of the COBOL programming language would have full contact with the central tabulator database on both a read and write basis, while running on the same computer as where the “master vote records” are stored. 10) Under this structure a case of accidental damage to the “crown jewels” of the election data is possible. A case of deliberate tampering of that data using uncertified, untested software would be child's play.” ([PDF](#), 11/03/2012)

**ES&S Called “Criminally Negligent From a Standpoint of Data Security” by Election Security Expert Jim March in Sworn Declaration.** “What they have done instead is criminally negligent just from a standpoint of data security. To double-check the results after this new system is implemented you'd have to go back to the original paper and/or any remaining “poll tapes” from the precincts (“cash register” type paper strips containing that precinct's vote totals). “Poll tapes” from the mail-in vote process may not even exist – most systems feed mail-in votes from scanners straight into the central tabulator with no independent record of the vote. In either case there would need to be public records access to either the poll tapes...or the original paper ballots. There has been widespread media complaints about the access to either sort of public records in Ohio.” ([PDF](#), 11/03/2012)

**Election Security Expert Jim March Says ES&S Chosen Methods of Data Collection Are “Unspeakably Stupid, Excessively Complex and Insanely Risky.”** “In conclusion, the idea of producing industry-standard .CSV data files of election results is not inherently bad. The method of execution chosen however is unspeakably stupid, excessively complex and insanely risky. In medical terms it is the equivalent of doing open heart surgery as part of a method of removing somebody's hemorrhoids. Whoever came up with this idea is either the dumbest Information Technology “professional” in the US or has criminal intent against the Ohio election process and if I were to guess it would be the latter.” ([PDF](#), 11/03/2012)

**Ahead of 2019 Elections, ES&S Has Failed to Install Software Patch Needed for Voting Machines Across Ohio Counties.** “[ES&S] which currently supplies the sign-in equipment voters use at their polling location, has said it would provide a software update to make the equipment compatible with recently ordered voting machines. But ES&S has been behind on compliance of its pledge, which has put some election boards across the state in a bind...getting it installed and being trained on operation, the [Hancock County] board’s motion Monday requires a decision from ES&S and the Secretary of State’s office on systems compatibility by July 12...If a decision hasn’t been received, the board authorized contacting Knowlnk, a St. Louis, Missouri-based company, to provide the “poll pad” equipment.” ([The Courier](#), 6/25/2019)

**In 2005, ES&S Surprised Small Ohio County With \$40,000 Per Year Service Fee for Election Software Written in 1996.**

“When Allen County, Ohio, replaced its old voting machines in 2005 with equipment from ES&S, officials didn’t realize they’d also be stuck with a service fee of \$40,000 per year to help run an election system that handled about 70,000 votes. “When we found out the cost, our jaws just about hit the floor,” says Ken Terry, who was election director there until this year. To top it off, Terry discovered that the county was paying top dollar for antiquated technology. It wasn’t until the machines were purchased, and in place, that county officials realized their new system ran on software written in 1996.” ([Bloomberg](#), 9/29/2016)

**ES&S HAS CONSISTENTLY DEMONSTRATED A SYSTEMATIC DISREGARD FOR BASIC SECURITY BEST PRACTICES AND A COMPLETE LACK OF COMPETENCE IN THE MANUFACTURING OF RELIABLE VOTING MACHINES**

**In May 2019, A Critical Firewall Vulnerability that Allowed Attackers to “Fully Compromise” Device Networks, Was Found in ES&S Voting Machines.** “The first is a bug in Cisco’s IOS operating system—not to be confused with Apple’s iOS—which would allow a hacker to remotely obtain root access to the devices. This is a bad vulnerability, but not unusual, especially for routers.... The second vulnerability, though, is much more sinister. Once the researchers gain root access, they can bypass the router’s most fundamental security protection...In practice, this means an attacker could use these techniques to fully compromise the networks these devices are on...“That means we can make arbitrary changes to a Cisco router, and the Trust Anchor will still report that the device is trustworthy. Which is scary and bad, because this is in every important Cisco product. Everything.” ([Wired](#), 5/13/19)

**Cisco Security Advisory Lists Firewall “ASA 5506-X” as First Affected Product.** ([Ciscos.com](#), 5/13/2019)

**The ES&S Firewall Systems “ASA-5506-X”, Made by Cisco, Was Used by ES&S in Michigan<sup>1</sup>, Florida<sup>2</sup>, and Iowa<sup>3</sup>.** (<sup>1</sup>[MI Contract](#), 3/1/2017) (<sup>2</sup>[FL Certification](#), 2/9/2012) (<sup>3</sup>[State of Iowa](#), 9/18/18)

*Did ES&S Properly Warn States and Counties that their Voting Machines Could Be “Fully Compromised?” Has ES&S Installed the Recommended Software Patch in Every Single Affected Voting Machine?*

**Nearly Every Make and Model of Voting Machine Created in the Last 15 Years Is Vulnerable to Hacking.** It was just another example of something that Eckhardt and other experts had suspected for many years: that many critical election systems in the United States are poorly secured and protected against malicious attacks. In the 15 years since electronic voting machines were first adopted by many states, numerous reports by computer scientists have shown nearly every make and model to be vulnerable to hacking. ([New York Times](#), 2/21/2018)

**As of September 2018, ES&S Failed to Fix Massive Security Flaw in Scanners Originally Discovered 11 Years Ago—Still Selling Scanners on Website.** An uncorrected security flaw in a vote-counting machine used in 23 U.S. states leaves it vulnerable to hacking 11 years after the manufacturer was alerted to it, security researchers say. The M650 high-speed ballot scanner is made



by Election Systems & Software, the nation's leading elections equipment vendor. The vulnerability was the most serious noted in voting equipment **in a report Thursday...** "If successfully hacked by someone intent on changing vote totals in a swing-state county, "it could flip the Electoral College," [Jake Braun] said... **ES&S did not respond when asked by The Associated Press why it had not corrected the Zip drive vulnerability** despite knowing about it for more than a decade. It also did not say whether it **continues to sell the M650, which was listed on its website product offerings as recently as last month.**" (*St. Louis Post-Dispatch*, Bajak, 11/28/2018)

**Election Expert on ES&S 'What I've seen in the past 10 years is that the vendors have absolutely fumbled every single attempt in security.'** "What I've seen in the past 10 years is that the vendors have absolutely fumbled every single attempt in security," **says Jacob D. Stauffer, vice president of operations for Coherent Cyber, who** has conducted voting-machine security assessments for California's secretary of state for a decade. In a report Stauffer and colleagues published last year about their recent assessment of ES&S machines, they found the voting machines and election-management systems to be rife with security problems." ([New York Times](#), 2/21/2018)

**ES&S's New Barcode-Ballot Producing Machines Called "A Ruse" that "Makes a Mockery of Notion that the Ballot is 'Voter-Verifiable.'** "The new machines being peddled by companies like Election Security & Software (ES&S), the nation's biggest vendor of voting technology, are designed to give the impression of being "voter-verifiable." **But it's a ruse. The machines produce a so-called "paper ballot," which voters can use to verify a text printout of their votes if they take the time. But it's not the text the voter is reading and reviewing, but the barcode beneath, that is actually tallied electronically as their vote...** Elections officials can't, either. The barcode-based setup "makes a mockery of the notion that the ballot is 'voter-verifiable,'" agreed Duncan Buell, a computer science professor at the University of South Carolina, because **"what the voter verifies is not what is tallied."** ([The New Republic](#), 3/06/2019)

**University of Iowa Computer Scientist Slammed ES&S For "Mediocre Programming," "Insufficient Pre-Election Testing," and a Complete Lack of "Security Conscious" in Any Phase of Their Design.** "University of Iowa computer scientist **Douglas Jones** said **both incidents** reveal mediocre programming and insufficient pre-election testing. And voting equipment vendors have never seemed security conscious "in any phase of their design," he said." ([AP News](#), 10/29/2018)

**ES&S Sold 22,619 Faulty Voting Machines That Lose Calibration Throughout Election Day Causing "Vote Flipping."** "There is a real chance that voters using iVotronic machines in your state will experience 'vote flipping' similar to that experienced by voters in West Virginia," the letter said. "What they've seen is **calibration drift on a unit,**" Merriman said. **"They're fine in the morning, but by afternoon they're starting to lose their calibration."** The phenomenon is described in a federal lawsuit filed in November 2005 by Bergquist Co., which makes touch screens for ES&S...It described how air pockets between layers of the screen and residual acid in an ink compound were causing the touchscreens to malfunction..." "Ultimately, Bergquist determined that the dielectric ink, which had caused the sudden 'out-of-calibration' problems, had been used in 22,619 **touch screens sold by Pivot** and incorporated in voting machines, and thus every screen had failed and required replacement." ([Salina Journal](#), 4/10/2009)

**2018 Report Commissioned by California Secretary of State Found 115 Critical and Important Software Patches to Be Missing and 176 Instances of Server Misconfigurations on ES&S Machines.** Please See Appendix A. ([ES&S Security Test Report](#), 8/28/2017)

**ES&S Misconfigured Windows 7 Software 96 Times on Machines They Chose to Provide to California Secretary of State for Security Testing.** Please See Appendix A. ([ES&S Security Test Report](#), 8/28/2017)

**The AP Said ES&S Faced No Significant Oversight and Operated Under a Shroud of Financial and Operational Secrecy.** “A trio of companies — ES&S of Omaha, Nebraska; Dominion Voting Systems of Denver and Hart InterCivic of Austin, Texas — sell and service more than 90 percent of the machinery on which votes are cast and results tabulated. Experts say they have long skimmed on security in favor of convenience, making it more difficult to detect intrusions such as occurred in Russia’s 2016 election meddling. The businesses also face no significant federal oversight and operate under a shroud of financial and operational secrecy despite their pivotal role underpinning American democracy.” ([AP News](#), 10/29/2018)

**In 2017, Rigorous Scrutiny of Voting Systems Found Multiple Vulnerabilities in ES&S’s Electionware System That Could Allow Intruders to Erase All Recorded Votes.** “California conducts some of the most rigorous scrutiny of voting systems in the U.S. and has repeatedly found chronic problems with the most popular voting systems. Last year, a state security contractor found multiple vulnerabilities in ES&S’s Electionware system that could, for instance, allow an intruder to erase all recorded votes at the close of voting. ([AP News](#), 10/29/2018)

**Security Researchers Discovered Critical Vulnerabilities In ES&S Software That Would Allow Attackers to Seize Control of System.** “Around this same time, security researchers discovered a critical vulnerability in pcAnywhere that would allow an attacker to seize control of a system that had the software installed on it, without needing to authenticate themselves to the system with a password. And other researchers with the security firm Rapid7 scanned the internet for any computers that were online and had pcAnywhere installed on them and found nearly 150,000 were configured in a way that would allow direct access to them. It’s not clear if election officials who had pcAnywhere installed on their systems, ever patched this and other security flaws that were in the software.” ([MotherBoard](#), 7/17/2018)

**ES&S Installed Third Party Software On Its Election System During the Same Time Period That Software Was Hacked.** “In 2006, the same period when ES&S says it was still installing pcAnywhere on election systems, hackers stole the source code for the pcAnywhere software, though the public didn’t learn of this until years later in 2012 when a hacker posted some of the source code online, forcing Symantec, the distributor of pcAnywhere, to admit that it had been stolen years earlier. Source code is invaluable to hackers because it allows them to examine the code to find security flaws they can exploit.” ([MotherBoard](#), 7/17/2018)

**ES&S Used Easily Hackable Cell Phone Modems to Upload Election Night Results.** “The ES&S model DS200 optical-scan voting machine has a cell-phone modem that it uses to upload election-night results from the voting machine to the “county central” canvassing computer. We know it’s a bad idea

to connect voting machines (and canvassing computers) to the Internet, because this allows their vulnerabilities to be exploited by hackers anywhere in the world...So, in summary: phone calls are not unconnected to the Internet; the hacking of phone calls is easy (police departments with Stingray devices do it all the time); and even between the cell-towers (or land-line stations), your calls go over parts of the Internet.” ([Freedom to Tinker](#), 2/22/2018)

**Despite Hackers Ability to Change Votes In ES&S Machines, ES&S Has No Way to Audit Its Own Firmware, So Corrupt Firmware Would Remain Indefinitely.** “In all three cases, the practical implication of this attack would be to allow attackers to change votes and hence election outcomes. This attack is potentially persistent, because unless iVotronic machines are audited before future elections, it is plausible that the firmware will remain on the iVotronic system indefinitely. According to the EVEREST report, ES&S has no way to audit its own firmware, so this means that persistently corrupted firmware is the rule, not the exception.” ([David Cahn – University of Pennsylvania](#), 4/26/2017)

**The 30,000 ES&S Optical Scanners Across 43 States Are “Naively Designed” and Allow For Attacks That Could Infect Central Unity Systems Used To Count Votes Countywide.** “ES&S M100 Optical Scan voting machines are paper ballot tabulators. 30,000 M100 Optical Scan machines are used to count votes in 43 states. Due to their design, the attack surface for these machines is smaller than that of touch screen voting systems. Since there is no user interface, regular voters might find it difficult to attack the M100. Not so for poll workers; M100 machines are naively designed, allowing for malware and firmware attacks that could, at best, alter the voting results for a single precinct, and at worst infect the central Unity system used to count countywide votes. ([David Cahn – University of Pennsylvania](#), 4/26/2017)

**ES&S Did Not Hire A Data Security Officer Until April of 2018.** “ES&S hired its first chief information security officer in April. None of the big three vendors would say how many cybersecurity experts they employ. Stimson said that “employee confidentiality and security protections outweigh any potential disclosure.” ([AP News](#), 10/29/2018)

**An Election Specialist Said the ES&S Breach “Raises A Lot of Questions About Their Ability To Keep Both the Voting Systems They Run and Their Own Networks Secure.”** “The implications of the exposure are much broader than Chicago because Election Systems & Software is the largest vendor of voting systems in the United States, said Susan Greenhalgh, an election specialist with Verified Voting, a non-partisan election integrity non-profit. “If the breach in Chicago is an indicator of ES&S's security competence, it raises a lot of questions about their ability to keep both the voting systems they run and their own networks secure,” she said.” ([USA Today](#), 08/18/2017)

**Election Technology Expert Said It Would Be “Unprofitable” For ES&S to Build Truly Secure Systems.** “In much of the nation, especially where tech expertise and budgets are thin, the companies effectively run elections either directly or through subcontractors. “They cobble things together as well as they can,” University of Connecticut election-technology expert Alexander Schwartzman said of the industry leaders. Building truly secure systems would likely make them unprofitable, he said.” ([AP News](#), 10/29/2018)

**ES&S Passed ProCircular Testing Yet Barred Company from Releasing Any Details.** “ProCircular’s team spent several weeks conducting penetration testing on the hardware,

software, and way the device performed. The firm found the [ES&S] devices to be, in their words, “reliable and secure.”... ProCircular did not release further details on the report due to a confidentiality agreement with ES&S. Such agreements are standard when a company undergoes a penetration test.” ([Cyberscoop](#), 4/24/2019)

**Cybersecurity Reporter, Eric Geller, Called the Brief Statement by ProCircular, Published Without Data, “The Exact Opposite of What Independent Experts Have Been Recommending for Decades.** “Does ES&S actually think a brief statement from a company that can’t publish its test results will reassure anyone? This is the exact opposite of what independent experts have been recommending for decades.” ([Twitter](#), 4/24/2019)

**Microsoft Will Stop Providing Free Support for ES&S Certified Windows 7 Software on January 14<sup>th</sup>.** “That’s significant because Windows 7 reaches its “end of life” on Jan. 14, meaning Microsoft stops providing technical support and producing “patches” to fix software vulnerabilities, which hackers can exploit. In a statement to the AP, Microsoft said Friday it would offer continued Windows 7 security updates for a fee through 2023.” ([AP](#), 7/13/2019)

**ES&S May Not Be Able To Certify Windows 10 Before 2020 Primaries.** “For many people, the end of Microsoft 7 support means simply updating. However, for election systems the process is more onerous. ES&S and Hart don’t have federally certified systems on Windows 10, and the road to certification is long and costly, often taking at least a year and costing six figures... Though ES&S is testing a new system it’s unclear how long it will take to complete the process — federal and possible state recertification, plus rolling out updates — and if it will be done before primaries begin in February.” ([AP](#), 7/13/2019)

**ES&S Did Not Complete Windows 7 Certification (Released in 2009) Until March 2019.** “ES&S, the nation’s largest vendor, completed its latest certification four months ago, using Windows 7. Hart’s last certification was May 29 on a Windows version that also won’t be supported by November 2020.” ([AP](#), 7/13/2019)

### ES&S LARGE-SCALE NEGLIGENCE EXPOSED PERSONAL DATA OF MILLIONS OF VOTERS, LEFT TENS OF THOUSANDS OF NAMES OFF ROLLS AND LED TO MASSIVE DELAYS IN VOTE COUNTS ACROSS THE COUNTRY

**In Chicago, ES&S Negligence Exposed Personal Data of 1.8 Million Voters, Including Partial Social Security Numbers and Driver’s License Information in 2017.** “Names, addresses, dates of birth and other information about Chicago’s 1.8 million registered voters was left exposed and publicly available online on an Amazon cloud-computing server for an unknown period of time, the Chicago Board of Election Commissions said. The database file was discovered August 11 by a security researcher at Upguard, a company that evaluates cyber risk. The company alerted election officials in Chicago on August 12 and the file was taken down three hours later. The exposure was first made public on Thursday.” ([USA Today](#), 08/18/2017)

**In Alabama, ES&S Used Critically Flawed and Unsecured Wireless Connections In Voting Machines Until the State Forced Them To Remove Wireless Connections Last Year.** “For instance, industry leader ES&S sells vote-tabulation systems equipped with cellular modems, a feature that experts say sophisticated hackers could exploit to tamper with vote counts. A few states ban such wireless connections; in Alabama, the state had to force ES&S to remove them from machines ordered for one of its counties earlier this year. “It seemed like there was a lot more emphasis about how cool the machines could be than there was actual evidence that they were secure,” said John Bennett, the Alabama secretary of state’s deputy chief of staff.” ([AP News](#), 10/29/2018)

**In Los Angeles County, ES&S “Sloppy System Integration” Left 118,000 Names Off Printed Voter Rolls In 2018.** “During this year’s primary elections, ES&S technology stumbled on several fronts. In Los Angeles County, more than 118,000 names were left off printed voter rolls. A subsequent outside audit blamed sloppy system integration by an ES&S subsidiary during a database merge.” ([AP News](#), 10/29/2018)

**In 2008, Florida’s ES&S DS200 Machines Had an Overvote Rate on Election Day that Was 18 Times Greater Than Any Other System in Florida.** “A study from the [Florida Fair Elections Center](#) shows that counties using the [ES&S DS200](#), which in the event of an overvote displayed a confusing message and did not automatically reject a ballot, had an overvote rate on Election Day 2008 that was as much as 18 times that of systems used in other Florida counties.” ([Brennan Center For Justice](#), 2010)

**ES&S Failed to Notify Elections Officials in Pulaski County, Arkansas that Screens Would Appear Distorted for Voters Over 6ft Tall, Potentially Causing Them to Choose Incorrect Candidate (2006).** “During early voting in the May primary, several voters complained of problems with an ES&S touch screen DRE. According to a local newscast, Pulaski County election officials tested the machine and determined that the machine was not broken; an optical illusion perceived by voters who were over six feet tall caused the problem. Officials determined that the angle at which particularly tall voters viewed the screen caused them to believe that they were voting for the candidate below the one for whom a vote was recorded... a company employee told her that they were already aware of optical illusion problems experienced by tall voters... Officials were livid at the thought that ES&S could have known about the problem and failed to warn them.” ([Brennan Center For Justice](#), 2010)

**ES&S Sent Madison County, Indiana 7,400 Faulty Ballots, Then Blamed County For Not Testing The Ballots First (2008).** “The Herald Bulletin reported “that as many as 7,400 of the 12,000-some ballots used for early voting could not be counted by the machines. As it turns out, the coding on that portion of the early ballots was in the wrong position on the paper, tripping up the machines.” According to an editorial in the paper, “an official from Omaha-based Election Systems & Software, which provided the counting system, seemed to acknowledge that the company had sent the county ballots that wouldn’t work. But the county should take some blame too for not taking the precaution of testing the new set of ballots when they arrived.” ([Brennan Center For Justice](#), 2010)

**ES&S Sent Tennessee County Incorrect Early Vote File, More than 10,000 Names Missing (2014).** “Last Tuesday, as Davidson County voters were casting their ballots in local judicial primaries, election officials realized there was a problem - more than 10,000 people could have voted twice, and no one working the polls would have known to stop them...After more than 13,000 people voted early for the



May elections, the commission sent those records to ES&S. But when the files came back, to be entered into the EPBs for use on election day, Wall says they only contained the records of a little more than 2,000 voters. The missing records meant that more than 10,000 early voters could have shown up again on Election Day and voted a second time without being detected at the time.” (*Nashville Scene*, Hale, 5/12/2014)

**In Kansas, ES&S Did Not Do Any Audit After Software Error Led To Kansas’ Most Populous County’s Vote Count Being Stalled For 13 Hours in 2018.** “No such audit was done in Kansas’ most populous county after a different sort of error in newly installed ES&S systems delayed the vote count by 13 hours as data uploading from thumb drives crawled.” ([AP News](#), 10/29/2018)

US SENATORS EXPRESS NATIONAL SECURITY CONCERNS AFTER ES&S LIED TO FEDERAL LAWMAKERS, REFUSED TO REVEAL WHICH STATES WERE SENT CRITICALLY FLAWED MACHINES, & VIGOROUSLY FOUGHT ATTEMPTS TO REVEAL RELIABILITY INFORMATION

**ES&S Revealed it is Owned by Private Equity Firm McCarthy Group, LLC.** “Pursuant to the recently modified State of North Carolina Election Systems Certification Program, the following entities and/or individuals own a 5% or greater interest or share in ES&S, any subsidiary company of ES&S, and ES&S’ parent company. Government Systems, Software & Services, Inc. owns 100% of the membership units of Election Systems & Software... Please be advised that McCarthy Group, LLC owns a controlling interest in Government Systems, Software, & Services, LLC.” ([PBS.TWIMG](#), 6/21/2019)

**In Letter to ES&S & Other Vendors, US Senators Warn Decades Old Voting Machine Vulnerabilities Are a Significant National Security Concern.** “Despite the progress that has been made, election security experts and federal and state government officials continue to warn that more must be done to fortify our election systems. Of particular concern is the fact that many of the machines that Americans use to vote have not been meaningfully updated in nearly two decades. Although each of your companies has a combination of older legacy machines and newer systems, vulnerabilities in each present a problem for the security of our democracy and they must be addressed.” ([Office of Senator Amy Klobuchar](#), 3/26/2019)

**US Senators Call Market for Election Equipment “Broken,” Claim ES&S/Others of Producing Vulnerable Voting Machines.** “In other words, the fact that VVSG 2.0 remains a work in progress is not an excuse for the fact that our voting equipment has not kept pace both with technological innovation and mounting cyber threats... The fact that you continue to manufacture and sell outdated products is a sign that the marketplace for election equipment is broken.” ([Office of Senator Amy Klobuchar](#), 3/26/2019)

**US Senators Conclude “Voter-Verifiable Paper Ballots” Are Basic Necessities For A Reliable Voting System.** “There is a consensus among cybersecurity experts regarding the fact that voter-verifiable paper ballots and the ability to conduct a reliable audit are basic necessities for a reliable voting system. Despite this, each of your companies continues to produce some machines without paper ballots” ([Office of Senator Amy Klobuchar](#), 3/26/2019)

**Senator Ron Wyden Said ES&S has “Figured Out a Way to be Above the Law” and Georgia Showed the Company is “Accountable to Nobody.”** “We’re up against some really entrenched, powerful interests, who have really just figured out a way to be above the law,” he said. “There is no other way to characterize it.” Furthermore, Wyden said, voting machine vendors have “been able to hotwire the political system in certain parts of the country.” He noted that newly elected Georgia Gov. Brian Kemp picked the top lobbyist for the voting giant Election Systems & Software as his deputy chief of staff. The companies, he said, “are accountable to nobody.” ([Politico](#), 3/14/19)

**Senator Ron Wyden Demanded ES&S Explain “Suspect Claims” the Company Made to the League of Women Voters of South Carolina that ES&S Machines Have Never Been Breached.** “I write to seek an explanation of suspect claims that Election Systems and Software (ES&S) has made regarding the security of your voting machines. In a January 15, 2019, letter to the League of Women Voters of South Carolina, ES&S wrote that ‘no ES&S machine has ever been breached or comprised in an election.’ Your company’s letter does not explain the basis for its assessment that its voting machines have a spotless cybersecurity track record.” ([Office of Senator Ron Wyden](#), 4/2/2019)

**Senator Ron Wyden Said Vendors like ES&S had “Sketchy Ethics,” “Lie to Public Officials,” and “Repeatedly Gouge Taxpayers.”** “Sen. Ron Wyden (D-Ore.) on Thursday attacked the small but powerful group of companies that controls the production of most voting equipment used in the U.S. ‘The maintenance of our constitutional rights should not depend on the sketchy ethics of these well-connected corporations that stonewall the Congress, lie to public officials, and have repeatedly gouged taxpayers, in my view, selling all of this stuff,’ Wyden said...” ([Politico](#), 3/14/19)

**ES&S Added Two New Lobbying Firms Last Fall in Anticipation of Increasing Pressure from Lawmakers to Protect Elections.** “Voting machine manufacturers are increasing their Capitol Hill presence as lawmakers demand they do more to protect U.S. elections against foreign hackers ... In October, ES&S hired Peck Madigan Jones, and paid the firm \$80,000 during the last three months of 2018. The company also reported hiring the lobbying firm Vectre Corp.” ([Bloomberg](#), 4/1/2019)

**ES&S Initially Lied When Asked If It Installed Third Party Hackable Software on Election-Management Systems Over Six Years.** “The nation’s top voting machine maker has admitted in a letter to a federal lawmaker that the company installed remote-access software on election-management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them. In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had “provided pcAnywhere remote connection software ... to a small number of customers between 2000 and 2006,” which was installed on the election-management system ES&S sold them. The statement contradicts what the company told me and fact checkers for a story I wrote for the New York Times in February. At that time, a spokesperson said ES&S had never installed pcAnywhere on any election system it sold.” ([MotherBoard](#), 7/17/2018)

**ES&S Refused to Tell Federal Lawmakers Which States/Counties Were Sold Critically Flawed Voting Machines.** “He notes that election officials who purchased the systems likely were not aware of the potential risks they were taking in allowing this and didn’t understand the threat landscape to make

intelligent decisions about installing such software...Although Wyden's office asked ES&S to identify which of its customers were sold systems with pcAnywhere installed, the company did not respond. ES&S would only say that it had confirmed with customers who had the software installed that they "no longer have this application installed."...As late as 2011 pcAnywhere was still being used on at least one ES&S customer's election-management system in Venango County, Pennsylvania." ([MotherBoard](#), 7/17/2018)

**ES&S Refused to Comment to Federal Lawmakers on Whether Critical Security Flaws in Voting Machine Software Were Adequately Patched.** "It's not clear if election officials who had pcAnywhere installed on their systems, ever patched this and other security flaws that were in the software...But when Wyden's office asked in a letter to ES&S in March what settings were used to secure the communications, whether the system used hard-coded or default passwords and whether ES&S or anyone else had conducted a security audit around the use of pcAnywhere to ensure that the communication was done in a secure manner, the company did not provide responses to any of these questions." ([MotherBoard](#), 7/17/2018)

**In Wisconsin, ES&S Filed A Lawsuit Demanding Presidential Campaigns Sign NDA's to Prevent Public Discussion of Machine Reliability Following Election Issues.** "Electronic Systems & Software and Dominion Voting Systems supply most of the machines used in Wisconsin elections. The two companies filed a lawsuit in April demanding the nondisclosure agreement prohibit Stein's auditors and campaign from publicly discussing any conclusions and criticisms stemming from the review. The companies argued public discussion amounts to an unauthorized use or disclosure of proprietary information." ([The Journal Times](#), 1/30/2019)

**In Colorado, ES&S Refused to Seek Certification After the State Required Vulnerability Testing of Voting Machines.** "In an April 2014 meeting with Colorado elections officials, ES&S objected to a new state requirement for vulnerability testing because it didn't allow for the results to be kept secret, Colorado Deputy Secretary of State Suzanne Staiert said in an interview. She said the company ultimately didn't seek certification because the system it was offering didn't meet state requirements. ES&S did not directly respond to a query about this incident. A company spokeswoman said a review of company correspondence found no sign that it resisted the testing requirement, although it did "ask clarifying questions." ([AP News](#), 10/29/2018)

**The Brennan Center For Justice Said there are "More Federal Regulations for Ballpoint Pens & Magic Markers Than There Are For Voting Systems."** "In contrast to other sectors, particularly those that the federal government has designated 'critical infrastructure,' there is almost no federal oversight of private vendors that design and maintain the systems that allow us to determine who can vote, how they vote, what voters see when they cast their vote, how votes are counted, and how those vote totals are communicated to the public," [the Brennan Center for Justice's Lawrence] Noren told Congress recently in a testimony. "In fact, there are more federal regulations for ballpoint pens and magic markers than there are for voting systems and other parts of our federal election infrastructure." ([Sludge](#), 6/10/2019)



**Following Pressure from Lawmakers, ES&S CEO Tom Burt Said the Company Would No Longer Sell Paperless Voting Machines as Primary Device for Casting Ballots.** "Voting machine maker ES&S has said it "will no longer sell" paperless voting machines as the primary device for casting ballots in a jurisdiction. ES&S chief executive Tom Burt confirmed the news in an op-ed. TechCrunch understands the decision was made around the time that four senior Democratic lawmakers demanded to know why ES&S, and two other major voting machine makers, were still selling decade-old machines known to contain security flaws." ([TechCrunch](#), 6/9/2019)

**After Facing Criticism for Denouncing Machine Vulnerabilities, ES&S CEO Called for Legislation Mandating Stronger Election Machine Testing Programs.** "The chief executive also called on Congress to pass legislation mandating a stronger election machine testing program. Burt's remarks are a sharp turnaround from the company's position just a year ago, in which the election systems maker drew ire from the security community for denouncing vulnerabilities found by hackers at the annual Defcon conference. ([TechCrunch](#), 6/9/2019)

**ES&S CEO Tom Burt Also Called For "Physical Paper Records of Votes" (*\*\*not the same as hand-marked paper ballots*).** "Second, we must have physical paper records of votes. Our company, Election Systems & Software, the nation's leading elections equipment provider, recently decided it will no longer sell paperless voting machines as the primary voting device in a jurisdiction. That's because it is difficult to perform a meaningful audit without a paper record of each voter's selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid postelection audits. ([Roll Call](#), 6/7/2019)

**Critics Called the ES&S Pivot New "Marketing" "After Years of Selling Voting Equipment It Knew Was Insecure."** "But critics say Election Systems & Software's open pivot to paper is simply marketing, after the company saw that paperless machines were on the way out. "After years of selling voting equipment that it knew was insecure, and fighting tooth and nail against real election security, ES&S is finally admitting that paper ballots are the most secure system currently available," Sen. Ron Wyden, whose PAVE Act is one of the strictest security bills introduced in the Senate, told CNN in a statement." ([CNN](#), 6/19/2019)

**Senator Wyden Said ES&S Should Tell Its "Friends in Georgia" to Stop Standing in the Way of Legislation to Help Protect American Democracy.** "If it is serious about this change of heart, ES&S would tell its friends in Georgia and Speaker McConnell to stop standing in the way of the PAVE Act's common-sense requirements to protect American democracy," the Oregon Democrat said. ([CNN](#), 6/19/2019)

**ES&S Paid Lobbying Firm Peck Madigan Jones \$150,000 to Lobby House and Senate Members.** ES&S hired lobbying firm Peck Madigan Jones in Oct. 2018 and paid it a combined \$150,000 to lobby the U.S. Senate and House of Representatives in the fourth quarter of 2018 and the first quarter of 2019. ([Sludge](#), 6/10/2019)

**ES&S Lobbyists Donated to Mitch McConnell—Who is "Single-Handedly" Standing in the Way of Any Election Security Legislation.** "Emily Kirlin, a lobbyist for Peck Madigan Jones who lobbies for ES&S on election security and H.R. 1, gave McConnell's campaign committee \$1,000 on February 19, and her colleague who works with her on the contract, Jen Olson, gave McConnell \$1,000 on March 4.

“It’s not surprising to me that Mitch McConnell is receiving these campaign contributions,” the Brennan Center for Justice’s Lawrence Noren told Sludge. “He seems single-handedly to be standing in the way of anything passing in Congress around election security...” ([Sludge](#), 6/10/2019)

**Public Citizen Called the ES&S Contributions to McConnell “A Reward from the Industry for Letting Them Off the Hook.”** “Mitch McConnell’s conflicts of interest in blocking any and all election security legislation is not only shameful, it is placing our democracy at risk,” Craig Holman, government affairs lobbyist at Public Citizen, told Sludge. “The conflicts of interest arise from more than the campaign contributions he is receiving from voting machine vendors—contributions which certainly appear to be a reward from the industry for letting them off the hook—but it is also a self-serving act for strictly partisan purposes. ([Sludge](#), 6/10/2019)

**Ballot Marking Devices Cost About 3x As Much as Truly Paper-Based Systems, Says Election Security Expert in Congressional Testimony.** “According to testimony from Alex Halderman, Professor of Computer Science and Engineering at the University of Michigan, equipping a precinct with ballot-marking electronic devices costs about three times as much as equipping it with a truly paper-based system along with a dedicated electronic device for voters with disabilities. “Fortunately, the most cost-effective approach is also the most secure: hand-marked paper ballots counted using optical scanners,” Halderman stated. ([Sludge](#), 6/10/2019)

**ES&S INDIANA CONTRACT TERMINATED AFTER INVESTIGATION REVEALS ES&S VIOLATED INDIANA STATE LAW, LIED TO ELECTION OFFICIALS, AND WERE RESPONSIBLE FOR ERRORS RESULTING IN LONG WAIT TIMES, VOTER ANXIETY, DISCOURAGED VOTERS, AND EMBARRASMENT**

**Johnson County Terminated Contract with ES&S After State Investigation Determined ES&S Responsible for Technical Issues that Triggered Long Lines in 2018.** What struggled to work were the electronic poll books used to check a voter’s registration, triggering long lines at polling stations. A state investigation determined that the vendor for the e-poll books, Election Systems & Software (ES&S), was responsible for the technical issue, and the Johnson County election board ultimately voted to terminate the contract. ([The Hill](#), 3/24/19)

**Johnson County Clerk Said the Community Had Lost Trust in ES&S.** “Trena McLaughlin, the county clerk for Indiana’s Johnson County who took office after the November vote, told The Hill that the election board decided to terminate its contract with ES&S because the community had lost trust in the vendor. “We have had a lot of people asking, ‘should we be using ES&S?’” she said.” ([The Hill](#), 3/24/19)

**ES&S Issues Resulted in Voter Anxiety, Discouraged Voting, and Brought Embarrassment and Negative Publicity to Johnson County.** “The problems which occurred in Johnson County was a source of negative publicity for the County. In addition to embarrassment, the more important impact was on voters who did not understand what was occurring and this likely created voter anxiety, impacted confidence in the electoral process, and probably discouraged voters from continuing to wait to cast a ballot. The work around offered on Election Day was not in compliance with the Indiana Election Code.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

**Indiana Officials Called Election Day Issues “Unacceptable” and Said the Responsibility “Rests on the Shoulders of ES&S.”** “The situation which occurred in Johnson is unacceptable for any Indiana electronic poll book vendor. The responsibility for what occurred rests on the shoulders of ES&S, because they opted for a limited WAF instance configuration with Microsoft Azure after switching from Amazon Web Services. The premise that their pre-election load testing adequately predicted election day needs is difficult to accept.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

**ES&S Violated Indiana State Law When It Failed to Report Several System “Anomalies” Prior to Election Day.** “The VSTOP investigators also concluded that ES&S failed to report several system “anomalies” that occurred prior to election day, which violates Indiana election law. And, attempts to fix the lagging computer issues on election day also resulted in a violation of state code.” ([CBS4Indy.com](#), 1/09/2019)

**ES&S Violated Indiana Law When It Offered County A Work-Around for Its Own Performance Issues.** “3. ES&S made a business decision to move from Amazon Web Service (AWS) to Microsoft Azure but did not notify the State of Indiana or VSTOP. 4. ES&S offered Johnson County a work-around to allow voters to be checked in at the vote centers. However, this work-around resulted in electronic poll books not being able to communicate between vote centers in Johnson County. This solution was not in compliance with the Indiana Election Code. 5. ES&S has stated that the Microsoft Azure Web Application Firewall (WAF), which is part of the Application Gateway, is the key reason for the performance issues on Election Day. 6.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

**“After Tests Failed to Predict Election Day Server Needs, ES&S Erased All Logs Prior to Election Day and All Diagnostic Logs For The General Election.”** “ES&S misjudged server needs and the impact of WAF instances for Election Day. Pre-election load tests conducted by ES&S did not adequately predict Election Day server needs. The logs for the load tests prior to the primary were not retained. Moreover, diagnostic logs were not retained by Microsoft or by ES&S for the General Election. 8. ES&S admitted, in retrospect, that 7 WAF instances was not sufficient for Election Day.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

**ES&S Lied to Indiana Officials About the Cause of Slow Electronic Poll Books On Election Day.** “ES&S initially maintained that the problem with slow electronic poll book performance on Election Day was caused by the Microsoft Azure Web Application Firewall (WAF). It was discovered in responses to VSTOP questions by ES&S, and in subsequent conversations with ES&S, that the problem was caused by the limited number of instances in the WAF that ES&S secured through Microsoft Azure for electronic poll book data traffic.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

**Indiana Officials Believe ES&S Issues May Have Occurred in All Counties On Election Day In 2018.** “The anomaly report from ES&S, required by law, was limited in scope concerning the issues encountered. Issues may have also occurred in all ES&S counties on Election Day as well as during early voting (see Appendix A).” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

**ES&S Did Not Have Their Systems Properly Set Up To Handle High Voter Turnout.** “The VSTOP report claims Johnson County’s election software vendor, ES&S inadequately anticipated server needs

on election day, and did not have their systems properly set up to handle the high voter turnout seen around the county.” ([CBS4Indy.com](https://www.cbs4indy.com), 1/09/2019)

**In 2018, ES&S Pollbooks Did Not Meet Performance Expectations in Indiana and Resulted In Longer Wait Times.** “The ES&S ExpressPoll EZRoster 3.2.2.1 did not meet performance expectations at vote centers in Johnson County, Indiana on Election Day, November 6, 2018. 2. The ExpressPoll EZ Roster 3.2.2.1 performance issues resulted in longer than expected wait times for voters.” ([Voting System Technical Oversight Program Report](#), 12/31/2018)

### Information Assurance Compliance

Using the NIST Security Content Automation Protocol (SCAP), all Electionware servers and workstations were scanned for misconfigurations in accordance with US federal IA standards. These standards conform to mitigating known vulnerabilities and hardening target systems on a US government network.

The following table presents a summary of patches missing on the operating system and misconfigurations on each class (workstation or server) of systems in the Electionware suite.

#### Electionware Servers

Missing Operating System Patches	
<b>Critical</b>	17
<b>Important</b>	49
<b>Moderate</b>	2
<b>Unrated</b>	8

SCAP Misconfigurations	
<b>Windows 2008 R2 STIG<sup>3</sup></b>	46
<b>Firewall STIG Configuration</b>	3
<b>.NET Framework 4 STIG Configuration</b>	2
<b>Internet Explorer 9 STIG Configuration</b>	13

#### Electionware Clients

Missing Operating System Patches	
<b>Critical</b>	24
<b>Important</b>	51
<b>Moderate</b>	1
<b>Unrated</b>	9

SCAP Misconfigurations	
<b>Windows 7 STIG</b>	51
<b>Firewall STIG Configuration</b>	3
<b>.NET Framework 4 STIG Configuration</b>	2
<b>Internet Explorer 9 STIG Configuration</b>	3
<b>Windows 7 USGCB<sup>4</sup> Configuration</b>	45
<b>Firewall USGCB Configuration</b>	8



## Appendix B: Vendor RFI Analysis: Statewide Voting Machine Contracts

Georgia Vendor RFI Analysis: Statewide Voting Machine Contracts (Millions)							
	ES&S	SOS	OSET	Hart	Smartmatic	Clear Ballot	UNISYN
<b>Total: Hand-Marked Paper Ballots</b>	<b>45.8</b>	<b>247</b>	<b>112</b>	<b>68.5</b>	<b>-</b>	<b>-</b>	<b>63</b>
<i>Total w/ Printing Cost Est (\$28M)*</i>	<i>73.8</i>	<i>247</i>	<i>112</i>	<i>96.5</i>			<i>91</i>
Machines	22.8	60	50	41	-	-	48
Printing, Licensing/Maintenance**	23	187	62	27.5	-	-	15
Caveats	NP	+LM		NP	None	None	NP
<b>Total: Ballot Marking Devices</b>	<b>207.4</b>	<b>207.4</b>	<b>202</b>	<b>174</b>	<b>169</b>	<b>156.5</b>	<b>185.4</b>
<i>Total w/ Printing Cost Est (\$5.8M)*</i>	<i>213.2</i>	<i>213.2</i>	<i>202</i>	<i>179.8</i>	<i>174.8</i>	<i>162.3</i>	<i>191.2</i>
Machines	150	150	131	117	135	101.5	137
Printing, Licensing/Maintenance	57.4	57.4	71	57	34	55	48.4
Caveats	NP	NP		NP	Avg, NP	DNA, NP	NP

\*for vendors that did not provide printing cost estimates, OSET Institute's 10 yr estimates were used

\*\*printing, licensing/maintenance costs are over a 10 yr period

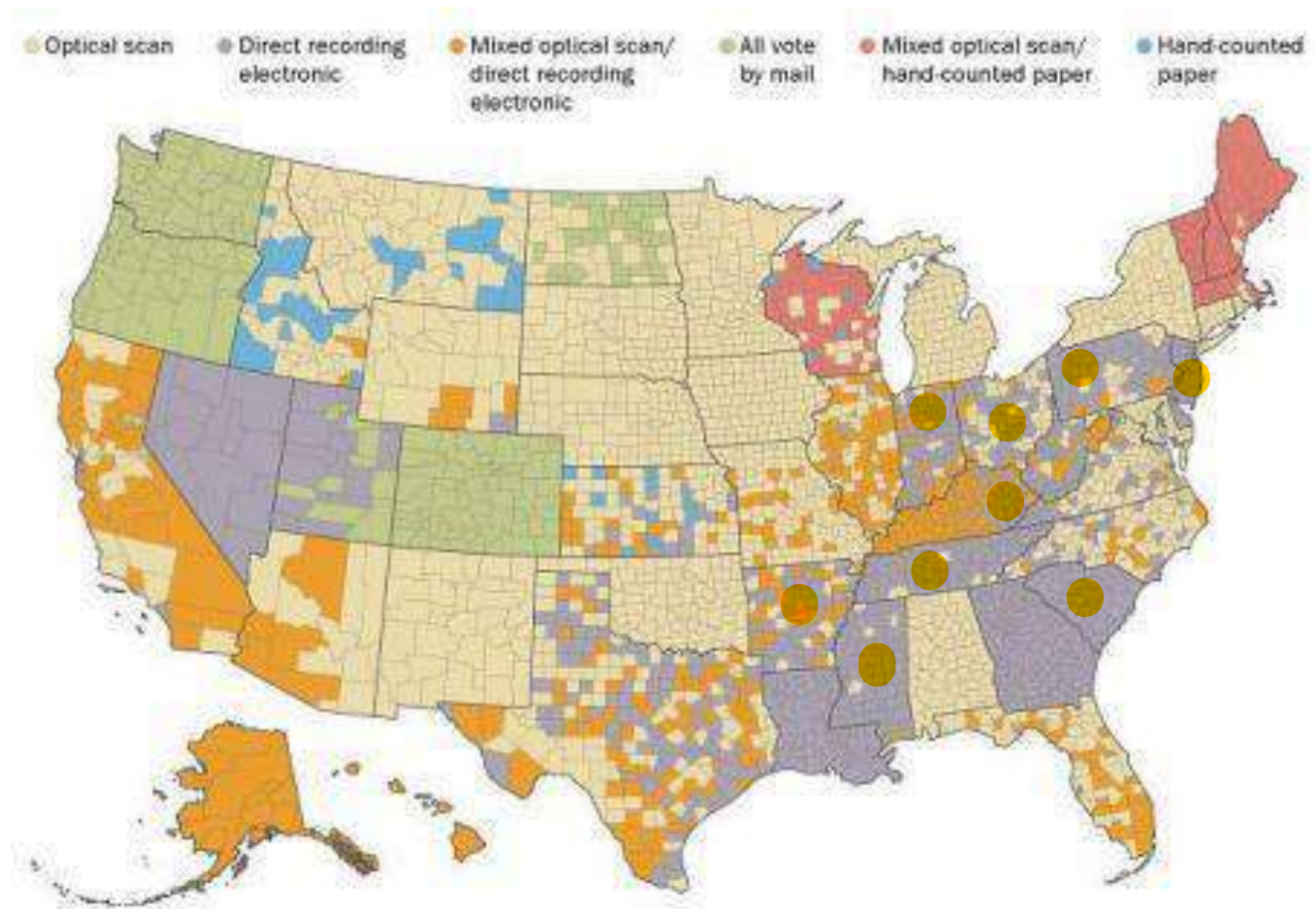
### KEY

- **NP:** No printing costs were included in original vendor estimate
- **+LM:** Licensing/maintenance cost added from ES&S report
- **DNA:** Data is not available...unredacted Clear Ballot link broken
- **None:** Did not provide details
- **Avg:** This is the average of the range provided in RFI

Dominion only provided a basic pricing sheet for every voting machine technology they offered. Which machines, how many, additional costs, were time prohibitive details. As such, Dominion was not included.

([GPR](#), 3/13/2019)

Appendix C: Map of Voting Systems Across the U.S.—Pew Research Center/Verified Voting Foundation



([Quartz](#), 7/9/2019)



OCTOBER 16, 2020 | JUDICIAL WATCH

# New Judicial Watch Study Finds 353 U.S. Counties in 29 States with Voter Registration Rates Exceeding 100%



## *1.8 Million 'Extra' Registered Voters*

(Washington, DC) – Judicial Watch announced today that a [September 2020 study](#) revealed that 353 U.S. counties had 1.8 million more registered voters than eligible voting-age citizens. In other words, the registration rates of those counties exceeded 100% of eligible voters. The study found eight states showing state-wide registration

rates exceeding 100%: Alaska, Colorado, Maine, Maryland, Michigan, New Jersey, Rhode Island, and Vermont.

The September 2020 study collected the most recent registration data posted online by the states themselves. This data was then compared to the Census Bureau's most recent five-year population estimates, gathered by the American Community Survey (ACS) from 2014 through 2018. ACS surveys are sent to 3.5 million addresses each month, and its five-year estimates are considered to be the most reliable estimates outside of the decennial census.

Judicial Watch's latest study is necessarily limited to 37 states that post regular updates to their registration data. Certain state voter registration lists may also be even larger than reported, because they may have excluded "inactive voters" from their data. Inactive voters, who may have moved elsewhere, are still registered voters and may show up and vote on election day and/or request mail-in ballots.

Judicial Watch relies on its voter registration studies to warn states that they are failing to comply with the requirements of the National Voter Registration Act of 1993, which requires states to make reasonable efforts to clean their voter rolls. Judicial Watch can and has sued to enforce compliance with federal law.

Earlier this month, Judicial Watch sued [Colorado](#) over its failure to comply with the National Voter Registration Act. In Judicial Watch's new study, 42 Colorado counties—or two thirds of the state's counties—had registration rates exceeding 100%. Particular data from the state confirms this general picture. As the complaint explains, a month-by-month comparison of the ACS's five-year survey period with Colorado's own registration numbers for the exact same months shows that large proportions of Colorado's counties have registration rates exceeding 100%. Earlier this year, Judicial Watch sued [Pennsylvania](#) and [North Carolina](#) for failing to make reasonable efforts to remove ineligible voters from their rolls as required by federal law. The lawsuits allege that the two states have nearly 2 million inactive names on their voter registration rolls. Judicial Watch also sued Illinois for refusing to disclose voter roll data in violation of Federal law.

“The new study shows 1.8 million excess, or ‘ghost’ voters in 353 counties across 29 states,” said Judicial Watch President Tom Fitton. “The data highlights the recklessness of mailing blindly ballots and ballot applications to voter registration lists. Dirty voting rolls can mean dirty elections.”

Judicial Watch’s study updates the results of a similar study from last year. In August 2019, Judicial Watch analyzed registration data that states reported to the federal Election Assistance Commission (EAC) in response to a survey conducted every two years on how states maintain their voter rolls. That registration data was compared to the then-most-recent ACS five-year survey from 2013 through 2017. The study showed that 378 U.S. counties had registration rates exceeding 100%.

Judicial Watch is a national leader for cleaner elections.

In 2018, the Supreme Court upheld a voter-roll cleanup program that resulted from a Judicial Watch settlement of a federal lawsuit with [Ohio](#). California [settled](#) a NVRA lawsuit with Judicial Watch and last year began the process of removing up to 1.6 million inactive names from Los Angeles County’s voter rolls. [Kentucky](#) also began a cleanup of hundreds of thousands of old registrations last year after it entered into a consent decree to end another Judicial Watch lawsuit.

In September 2020, Judicial Watch sued [Illinois](#) for refusing to disclose voter roll data in violation of Federal law.

Judicial Watch Attorney Robert Popper is the director of Judicial Watch’s clean elections initiative.

## STATES AND COUNTIES WITH REGISTRATION RATES EXCEEDING 100%

(\* means no separate reporting of inactive registrations)

**Alabama:** Lowndes County (130%); Macon County (114%); Wilcox (113%); Perry County (111%); Madison County (109%); Hale County (108%); Marengo County (108%); Baldwin (108%); Greene County (107%); Washington County (106%); Dallas County (106%); Choctaw County (105%); Conecuh County (105%); Randolph County (104%); Shelby County (104%); Lamar County (103%); Autauga County (103%); Clarke County (103%); Henry County (103%); Monroe County (102%); Colbert County (101%); Jefferson County (101%); Lee County (100%); Houston County (100%); Crenshaw County (100%)

**\*Alaska: Statewide (111%)**

**Arizona:** Santa Cruz County (107%); Apache County (106%)

**\*Arkansas:** Newton County (103%)

**Colorado: Statewide (102%);** San Juan County (158%); Dolores County (127%); Jackson County (125%); Mineral County (119%); Ouray County (119%); Phillips County (116%); Douglas County (116%); Broomfield County (115%); Elbert County (113%); Custer County (112%); Gilpin County (111%); Park County (111%); Archuleta County (111%); Cheyenne County (111%); Clear Creek County (110%); Teller County (108%); Grand County (107%); La Plata County (106%); Summit County (106%); Baca County (106%); Pitkin County (106%); San Miguel County (106%); Routt County (106%); Hinsdale County (105%); Garfield County (105%); Gunnison County (105%); Sedgwick County (104%); Eagle County (104%); Larimer County (104%); Weld County (104%); Boulder County (103%); Costilla County (103%); Chaffee County (103%); Kiowa County (103%); Denver County (103%); Huerfano County (102%); Montezuma County (102%); Moffat County (102%); Arapahoe County (102%); Jefferson County (101%); Las Animas County (101%); Mesa County (100%)

**\*Florida:** St. Johns County (112%); Nassau County (109%); Walton County (108%); Santa Rosa County (108%); Flagler County (104%); Clay County (103%); Indian River County (101%); Osceola County (100%)

**\*Georgia:** Bryan County (118%); Forsyth County (114%); Dawson County (113%); Oconee County (111%); Fayette County (111%); Fulton County (109%); Cherokee County (109%); Jackson County (107%); Henry County (106%); Lee County (106%); Morgan County (105%); Clayton County (105%); DeKalb County (105%); Gwinnett County (104%); Greene County (104%); Cobb County (104%); Effingham County (103%); Walton County (102%); Rockdale County (102%); Barrow County (101%); Douglas County (101%); Newton County (100%); Hall County (100%)

**\*Indiana:** Hamilton County (113%); Boone County (112%); Clark County (105%); Floyd County (103%); Hancock County (103%); Ohio County (102%); Hendricks County (102%); Lake County (101%); Warrick County (100%); Dearborn County (100%)

**Iowa:** Dallas County (115%); Johnson County (104%); Lyon County (103%); Dickinson County (103%); Scott County (102%); Madison County (101%); Warren County (100%)

**\*Kansas:** Johnson County (105%)

**Maine:** **Statewide (101%);** Cumberland County (110%); Sagadahoc County (107%); Hancock County (105%); Lincoln County (104%); Waldo County (102%); York County (100%)

**Maryland:** **Statewide (102%);** Montgomery County (113%); Howard County (111%); Frederick County (110%); Charles County (108%); Prince George's County (106%); Queen Anne's County (104%); Calvert County (104%); Harford County (104%); Worcester County (103%); Carroll County (103%); Anne Arundel County (102%); Talbot County (100%)

**\*Massachusetts:** Dukes County (120%); Nantucket County (115%); Barnstable County (103%)

**\*Michigan:** **Statewide (105%);** Leelanau County (119%); Otsego County (118%); Antrim County (116%); Kalkaska County (115%); Emmet County (114%); Berrien

County (114%); Keweenaw County (114%); Benzie County (113%); Washtenaw County (113%); Mackinac County (112%); Dickinson County (112%); Roscommon County (112%); Charlevoix County (112%); Grand Traverse County (111%); Oakland County (110%); Iron County (110%); Monroe County (109%); Genesee County (109%); Ontonagon County (109%); Gogebic County (109%); Livingston County (109%); Alcona County (108%); Cass County (108%); Allegan County (108%); Oceana County (107%); Midland County (107%); Kent County (107%); Montmorency County (107%); Van Buren County (107%); Wayne County (107%); Schoolcraft County (107%); Mason County (107%); Oscoda County (107%); Iosco County (107%); Wexford County (106%); Presque Isle County (106%); Delta County (106%); Alpena County (106%); St Clair County (106%); Cheboygan County (105%); Newaygo County (105%); Barry County (105%); Gladwin County (105%); Menominee County (105%); Crawford County (105%); Muskegon County (105%); Kalamazoo County (104%); St. Joseph County (104%); Ottawa County (103%); Clinton County (103%); Saginaw County (103%); Manistee County (103%); Lapeer County (103%); Calhoun County (103%); Ogemaw County (103%); Macomb County (103%); Missaukee County (102%); Eaton County (102%); Shiawassee County (102%); Huron County (102%); Lenawee County (101%); Branch County (101%); Osceola County (101%); Clare County (100%); Arenac County (100%); Bay County (100%); Lake County (100%)

**\*Missouri:** St. Louis County (102%)

**\*Montana:** Petroleum County (113%); Gallatin County (103%); Park County (103%); Madison County (102%); Broadwater County (102%)

**\*Nebraska:** Arthur County (108%); Loup County (103%); Keya Paha County (102%); Banner County (100%); McPherson County (100%)

**Nevada:** Storey County (108%); Douglas County (105%); Nye County (101%)

**\*New Jersey: Statewide (102%);** Somerset County (110%); Hunterdon County (108%); Morris County (107%); Essex County (106%); Monmouth County (104%); Bergen County (103%); Middlesex County (103%); Union County (103%); Camden



County (102%); Warren County (102%); Atlantic County (102%); Sussex County (101%); Salem County (101%); Hudson County (100%); Gloucester County (100%)

**\*New Mexico:** Harding County (177%); Los Alamos County (110%)

**New York:** Hamilton County (118%); Nassau County (109%); New York (103%); Rockland County (101%); Suffolk County (100%)

**\*Oregon:** Sherman County (107%); Crook County (107%); Deschutes County (105%); Wallowa County (103%); Hood River County (103%); Columbia County (102%); Linn County (101%); Polk County (100%); Tillamook County (100%)

**Rhode Island:** Statewide (101%); Bristol County (104%); Washington County (103%); Providence County (101%)

**\*South Carolina:** Jasper County (103%)

**South Dakota:** Hanson County (171%); Union County (120%); Jones County (116%); Sully County (115%); Lincoln County (113%); Custer County (110%); Fall River County (108%); Pennington County (106%); Harding County (105%); Minnehaha County (104%); Potter County (104%); Campbell County (103%); McPherson County (101%); Hamlin County (101%); Stanley County (101%); Lake County (100%); Perkins County (100%)

**Tennessee:** Williamson County (110%); Moore County (101%); Polk County (101%)

**Texas:** Loving County (187%); Presidio County (149%); McMullen County (147%); Brooks County (117%); Roberts County (116%); Sterling County (115%); Zapata County (115%); Maverick County (112%); Starr County (110%); King County (110%); Chambers County (109%); Irion County (108%); Jim Hogg County (107%); Polk County (107%); Comal County (106%); Oldham County (104%); Culberson County (104%); Kendall County (103%); Dimmit County (103%); Rockwall County (102%); Motley County (102%); Parker County (102%); Hudspeth County (101%); Travis



County (101%); Fort Bend County (101%); Kent County (101%); Webb County (101%); Mason County (101%); Crockett County (101%); Waller County (100%); Gillespie County (100%); Duval County (100%); Brewster County (100%)

**Vermont: Statewide (100%)**

**Virginia:** Loudoun County (116%); Falls Church City (114%); Fairfax City (109%); Goochland County (108%); Arlington County (106%); Fairfax County (106%); Prince William County (105%); James City County (105%); Alexandria City (105%); Fauquier County (105%); Isle of Wight County (104%); Chesterfield County (104%); Surry County (103%); Hanover County (103%); New Kent County (103%); Clarke County (103%); King William County (102%); Spotsylvania County (102%); Rappahannock County (102%); Albemarle County (101%); Stafford County (101%); Northampton County (101%); Poquoson City (100%); Frederick County (100%)

**Washington:** Garfield County (119%); Pend Oreille County (112%); Jefferson County (111%); San Juan County (108%); Wahkiakum County (108%); Stevens County (103%); Pacific County (103%); Clark County (102%); Island County (102%); Klickitat County (102%); Thurston County (102%); Lincoln County (101%); Whatcom County (100%); Asotin County (100%)

**\*West Virginia:** Mingo County (104%); Wyoming County (103%); McDowell County (102%); Brooke County (102%); Hancock County (100%)

###

---

© 2019 Judicial Watch, Inc.

Judicial Watch is a 501(c)(3) nonprofit organization. Contributions are received from individuals, foundations, and corporations and are tax-deductible to the extent allowed by law.

[Shop](#) [Donate](#)



## INDIANA'S VOTING MACHINES VULNERABLE TO SECURITY ISSUES

### BACKGROUND

Efficient and accurate voting systems play a pivotal role in maintaining voter confidence in the election system. Russian interference in the 2016 U.S. presidential election and other incidents have emphasized the need for the country to rethink the security of its existing voting infrastructure. This can include ensuring safe and secure polling places, up-to-date voting equipment, and verifiable paper records of votes.

In 2019, voters in Indiana filed a federal suit to replace paperless voting machines in the state, which do not leave a paper trail of votes that were cast.<sup>1</sup> These paperless electronic machines rose to prominence after the Help America Vote Act banned the use of lever machines and punch cards in federal elections following the Florida recount controversy of 2000. However, concerns with these types of machines began to arise as early as the 2002 elections.<sup>2</sup> The 2019 Indiana lawsuit cited that the use of paperless electronic voting machines leaves Indiana vulnerable to security risks.

Given these issues, we examined data from the organization Verified Voting<sup>3</sup> to review the prevalence and types of voting equipment used in Indiana polling sites as of 2020. This brief further assesses the risks and implications

### SUMMARY

- Although most of the voters in the United States vote using hand-marked ballots, the majority of Hoosier voters use direct-recording electronic (DRE) voting machines.
- DRE machines can be vulnerable to security risks, especially when they do not leave a paper record of votes that were cast.
- Nearly 60 percent of Indiana's voting machines are paperless.
- Indiana is only one of eight states that will use paperless voting machines in the November 2020 election.
- A lack of funding is a large factor in the state's delay in moving to paper-based voting systems.

of using paperless audit voting machines and provides recommendations to increase the security of Indiana elections in the future .

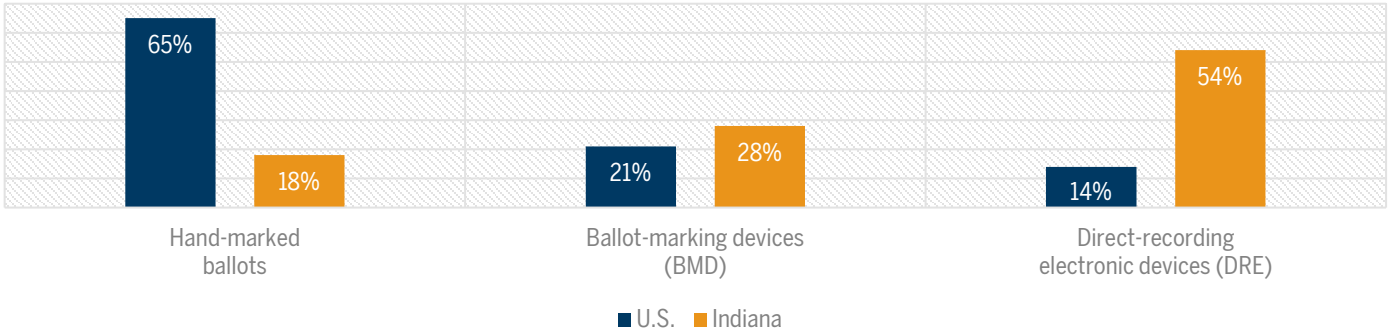
### FINDINGS

Technologies for computer-assisted voting include optical scanners, ballot-marking devices (BMDs), and direct-record electronic (DRE) voting machines (Table 1).

**TABLE 1. Types of voting machines used across the United States**

TYPE OF VOTING EQUIPMENT <sup>3</sup>	DESCRIPTION
Optical/digital scan	Voters make their selection on paper ballots, which is then read by an optical or digital scanner and stored.
Ballot-marking device (BMD)	Voters make their selection through either a touch screen or mechanical input. This selection is not stored or counted on the machine itself. Rather, it is printed out so that it can be scanned by a reader.
Direct-recording electronic (DRE) voting machine, with verified voting paper audit trail (VVPAT)	Voters make their selection through a touch screen or push-button interface. Votes are stored in the computer memory. A paper record is used either by the voter to review the selection prior to casting the vote, or to facilitate a recount or audit.
Direct-recording electronic (DRE) voting machine, without VVPAT	Voters make their selection through a touch screen or push-button interface. Votes are stored in the computer memory and do not leave a paper record.

**FIGURE 1.** Percentage of voters in United States and Indiana jurisdictions using machine type (2020)

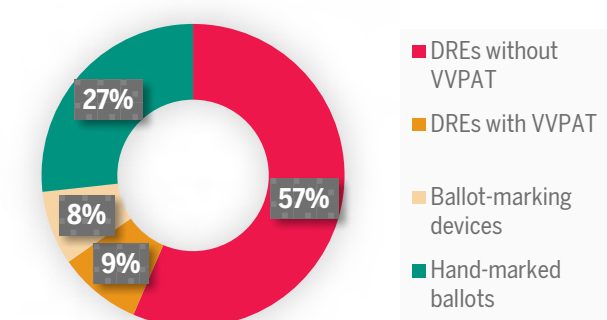


Indiana has about 4.5 million registered voters. While most U.S. voters live in jurisdictions that use hand-marked ballots, most Indiana voters live in jurisdictions that use DREs (Figure 1). Indiana is one of only eight states to still use DRE machines without a verified voting paper audit trail (Table 2). In fact, almost 60 percent of all of the voting equipment used in Indiana does not have a paper record (Figure 2).

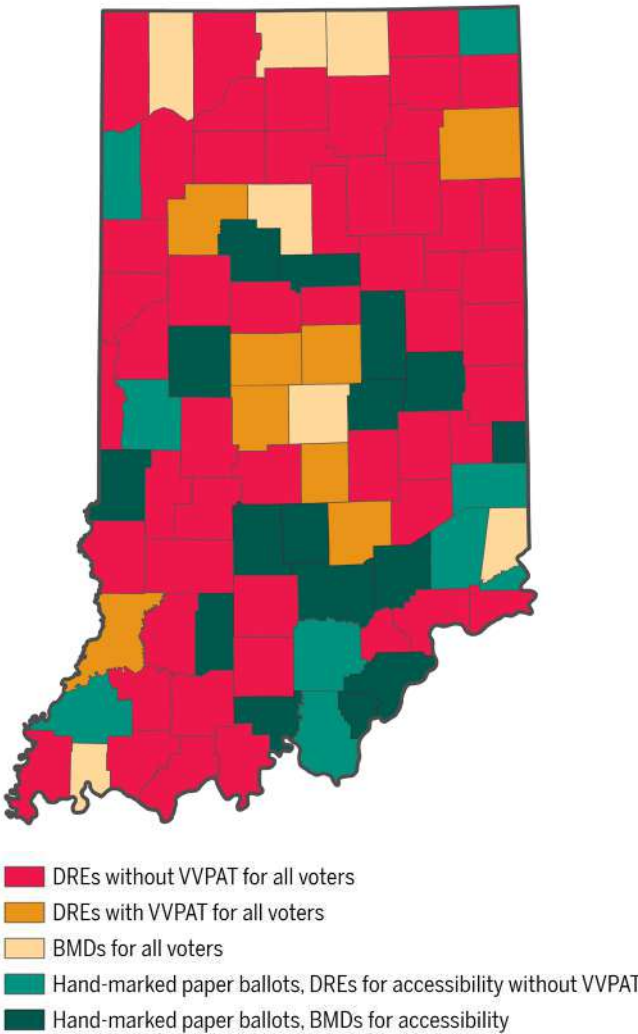
**TABLE 2.** States using voting equipment without a verified voting paper audit trail (2020)

STATE	PERCENTAGE OF JURISDICTIONS
Louisiana	100%
Mississippi	81%
New Jersey	81%
Tennessee	69%
Indiana	57%
Texas	37%
Kentucky	25%
Kansas	4%

**FIGURE 2.** Voting equipment in Indiana polling sites (2020)



**FIGURE 3.** Voting equipment in Indiana polling sites (2020)



Marion County is the most populated county in Indiana, with about 641,000 voters. All polling sites in Marion County currently use BMDs (Figure 3). In contrast, Allen and Hamilton Counties—the counties with the third and fourth most registered voters—use DREs with VVPAT. However,

both counties only have about half of the registered voters in Marion County. Only 16 of Indiana's 92 counties (17 percent) use hand-marked paper ballots with BMDs.

## IMPLICATIONS

Using voting machines without a paper audit trail can leave Indiana vulnerable to several election security issues. Without a paper record of votes that were cast, it can be difficult to detect breaches or errors in the system, or to verify vote totals if an issue is uncovered.<sup>2</sup> At a 2018 hacking conference, a computer scientist demonstrated that he could infiltrate a paperless DRE system to switch votes cast for one candidate into votes for the opponent. Because there was no paper trail of who voters selected on the ballot, there was no way to verify the true count of votes for each candidate.<sup>4</sup> These vulnerabilities were further highlighted in real-world cases during both the Georgia gubernatorial and Texas senate races of 2018. Complaints were filed in both states alleging that DREs used during the elections either deleted or switched votes, likely due to a software glitch blamed on outdated software and old machines.<sup>5</sup> These glitches due to old machines should be of concern in Indiana. In the 2016 election, 83 percent of Indiana counties used voting machines that were at least 8 years old.<sup>6</sup>

## DISCUSSION

Since the foreign interference in the 2016 U.S. elections, the U.S. Senate intelligence committee acknowledged that paper-based systems, such as paper ballots and optical scanners, were the least susceptible to cyberattack.<sup>7</sup> In response to security concerns, a law passed in 2019 requires that all Indiana counties move to paper trail voting systems by 2030.<sup>8</sup> However, concerns have been raised that this timeline leaves elections vulnerable to security risks for the next 10 years.<sup>9</sup> Although some Indiana jurisdictions have made progress in moving to paper-based voting systems,<sup>10</sup> a lack of funding has been cited as a reason for other jurisdictions' delays in securing paper trail voting machines.<sup>2</sup> In 2018, the Indiana Secretary of State requested \$75 million to update the state's voting machines with paper trail systems, but this amount was reduced to \$6 million due to other state funding priorities. This amount will only update 10 percent of DREs in the

state with a paper trail audit system,<sup>9</sup> highlighting the need for further funding to be devoted to securing paper-based voting systems.

## RECOMMENDATIONS

- Jurisdictions that are unable to update their machines prior to the November 2020 election, should take extra care in storing, maintaining, and testing machines before and after the election.
- Local officials should adopt effective practices for machine maintenance, as well as support the training of poll workers for tackling system failures and emergencies on the election day.
- Election officials should consider upgrading their plans for post-election audits to catch miscounting of votes or to find manipulated votes.

## REFERENCES

1. Indiana Vote by Mail vs. Indiana Election Commission, 1:19-cv-4245 (Ind., U.S. District Court, Filed 2019). <https://www.courthousenews.com/wp-content/uploads/2019/10/indiana-voting.pdf>.
2. Gambhir, R. J. & Karsten, J. (2019). Why paper is considered state-of-the-art voting technology. *Brookings Institute*. <https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/>.
3. Verifier Tool (2020). *Verified Voting*. <https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020>.
4. Halpern, S. (2018). Election-hacking lessons from the 2018 DEF CON Hackers Conference. *The New Yorker*. <https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers-conference>
5. Vasquez, C. & Choi, M. (2018). Voting machine errors already roil Texas and Georgia races. *Politico*. <https://www.politico.com/story/2018/11/05/voting-machine-errors-texas-georgia-2018-elections-midterms-959980>
6. Rabinowitz, K. (2018). Election security a high priority—Until it comes to paying for new voting machines. *ProPublica*. <https://www.propublica.org/article/election-security-a-high-priority-until-it-comes-to-paying-for-new-voting-machines>
7. *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1, 58.*
8. Senate Bill 570. (2019). Indiana General Assembly. <http://iga.in.gov/legislative/2019/bills/senate/570#digest-heading>
9. Mack, J. L. (2019). Federal complaint filed to force upgrading Indiana voting machines by 2020 elections. *IndyStar*. <https://www.indystar.com/story/news/politics/elections/2019/10/17/federal-complaint-force-upgrade-indiana-voting-machines/4006287002/>
10. Geller, E., Jin, B., Hermani, J., & Farrell, M. B. (2019). The scramble to secure America's voting machines. *Politico*. <https://www.politico.com/interactives/2019/election-security-americas-voting-machines/index.html>



## INDIANA UNIVERSITY PUBLIC POLICY INSTITUTE

The IU Public Policy Institute delivers unbiased research and data-driven, objective, expert policy analysis to help public, private, and nonprofit sectors make important decisions that impact quality of life in Indiana and throughout the nation. As a multidisciplinary institute within the Paul H. O'Neill School of Public and Environmental Affairs, PPI also supports the Center for Health & Justice Research (CHJR), the Center for Research on Inclusion & Social Policy (CRISP), the Manufacturing Policy Initiative (MPI), and the Indiana Advisory Commission on Intergovernmental Relations (IACIR).

### PREPARED BY

**Katie Rukes**, PPI Program Analyst

**Joti K. Martin**, PPI Policy Analyst

**Shreya Paul**, PPI Research Assistant

with assistance from **Karla Camacho-Reyes**, CRISP Special Projects Coordinator

101 W. Ohio Street, Suite 400  
Indianapolis, IN 46204

**Phone:** (317) 278-1305

**Email:** [iuppi@iu.edu](mailto:iuppi@iu.edu)

[policyinstitute.iu.edu](http://policyinstitute.iu.edu)

Follow us on Twitter

[@IUPublicPolicy](https://twitter.com/IUPublicPolicy)

LinkedIn

[Indiana University Public Policy Institute](https://www.linkedin.com/company/indiana-university-public-policy-institute/)

JULY 26, 2018



# Public Citizen Calls on Largest Voting Machine Vendor to Stop Selling Machines That Connect to the Internet, Increase Costs to Taxpayers

July 26, 2018

**Public Citizen Calls on Largest Voting Machine Vendor to Stop Selling Machines That Connect to the Internet, Increase Costs to Taxpayers**

***Modems Make Machines Vulnerable to Hacking and Fail to Meet Federal Standards***

WASHINGTON, D.C. – Election Systems and Software (ES&S) must stop selling vote counting machines with modems because they make such machines vulnerable to hacking, Public Citizen said today in a [letter](#) (PDF) to the Nebraska-based company. In addition, Public Citizen called on the company to remove remote access software from machines it already has sold.

“ES&S has made American democracy even more vulnerable to a growing and unprecedented threat of hacking by entities both foreign and domestic,” said Aquene Freechild, Democracy Is For People Campaign co-director. “Instead of apologizing and addressing concerns from the intelligence community, Congress, election officials and concerned citizens, ES&S is selling voting machines with modems to connect them to the internet.”

On its website, the company advertises modems as a key feature of its popular DS200 ballot scanners. But in fact, the modems are an optional add-on and with them the machines do not meet U.S. Election Assistance guidelines. In addition to being a security risk, the modems aren’t cheap, costing \$249 a piece according to an ES&S contract with [Michigan counties](#) (PDF) from 2017. Some counties buy hundreds of these machines at a time, and these charges are paid for by taxpayers.

ES&S is the largest voting system vendor in the U.S. market and provides voting systems for 43.8 percent of U.S. voters, according to a 2017 [report](#) (PDF) by the Wharton School of Business.

A second concern is that some ES&S machines contain software that enables technicians to access the machines remotely. According to a [Motherboard article](#), ES&S admitted in a letter to U.S. Sen. Ron Wyden (D-Ore.) that it installed the remote access software pcAnywhere in machines sold between 2000 and 2007, although the company said it has not done so since 2008.

Allowing remote access also makes the machines vulnerable to hacking in general, as the pcAnywhere software contains [flaws](#) that could allow [unauthorized actors](#) to take control of the machines. The source code for pcAnywhere was stolen by [hackers in 2006](#) and posted online in 2012, leading the software developer to call on users to uninstall pcAnywhere while a patch was developed. Such hacks illustrate the danger of creating remote access “[back doors](#)” in voting systems. For that reason, Public Citizen is calling on ES&S to remove the software from every voting system still in use. If removing the software is not possible, the company should compensate election officials who may need to purchase new machines without this security vulnerability.

Public Citizen sent the letter to elections officials in all 50 states, calling on them to ensure their voting machines do not have modems or remote access software installed, especially after foreign actors took a documented interest in U.S. voting machines during the 2016 elections.

### **Why Modems Pose a Security Risk**

Modems provide a connection to the internet and cell networks that make voting machines more vulnerable to hacking. A common talking point in defense of current voting systems is that they are “air-gapped,” which means that the machines are not connected to the internet, cell networks or other machines, and thus less vulnerable to cyberattacks from those sources.

Rhode Island officials using the DS200s with modems claim the modems are active only for [a minute](#) at the end of the evening when reporting the vote totals, and that the reported totals are unofficial. The problem is that very little time is needed to breach the modem, and malware, once installed, could impact vote totals in future elections. Further, it is reasonable to assume that, at least in some cases, the modems are activated during pre-election testing or poll worker training. As with other types of hacks, intelligently designed malware can be difficult to detect.

The [New York Times Magazine](#) reported on the problem of modems in voting machines in February, describing how a hacker could access vote tabulating machines via a device called a [Stingray](#) or by hacking the phone routing network. A hacker could fool the modems into communicating with the hacker as if they



were an authorized network, allowing the hacker to install malware that could change current or future election results.

Even so-called “air-gapped” voting machines are vulnerable to hacking. Such machines still must be programmed before each election. Bugs and hacks can be introduced to the machines through the vendor and by maintenance staff through the programming process. As a result, a breach of the vendor electronically or by staff could result in malware being installed on air-gapped voting machines. Checking the machine vote count by doing a rigorous post-election audit is the best way to detect any problems with the count and to recover from an attack.

### **Voting Machines With Modems Lack Federal Certification**

Many states rely on U.S. Election Assistance Commission (EAC) guidelines when they certify systems for local use. ES&S doesn’t hide that its DS200 scanner includes a modem. On one page of its website, the company lists the “modem” as the first asset of the scanner for reporting election results from the polling location.

But election officials may not be aware that the DS200 is not federally certified if it includes a modem or other connectivity equipment. Another page on the ES&S website claims that the D200 with the modem feature is “fully compliant with the usability, accessibility, and security enhancements found in the [U.S. Election Assistance Commission Guidelines known as] 2005 Voluntary Voting Systems Guidelines.” But bidding documents issued by the company illustrate that the internet connectivity components are not EAC certified. Federal certification is not required by all states and EAC guidelines serve as an important quality floor for election officials and vendors, helping to determine what minimum features should be required in new voting systems.

### **Insecure Technology at High Prices**

In addition to posing a security threat, the modems add significant cost to the voting systems. ES&S quoted Michigan (PDF) a price of \$249 per modem in 2017, and a single county needed 391—for a total cost of \$97,359 for only that county. Public officials should beware of spending taxpayer dollars on this insecure technology.

Some states, like New York and California, modified their contracts to block modems from being installed in their DS200 scanners. But other states, including Minnesota, Wisconsin, Rhode Island and Michigan, have at least some counties with modems in place. According to news reports, the second largest voting machine company, Dominion Voting Systems, has also sold ballot scanners with wireless connectivity. In 2015, Maryland contracted to buy DS200s; although the contract originally included modems, the state revised their contract to exclude them, saving taxpayers \$1.3 million (PDF).

The public may be shocked that election officials allow modems in voting machines given prominent hacking attacks in recent elections. McClatchy [reported](#) that ES&S maintains an “advisory board” of election officials, some of whom reportedly accepted trips to Las Vegas, lodging and meals from the corporation.

### **A Troubled History**

ES&S has run into trouble for connecting voting machines to the internet and installing remote access software in them. Earlier this year, U.S. Sen. Ron Wyden (D-Or.) sent a [letter](#) (PDF) to ES&S inquiring about the firm’s security practices.

ES&S initially did not answer Wyden’s detailed questions about security. In response to a question from the New York Times in spring 2018, the company denied any knowledge that its voting systems were ever sold with remote-access software, although in 2006 and 2011 remote access software was discovered in ES&S vote tabulating systems. In its [initial response](#) (PDF) to Wyden, ES&S implied that all its voting systems follow federal security guidelines, even though modems or remote access software make these systems noncompliant. But on July 17, 2018, a journalist obtained another response from ES&S to Wyden, in which it admitted that the company did in fact knowingly install remote access software in its machines between 2000 and 2007. It’s unclear if the company plans to remove or disable pcAnywhere software in machines already in use.

Last March, Sens. Amy Klobuchar (D-Minn.) and Jeanne Shaheen (D-N.H.) sent a [letter](#) to the country’s three largest voting system vendors – ES&S, Dominion Voting Systems and Hart Intercivic – asking whether the corporations have to share the source code for their voting systems with the Russian government for regulatory review. Some software companies have been asked to share their source code with Russian authorities in order to be able to access to the Russian market.

One of the biggest concerns is that the vendors or maintenance staff who typically have access to the machines could be compromised. A Florida-based [election system contractor](#) was hacked before the 2016 election.

[Reuse of passwords](#) is also a likely concern for voting machine vendors and election administrators. Hacks of large sites like LinkedIn have swept up passwords used by dozens of ES&S employees, which could be used to access work machines.

Other vendors have used easily guessable passwords such as [‘abcde’](#) and [‘admin,’](#) or posted the firewall configurations and password of their voting system online.

### **The Election Security Crisis**

There is consensus within Congress, the U.S. intelligence community and the election security community that U.S. elections remain vulnerable to hacks and

computer error. Yet too little has changed in many states and counties. Some states and counties are doing everything they can with the funding available but need more money. Other states and counties have changed little since before the 2016 election.

The hacks of [Yahoo](#), [LinkedIn](#), and [Experian](#) – which sometimes when undetected for years – illustrate that corporate entities with enormous security budgets remain vulnerable. Local governments running elections have far fewer resources available to protect voter data and voting systems.

### **Recovery Remains Critical**

The election security advocacy community has been focused on critical tools for recovery in case of a hack – paper ballots, audits to check the paper against the machine count and recovery systems, should the voter rolls be hacked. Recovery systems are critical because no system is perfectly secure. Although audits of paper ballots would expose any mismatch between machine tallies and the votes on paper, allowing election administrators to find both computer errors and hacks, only a handful of states conduct rigorous post-election [audits](#).

Local election officials run America's elections in most states, receiving help from state election officials and sometimes the federal government at their discretion. Members of Congress, the intelligence and [election security community](#) are raising [concerns](#) that stronger preventative measures to protect voting systems need to be taken ahead of the 2018 general election.

The last thing we need to be doing is make voting systems less secure by purchasing new voting systems that have hackable modems in them.

###





BOWEN CENTER FOR PUBLIC AFFAIRS  
DEPARTMENT OF POLITICAL SCIENCE

Muncie, Indiana 47306-0082  
Phone: 765-285-8982  
Fax: 765-285-5894

October 30, 2013

The Honorable Connie Lawson  
Secretary of State of Indiana  
201 State House  
302 West Washington Street  
Indianapolis, IN 46204

Dear Secretary Lawson:

The Voting System Technical Oversight Program (VSTOP) is pleased to present the enclosed documents for your review and approval.

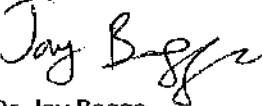
These documents, **Indiana Electronic Poll Book Certification Test Protocol for the Voting System Technical Oversight Program** and **CERTIFICATION TEST REPORT FOR EXAMINATION OF ELECTRONIC POLL BOOK FOR THE VOTING SYSTEM TECHNICAL OVERSIGHT PROGRAM**, have been developed following extensive consultation with nationally accredited testing laboratories and electronic pollbook vendors. We believe that these documents have been significantly improved by the comments and suggestions we have received from the laboratories, vendors, and members of the Election Division staff.

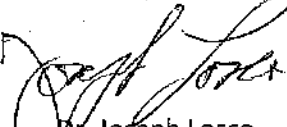
The development of these protocols has also helped us identify further practical issues in the implementation of the new technology employed in electronic poll books. Resolving some of these issues may require legislation for the 2014 session (such as refining our terminology to distinguish between "electronic poll lists" and "electronic poll books", or in clarifying how counties using electronic pollbooks should implement existing laws permitting a voter to indicate a change of name or change of address within a precinct by "writing on the poll list"). Other issues and our experiences in implementing these protocols may require future revisions to the documents, which we will submit to you for further consideration.

We are eager to proceed with testing and certification process regarding the pending applications from five ePollBook vendors, and expect to receive additional applications after these documents are approved.

We join with you in celebrating in achieving this milestone in Indiana's groundbreaking implementation of the electronic pollbook certification process. VSTOP is confident that these documents will be useful to other states that consider undertaking this important process.

Respectfully submitted by the VSTOP Team,

  
Dr. Jay Bagga

  
Dr. Joseph Losco

  
Dr. Ray Scheele

Attachments:

1. **Indiana Electronic Poll Book Certification Test Protocol for the Voting System Technical Oversight Program**
2. **CERTIFICATION TEST REPORT FOR EXAMINATION OF ELECTRONIC POLL BOOK FOR THE VOTING SYSTEM TECHNICAL OVERSIGHT PROGRAM**