Pamela Holmes

From: Elections Internet <Elections@sos.texas.gov>
Sent: Friday, March 15, 2019 11:32 AM
Subject: MASS EMAIL-- (EA/VR/CJ 1139) -- Election Security Assessment Guidance
Attachments: Joint Letter to County Elections Administrators_8.29.18.pdf; Shared Services ILC - TEMPLATE.PDF; MSS Terms and Conditions - TEMPLATE.PDF; ESA SPP - TEMPLATE.pdf

Sensitivity: Personal

County Election Officials,

As you may be aware, Texas received funding from the US Election Assistance Commission ("EAC") as a result of the 2018 Help America Vote Act ("HAVA") Security Funding. As we announced in the attached joint letter in August of 2018, the Texas Secretary of State ("SOS") has partnered with the Texas Department of Information Resources ("DIR") to provide an Election Security Assessment ("ESA") program through DIR's Shared Technology Services, Managed Security Services ("MSS"). DIR has contracted with AT&T as its MSS vendor, who has partnered with CyberDefenses for the ESA project. The ESA is designed to provide recommendations to improve the security of the election process at the county level through a comprehensive review of the procedures, technology and affected staff.

To the counties that have already participated, we want to say -- Thank You. These counties have provided extremely helpful and positive feedback. For those that have not yet executed the necessary documents to schedule an assessment, I want to take a few moments to provide a general overview of this important program and encourage your county's participation.

How to participate:

First and foremost, if you haven't already been contacted by AT&T or if you have been contacted and wish to proceed with an assessment, please reach out to Gene Moore – AT&T – gm4738@att.com, 214-794-3149. Gene will gather the information needed to move to the next step, and will be your contact person during the preparation phase of the assessment.

To participate in the project, there are three contractual components:

1. Interlocal Contract ("ILC") for Shared Technology Services between the county and DIR, which requires a signature, along with Terms and Conditions for Managed Security Services. This allows the counties to participate in the Shared Technology Services MSS Program.

2. Solutions Proposal Package ("SPP"), which is similar to a scope of work and contains responsibilities for both parties. The SPP has been pre-negotiated by DIR, SOS, and AT&T. No changes can be made to the SPP without SOS approval and will only be considered on a very limited basis.

3. Certifications required by SOS:
   - The county has identified a Single Point of Contact ("SPOC") who will be responsible for coordinating the ESA effort with county staff, including election management, voter registration, IT, and other affected staff.
   - The agreement/project has been approved by Commissioners Court, or the project does not require Commissioners Court approval and the SPOC is authorized to sign.
   - The county accepts the SPP without changes or accepts the SPP with changes if agreed to by SOS and DIR.

County approval:

Pamela Holmes

From: Elections Internet <Elections@sos.texas.gov>
Sent: Monday, August 12, 2019 1:23 PM
Subject: Mass Email Advisory (CC/EA/VR) Advisory 2019-12 - House Bill 1421 and Election Security Assessments

Flag Status: Flagged

Dear County Election Officials:

As you may know, the 86th Texas Legislature passed HB 1421, imposing certain requirements on the Secretary of State ("SOS") and counties as it pertains to election security. We have issued Advisory 2019-12 - House Bill 1421 and Election Security Assessments to explain the obligations imposed by this legislation.

There are two requirements that we want to draw your attention to:

1. **Election Security Assessments:** HB 1421 provides that a county election officer must request an assessment of the cybersecurity of the county's election system from a qualified provider if SOS recommends an assessment and the necessary funds are available. Because funds are available and SOS has recommended the assessment, it is required that each county receive one. We want to make this process as streamlined as possible. Keep in mind that no county funds are required for the election security assessments – SOS will pay DIR directly for your county's assessment. If your county has not executed all of the necessary steps to schedule an assessment, please reach out to Gene Moore – AT&T – gm4738@att.com, 214-794-3149, as soon as possible. Gene will gather the required information, and will be your contact person during the preparation phase of the assessment. Additionally, if you have any questions for DIR, please call 1-855-275-3471 and ask to be connected to a Shared Services Contract Manager or email dirsharedservices@dir.texas.gov. If you have a county purchaser, it might be helpful to engage that person as well since they may be familiar with DIR.

2. **County Cybersecurity Training**: HB 1421 requires county election officers to request training from the SOS on cybersecurity. The training we are providing is through The SANS Institute and is called "Securing the Human." This is a web-based training course. To sign up for the training, please complete the form at the provided link, so that we can assign your county users to the training modules. Every individual with TEAM access must complete this training by September 30, 2019. Users who have not completed their security training by this date will lose access to TEAM. If you have any additional questions about obtaining log-in credentials for the training, please contact us at electionsecurity@sos.texas.gov.

We hope this information has been helpful to you and we look forward to assisting you with your training needs. Please let us know if you have any questions or concerns.

Christina Worrell Adkins
Legal Director – Elections Division
Office of the Texas Secretary of State
1019 Brazos Street | Rudder Building, 2nd Floor | Austin, Texas 78701
1.800.252.VOTE (8683)
elections@sos.texas.gov | www.sos.texas.gov

We recognize counties operate differently, and we want to make sure the engagement is authorized through the appropriate channels within the county while making the process as simple as possible. For example, we don't want you to have to go before Commissioners Court more than once to obtain the necessary approvals for all documents pertaining to this project. To that end, I've attached generic (template) copies of the ILC, Terms and Conditions, and the SPP for you and stakeholders within your county to review and present to Commissioners Court, preferably at the same time. Official documents with the county's name on it will come at various stages in the process (more on that below).

We recommend Commissioners Court be advised of the following:

- ✓ The ESA is being funded with the 2018 HAVA Election Security Grant Funds authorized under Title I, Section 101 of the Help America Vote Act of 2002, which will be paid by SOS to DIR on the county's behalf. Costs within the project's scope have been pre-negotiated. The county WILL NOT be invoiced.

- ✓ A Single Point of Contact will need to be designated who will be responsible for coordinating the ESA effort with county staff, including election management, voter registration, IT, and other affected staff. It would also be beneficial for the SPOC to have some decision-making and signature authority. For instance, the ILC and Terms and Conditions with the county's name can be made available at the Commissioners Court meeting if coordinated with AT&T; however, the SPP will not be available until the County is "on-boarded" into the MSS program (approx. 5 days after returning the signed ILC). Therefore, it would be beneficial for the SPOC to have signature authority to avoid having to go back to Commissioners Court for SPP approval. Since the SPP template attached to this email will be the same, less the county name, our hope is that it will be sufficient for the Commissioners Court to sign off on and give the SPOC the authority to officially approve it once the county has been "on-boarded" into the MSS program. In addition, a Project Acceptance Letter (PAL) will have to be approved at the end of the project stating that the county has received the assessment report and acknowledges that the project can close.

- ✓ The areas that will be reviewed include the voter registration (VR) system, VR application storage, staff security knowledge, election devices, ballot creation process and tools, election results publication and tools, non-connected network and systems, general computer/endpoints, security devices, internet connected election network, network access, vulnerability detection, management tools, maintenance and remote support, threat intelligence, social engineering, external web-site vulnerability testing, third-party risk assessments, and cyber security capability.

- ✓ The following deliverables are provided as the output of the ESA to the county:
  Election Security Assessment Scorecard
  Election Security Assessment Report
  The deliverables will be encrypted and made available through a restricted access server. The information will be presented to the county in a final "closeout" presentation by Cyberdefenses and AT&T. We suggest the counties only invite critical personnel for this review as the information may be sensitive in nature. In addition, to the extent that you receive public information requests for any of the deliverables, this information is protected from public disclosure under Section 552.139 of the Texas Government Code.

- ✓ AT&T and Cyberdefenses have vast experience in this field and understand the sensitivity and complexity of this endeavor. They will work with the county to determine the appropriate schedule as to not disrupt county operations, and all findings will remain completely confidential. For questions regarding the assessment process, please contact Elections@cyberdefenses.com.

I would like to emphasize the importance of your participation in this vital program. As DIR and its partners provide SOS with aggregate information, SOS will move onto phase two of the project, which will be remediation. In other words, the quicker we can complete the assessments, the quicker we can evaluate the use of grant funds for security enhancements at the county level.

Lastly, if you or any of the county stakeholders have any questions or concerns, please feel free to contact our office. I am always available and Dan Glotzer, our Election Funds Manager, is helping to coordinate this project with DIR and AT&T. He can be reached at dglotzer@sos.texas.gov, 512-463-9861.

Sincerely,

Keith Ingram
Director, Elections Division
Office of the Secretary of State
800-252-VOTE(8683)
www.sos.state.tx.us/elections/index.shtml
For Voter Related Information, please visit:

VOTETEXAS.GOV
POWERED BY THE TEXAS SECRETARY OF STATE

The information contained in this email is intended to provide advice and assistance in election matters per §31.004 of the Texas Election Code. It is not intended to serve as a legal opinion for any matter. Please review the law yourself, and consult with an attorney when your legal rights are involved.

See pg 2

Texas Secretary of State
Ruth R. Hughs

Note - Navigational menus along with other non-content related elements have been removed for your convenience. Thank you for visiting us online.

Election Advisory No. 2019-12

To: Election Officials

From: Keith Ingram, Director of Elections

Date: August 5, 2019

RE: House Bill 1421 and Election Security Assessments

In its 86th Regular Session (2019), the Texas Legislature enacted House Bill 1421, adding Chapter 279 to the Texas Election Code. The new Chapter 279—titled "Cybersecurity of Election Systems"—defines key election terms and imposes requirements on the Secretary of State and county election officers related to election security. HB 1421 takes effect September 1, 2019.

Election Security Best Practices

Under Section 279.002 of the Texas Election Code, the Secretary of State is required to adopt rules that (1) define classes of protected election data, and (2) establish best practices for identifying and reducing risk to the electronic use, storage, and transmission of election data and the security of election systems. The new legislation further provides that if state funds are available to assist counties, county election officers must implement cybersecurity measures to ensure that all devices with access to election data comply to the highest extent possible with the rules promulgated by the Secretary of State.

The Secretary of State's office is working with information security resources and county election officials to develop these best practices. When they are finalized, we will be sending out an election law advisory regarding these new policies and procedures.

Training Requirements

Under Section 279.002, the Secretary of State is required to offer training on election security best practices to all appropriate personnel in the Secretary of State's office and, on request, to county election officers. County election officers are required to request such training on an annual basis. All costs associated with such training shall be paid for by the Secretary of State with available state funds. The training will be web-based unless a county election officer requests in-person training, which will be provided when feasible. The Secretary of State will monitor web-based training compliance via the TEAM application. All users to TEAM will be required to complete this security training to maintain access to TEAM.

We will be sending out a separate email with instructions on how to request training for your county office. Please note that training will become available immediately and must be completed by **September 30, 2019. Users who have not completed their security training by this date will no longer be allowed to access the TEAM application.**

Breach Notification Requirements

HB 1421 also contains reporting requirements related to cybersecurity breaches. First, it states that if a county election officer becomes aware of a breach of cybersecurity that affects election data, the officer shall immediately notify the Secretary of State of such breach. Additionally, the bill provides that if the Secretary of State becomes aware of a cybersecurity breach, the Secretary shall immediately provide notice of the breach to members of the standing committees of each house of the legislature with jurisdiction over elections.

Once a county election officer becomes aware of a potential breach, they should make contact with the Secretary of State's office within 24 hours of receiving such notification. County election officers can report cybersecurity breaches by contacting the Secretary of State's office in person or by phone or email. The communication should be directed to the Director of Elections or the agency IT director. The best practices that our office is currently developing will include examples of reportable breaches and the necessary protocols to follow.

Election Security Assessments

HB 1421 also provides that if there are state funds available and the Secretary of State recommends an assessment, a county election officer shall request an assessment of the cybersecurity of the county's election system from a provider of cybersecurity assessments. Texas has received funding from the U.S. Election Assistance Commission as a result of the 2018 Help America Vote Act ("HAVA") Security Funding. As we announced in August 2018, the Secretary of State has partnered with the Texas Department of Information Resources ("DIR") to provide an Election Security Assessment ("ESA") program through DIR's shared services contract. At the time the program was created, the ESAs were optional. HB 1421 makes these assessments **mandatory for all counties**.

All paperwork associated with initiating a county ESA must be completed by December 31, 2019. Counties must complete their ESA by July 31, 2020.

If you have not already scheduled your ESA, please contact elecassessment@sos.texas.gov for more details about the program.

Funding for Remediation

The Secretary of State is working with the DIR ESA vendor to develop remediation strategies and tools that will benefit counties statewide. Having an assessment will make those tools more understandable and effective. In addition, SOS will not be able to assess funding options for county-specific remediation recommendations until a significant number of counties have completed the ESAs. In other words, counties that do not complete an assessment in a timely manner may not benefit from additional HAVA-funded products and services.

KI:CA

H.B. No. 1421

AN ACT

relating to cybersecurity of voter registration lists and other election-related documents, systems, and technology.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Title 16, Election Code, is amended by adding Chapter 279 to read as follows:

CHAPTER 279. CYBERSECURITY OF ELECTION SYSTEMS

Sec. 279.001. DEFINITIONS. In this chapter:

(1) "County election officer" means an individual employed by a county as an elections administrator, voter registrar, county clerk, or other officer with responsibilities relating to the administration of elections.

(2) "Election data" means information that is created or managed in the operation of an election system.

(3) "Election system" means a voting system and the technology used to support the conduct of an election, including the election data processed or produced in the course of conducting an election, such as voter registration information, ballot information, collected and tabulated votes, election management processes and procedures, and other election-related documents and election data.

Sec. 279.002. ELECTION CYBERSECURITY: SECRETARY OF STATE. (a) The secretary of state shall adopt rules defining classes of protected election data and establishing best practices for identifying and reducing risk to the electronic use, storage, and transmission of election data and the security of election systems.

(b) The secretary of state shall offer training on best practices:

(1) on an annual basis, to all appropriate personnel in the secretary of state's office; and

(2) on request, to county election officers in this state.

(c) If the secretary of state becomes aware of a breach of cybersecurity that impacts election data, the secretary shall immediately notify the members of the standing committees of each house of the legislature with jurisdiction over elections.

Sec. 279.003. ELECTION CYBERSECURITY: COUNTY ELECTION OFFICERS. (a) A county election officer shall annually request training on cybersecurity from the secretary of state. The secretary of state shall pay the costs associated with the training with available state funds.

(b) A county election officer shall request an assessment of the cybersecurity of the county's election system from a provider of cybersecurity assessments if the secretary of state recommends an assessment and the necessary funds are available.

(c) If a county election officer becomes aware of a breach of cybersecurity that impacts election data, the officer shall immediately notify the secretary of state.

(d) To the extent that state funds are available for the purpose, a county election officer shall implement cybersecurity measures to ensure that all devices with access to election data comply to the highest extent possible with rules adopted by the secretary of state under Section 279.002.

SECTION 2. This Act takes effect September 1, 2019.

President of the Senate

Speaker of the House

I certify that H.B. No. 1421 was passed by the House on April 16, 2019, by the following vote: Yeas 121, Nays 15, 1 present, not voting; and that the House concurred in Senate amendments to H.B. No. 1421 on May 23, 2019, by the following vote: Yeas 115, Nays 23, 1 present, not voting.

Chief Clerk of the House

I certify that H.B. No. 1421 was passed by the Senate, with amendments, on May 21, 2019, by the following vote: Yeas 31, Nays 0.

Secretary of the Senate

APPROVED: _____
Date

_____
Governor