Mensaje del Director sobre Ciberseguridad

Como estoy seguro de que todos ustedes ya saben, uno de los principales puntos de interés para esta Elección General es la ciberseguridad. Específicamente, los miembros del público quieren saber los pasos que estamos tomando para garantizar que nuestros sistemas electorales sean seguros, que los votos no se alteren y que se proteja la integridad de los votos.

En primer lugar, es importante tener en cuenta lo siguiente:

1. Utilizamos boletas de papel, por lo que tenemos una copia de seguridad de los resultados que informamos en la Noche de Elecciones.

2. Después de cada elección, realizamos una auditoría a mano de una muestra de las papeletas y la comparamos con nuestros resultados informados. Esta práctica nos ayuda a encontrar cualquier discrepancia entre nuestros resultados informados y los votos reales como resultado de un ciberataque en nuestro equipo o sistema de tabulación.

3. Nuestros sistemas de tabulación y equipo de votación no están conectados a Internet ni están conectados a ninguna otra red.

4. Tenemos un equilibrio bipartidista entre los 85 empleados de CCBOE. Ninguna persona sola puede tener acceso al la cámara de papeletas. Esto requiere dos personas, una R y una D, cada una de las cuales tiene un código de acceso. Para poder ingresar, el sistema requiere tanto el código de acceso R como el código de acceso D.

Estas cuatro prácticas se han implementado en muchas elecciones y son una de las razones principales por las que todavía no hemos experimentado una brecha de seguridad cibernética crítica. En muchos sentidos, ya nos pusieron por delante del juego con la ciberseguridad. Sin embargo, todavía se puede hacer más para reforzar aún más nuestros sistemas de seguridad.

No es ningún secreto que la manipulación de las elecciones es una amenaza creíble en la sociedad actual. En respuesta a esto, el gobierno federal proporcionó $ 380 millones a los estados para fondos de ciberseguridad (Ohio ha recibido $ 12 millones de esta suma). Como resultado, el Secretario de Estado de Ohio ha mejorado su infraestructura de TI y ha actualizado la base de datos de registro de votantes en todo el estado con características de seguridad adicionales. El SOS también ha celebrado varias sesiones de capacitación temáticas sobre seguridad cibernética en todo el estado, a las que asistieron CCBOE y empleados de TI del condado.

Otro requisito del Secretario de Estado es que los BOE creen una Evaluación de Seguridad de Infraestructura Electoral. Nos estamos asociando con un consultor privado de ciberseguridad que someterá nuestros sistemas a una variedad de pruebas, tomando nota de qué áreas necesitan más mejoras. Entonces podremos solucionar directamente esas áreas.

Con todas estas prácticas, confiamos en que hemos reducido significativamente nuestra vulnerabilidad a un ataque cibernético. Sin embargo, esto no significa que podamos relajarnos en nuestra vigilancia

cuando estamos observando. Si alguna vez se encuentra con alguna actividad sospechosa, es importante que nos notifique de inmediato llamando al (216) 443-8683.