Este documento fue creado como parte del Consejo de Coordinación Gubernamental de Infraestructura Electoral y del Grupo de Trabajo Conjunto del Plan Específico de Subsector del Consejo de Coordinación de Subsector.

Actualización del estado del plan específico del subsector de infraestructura electoral 2022

En enero de 2017, el Departamento de Seguridad Nacional (DHS) estableció el Subsector de Infraestructura Electoral bajo el Sector de Instalaciones Gubernamentales a través de una designación de infraestructura crítica para la infraestructura electoral. La designación deja en claro tanto a nivel nacional como internacional que la infraestructura electoral disfruta de todos los beneficios y protecciones de la infraestructura crítica que el gobierno de los EE. UU. tiene para ofrecer.[1]

Desde sus inicios, el subsector ha establecido y desarrollado alianzas sólidas entre las partes interesadas del gobierno a nivel local, estatal y federal y entre los sectores público y privado, formando tanto un Consejo Coordinador Gubernamental (CCG) como un Consejo Coordinador Sectorial (CCS). Estos organismos han brindado un mecanismo enfocado en la colaboración entre los funcionarios electorales estatales y locales, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Comisión de Asistencia Electoral (EAC), las fuerzas del orden público, la comunidad de inteligencia y los socios del sector privado para mejorar el intercambio de información sobre riesgos para los sistemas electorales de la nación, identificar recursos para ayudar a mitigar dichos riesgos, comunicar las mejores prácticas, abordar las vulnerabilidades identificadas y permitir el acceso de los funcionarios electorales y partes del sector privado a la información sobre amenazas.

El Plan Específico del Subsector de Infraestructura Electoral Conjunta (SSP, por sus siglas en inglés), inicialmente aprobado por el GCC y el SCC en 2020, proporcionó un marco para que la industria y los socios gubernamentales establecieran prioridades compartidas para los esfuerzos de seguridad frente a las amenazas a la infraestructura electoral, al mismo tiempo que establecía un camino para la colaboración continua y el desarrollo de capacidades. Desde la aprobación del SSP conjunto, el entorno de amenazas ha evolucionado y el subsector ha respondido con nuevos procesos y capacidades. En consecuencia, el SSP anterior ya no está operativo. El Plan Nacional de Protección de Infraestructura (Plan Nacional), que proporciona un marco de referencia para todos los sectores y subsectores de infraestructura crítica, está siendo revisado por CISA y sus partes interesadas y se espera que finalice a mediados de 2022. Está pendiente una actualización del Plan Específico del Subsector de Infraestructura Electoral, junto con el Plan Nacional actualizado.

Por ahora, este documento proporciona una guía provisional conjunta para la participación del Subsector de Infraestructura Electoral hasta las elecciones intermedias de 2022. Se enfoca en las actividades que el GCC y el SCC han identificado para abordar las prioridades de seguridad actuales del subsector. Estos esfuerzos tienen como objetivo impulsar las capacidades colectivas para responder a incidentes nacionales o de gran escala y desarrollar resiliencia en todo el ecosistema electoral a través del intercambio coordinado de información y la mitigación de riesgos.

---

1 La designación del Departamento de Seguridad Nacional de enero de 2017 define la “infraestructura electoral” de la siguiente manera:“*instalaciones de almacenamiento, lugares de votación y lugares centralizados de tabulación de votos utilizados para respaldar el proceso electoral, y tecnología de la información y las comunicaciones para incluir bases de datos de registro de votantes, máquinas de votación y otros sistemas para administrar el proceso electoral e informar y mostrar los resultados en nombre del estado y gobiernos locales”.* https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-electioninfrastructure-critical.

VISIÓN DEL SUBSECTOR DE INFRAESTRUCTURA ELECTORAL

Un enfoque unificado del gobierno y el sector privado para empoderar a la comunidad de interesados electorales para desarrollar resiliencia ante las amenazas y los riesgos de la infraestructura electoral.

MISIÓN DEL SUBSECTOR DE INFRAESTRUCTURA ELECTORAL

Coordinar los esfuerzos de los funcionarios electorales estatales y locales, el sector privado y los socios sin fines de lucro, y el gobierno federal para manejar los riesgos y asegurar la infraestructura electoral contra amenazas nuevas y en evolución.

Problemas actuales

Abordar la seguridad física de las instalaciones y el personal electoral

En el período previo y posterior a las elecciones generales de 2020, los funcionarios públicos y los particulares cuyos trabajos implicaban administrar elecciones o apoyar a quienes administran elecciones se convirtieron en objeto de teorías de conspiración y comunicaciones amenazantes. Las instalaciones electorales, incluidas las oficinas gubernamentales y los centros de tabulación, se convirtieron en el foco de protestas u otras actividades. Las instalaciones de la industria privada también fueron blanco de protestas u otras personas que amenazaron y/o buscaron interrumpir las operaciones comerciales.

Los funcionarios electorales estatales y locales deben equilibrar la seguridad con el acceso y la transparencia. Los funcionarios electorales operan según los principios de transparencia y acceso público abierto, lo que puede crear desafíos para adoptar principios y prácticas de seguridad física para proteger a los trabajadores y empleados. Los sitios de votación pueden ser objetivos fáciles debido a su acceso abierto y barreras de seguridad limitadas, y los trabajadores del día de las elecciones son en su mayoría empleados temporales.

CISA actualmente brinda a los sectores público y privado acceso a una amplia gama de capacitaciones, ejercicios y recursos de mejores prácticas que se enfocan en los métodos predominantes de ataque a la seguridad física (por ejemplo, tirador activo, embestida de vehículos y bombardeo), junto con las medidas de protección correspondientes a través de Seguridad física de Lugares de Votación e Instalaciones Electorales orientación que los funcionarios electorales y los socios del sector privado pueden usar para mejorar su postura de seguridad física. Recursos comunitarios también están disponibles a través del Centro de Programas y Asociaciones de Prevención del DHS para ayudar a prevenir que las personas se radicalicen hacia la violencia.

En julio de 2021, el Departamento de Justicia de EE. UU. (DOJ, por sus siglas en inglés) creó el Grupo de trabajo sobre amenazas contra los trabajadores electorales para liderar la respuesta de las fuerzas del orden público federales a las amenazas a la comunidad electoral y, cuando corresponda, para investigar penalmente y enjuiciar dichas amenazas. Además de repetidas comunicaciones informales y divulgación, los líderes del DOJ y los representantes del Grupo de Trabajo brindaron numerosas presentaciones a la comunidad electoral sobre recopilación, preservación e informes de amenazas, incluso en reuniones con la Asociación Nacional de Secretarios de Estado (NASS), la Asociación Nacional de Secretarios de Estado Directores Electorales (NASED), Centro Electoral y una variedad de otros grupos de partes interesadas.

El esfuerzo Last Mile de CISA proporciona carteles personalizables que las jurisdicciones pueden colocar en sus oficinas que detallan las leyes estatales específicas que rigen las amenazas, el acoso y otras actividades relevantes, así como la información de contacto de las fuerzas del orden público federales, estatales y locales. CISA también ha proporcionado recursos sobre prevención de doxing para ayudar a los miembros del subsector a tomar medidas para proteger su información personal antes de que pueda hacerse pública. Finalmente, la EAC creó una página web agregar información para los funcionarios electorales que experimentan amenazas, incluidos los recursos de salud mental para quienes experimentan amenazas, acoso otras comunicaciones no deseadas.

Hay trabajo por hacer continuamente para garantizar la seguridad tanto de las instalaciones electorales como de los propios miembros del subsector, incluido el desarrollo formal de protocolos para informar dicha actividad hostil.

Manejo de riesgos para la cadena de suministro

El gobierno federal ha priorizado los esfuerzos para crear conciencia sobre los riesgos asociados con las cadenas de suministro de la industria y los productos y/o servicios relacionados que pueden contener una funcionalidad potencialmente maliciosa, son falsificados o son vulnerables debido a las prácticas de fabricación y desarrollo. Comprender y adoptar procesos para garantizar la integridad, la seguridad, la resiliencia y la calidad del producto son todas consideraciones para los esfuerzos de gestión de riesgos de la cadena de suministro (SCRM).

En respuesta a la Orden Ejecutiva 13873, el Grupo de trabajo SCRM de tecnología de la información y las comunicaciones (TIC) de CISA trabajó con la industria y los socios gubernamentales para:

- Desarrollar una taxonomía estandarizada de elementos de TIC (por ejemplo, hardware, software y servicios)
- Realizar evaluaciones críticas sobre estos elementos de las TIC con los aportes apropiados de las partes interesadas
- Evaluar los riesgos de seguridad nacional derivados de las vulnerabilidades en el hardware, software y servicios de TIC, incluidos los componentes que permiten comunicaciones 5G.

Los representantes del Grupo de Trabajo se han reunido con los líderes del SCC de Infraestructura Electoral para mantener informados a los socios de la industria sobre su progreso.

En junio de 2021, el SCC de Infraestructura Electoral estableció un Grupo de Trabajo SCRM del Consejo de Coordinación Sectorial para explorar posibles prácticas y esfuerzos de mitigación de riesgos dentro del subsector. El grupo de trabajo SCRM busca ayudar a los proveedores de tecnología electoral y a los funcionarios electorales con las prácticas de adquisición de software, hardware y servicios relacionados con las elecciones para evaluar y reducir los riesgos para la jurisdicción electoral y sus socios de la cadena de suministro. En la economía global actual, es casi imposible no confiar en una cadena de suministro que se extiende a todas partes del mundo. Como tal, la gestión de riesgos de la cadena de suministro es necesaria para garantizar que los funcionarios electorales y sus socios de la cadena de suministro solo adquieran software, hardware y servicios relacionados con las elecciones de fuentes legítimas que cuenten con un programa para garantizar la integridad de la cadena de suministro.

En febrero de 2022, el Subgrupo SCRM sobre papeletas electorales emitió un libro blanco que describe las mitigaciones de riesgos para los socios del subsector con respecto a las papeletas electorales y los sobres. El Grupo de Trabajo también publicó un documento en marzo de 2022 como una introducción sobre cómo las organizaciones y los socios de la cadena de suministro aguas abajo, incluidos los funcionarios electorales, pueden proteger mejor su cadena de suministro. Busca proporcionar la siguiente información relacionada con el manejo de riesgos de la cadena de suministro electoral:

- Brindar orientación al Grupo de trabajo SCRM sobre la gestión de riesgos de la cadena de suministro relacionada con el software electoral para ayudar a otros a adquirir software, hardware y servicios relacionados con las elecciones;

- Aprovechar los recursos existentes proporcionados por CISA y el Grupo de trabajo SCRM de ITC;

- Proporcionar listas de verificación y otros recursos que los proveedores de tecnología y los funcionarios electorales pueden usar para evaluar su estrategia de gestión de riesgos de la cadena de suministro de software electoral;

- Identificar las mejores prácticas con respecto a la gestión de riesgos de la cadena de suministro de software dentro de la comunidad electoral; y

- Comparta recursos a través de la comunidad electoral para aumentar la conciencia sobre las prácticas de gestión de riesgos de la cadena de suministro.

Este trabajo complementa los esfuerzos de una variedad de partes interesadas para actualizar las Directrices del Sistema de Votación Voluntaria federal (VVSG[2]), aprobado por la Comisión de Asistencia Electoral de los Estados Unidos (EAC). Estas pautas cubren las especificaciones de diseño, desarrollo y prueba de precisión, seguridad, funcionalidad, privacidad, facilidad de uso y accesibilidad de los sistemas de votación certificados. Los fabricantes de sistemas de votación que envían el sistema de votación a la EAC para su prueba y certificación actualmente brindan al gobierno federal una variedad de información sobre proveedores y proveedores de productos y componentes.

Asegurando la Cadena de Custodia

La atención pública prolongada sobre la administración de las elecciones significa que los procesos mediante los cuales los funcionarios electorales obtienen equipos y materiales están bajo la lupa. Conocidos como "cadena de custodia", estos procesos incluyen cómo los funcionarios garantizan la integridad continua de todo, desde boletas hasta libros de votación y máquinas de votación durante su ciclo de vida, incluido su control o transferencia de un lugar a otro o de persona a persona. Esto también puede extenderse a la información o los registros digitales para garantizar que la integridad y la confidencialidad no se vean comprometidas. Si bien cada estado y territorio tiene sus propios requisitos específicos de jurisdicción, es fundamental que los funcionarios electorales también comprendan el papel que desempeñan los procedimientos de cadena de custodia en la seguridad más amplia del ecosistema electoral. Además, la mayoría de los proveedores de apoyo electoral del sector privado tienen acuerdos contractuales que describen los permisos para el acceso de terceros a los equipos.

Según el DHS, las amenazas a la cadena de custodia pueden provocar interrupciones no programadas (es decir, mal funcionamiento del equipo), incidentes delictivos y ataques terroristas, incidentes cibernéticos, ataques a la cadena de suministro (explotación de vulnerabilidades para causar fallas en el sistema o la red) u operaciones de influencia extranjera (para propagar desinformación o socavar los procesos democráticos). Específicamente en las elecciones, la pérdida del control físico o digital de la cadena de custodia puede resultar en que las oficinas electorales no puedan garantizar que el equipo o los registros no hayan sido alterados o manipulados en violación de los procesos establecidos.

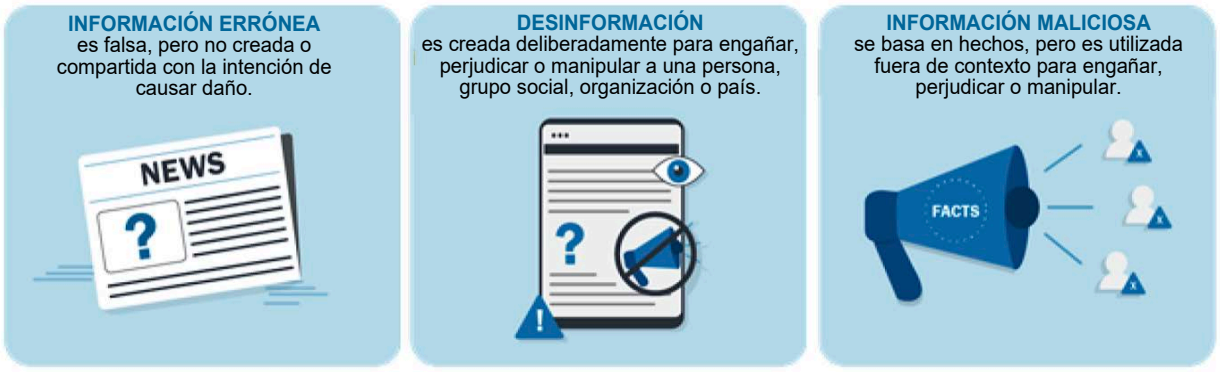
En 2021, ambos CISA y el EAC emitió documentos de orientación sobre la cadena de custodia centrados en la infraestructura crítica en general y las elecciones. Además, una capacitación CISA desarrollada recientemente,"Generar confianza a través de Prácticas Seguras", discute la implementación y comunicación de los procedimientos de cadena de custodia. Se necesita más educación y capacitación para ayudar a los funcionarios electorales a desarrollar e implementar protocolos de cadena de custodia, incluida la forma en que se relacionan con la integridad del subsector en general.

Además de educar a los miembros del subsector sobre los procedimientos de la cadena de custodia, los funcionarios electorales estatales y locales deben educar a sus partes interesadas (legisladores, apropiadores y votantes) sobre estos procesos para informar la toma de decisiones y combatir la información errónea, la desinformación y la mala información. Más recursos de capacitación del GCC sobre la cadena de custodia pueden ayudar a los funcionarios electorales estatales y locales a comunicarse de manera más efectiva sobre este tema.

[2] Voluntary Voting System Guidelines | U.S. Election Assistance Commission (eac.gov)

Contrarrestar la información errónea, la desinformación y la información electoral errónea

La información errónea, la desinformación y la información maliciosa (MDM) han representado durante mucho tiempo una amenaza para la seguridad y la integridad de las elecciones.[3] Si bien a menudo es inadvertida, la información errónea brinda a los votantes una orientación inexacta, como la fecha límite de registro de votantes o el lugar de votación incorrectos, y puede ser perjudicial hasta el punto de privar a los votantes de sus derechos. Las formas maliciosas de MDM son herramientas utilizadas para confundir intencionalmente a los votantes y socavar la confianza en el proceso electoral. Llevado al extremo, el MDM puede resultar en amenazas o violencia contra los trabajadores, funcionarios o voluntarios electorales.



Los funcionarios electorales individuales, los proveedores de la industria y otras organizaciones representadas por los consejos del subsector han implementado esfuerzos para contrarrestar el MDM. Por ejemplo, NASS lanzó #TrustedInfo iniciativa para alentar a los votantes a obtener información electoral directamente de los funcionarios electorales. CISA desarrolló Rumor página web de control y muchos estados individuales y jurisdicciones electorales locales y varios proveedores de tecnología electoral también produjeron páginas web de "control de rumores" o "mito versus realidad" para proporcionar información precisa sobre la administración electoral, la tecnología y la seguridad y para disipar la confusión de MDM y votantes.

Después de las elecciones de 2020, el GCC y el SCC lanzaron el Grupo de trabajo conjunto sobre información errónea/desinformación para aprovechar las oportunidades de coordinar esfuerzos en todo el subsector. Hasta el momento, el grupo de trabajo ha creado dos productos para ayudar a los funcionarios electorales estatales y locales y a los proveedores de la industria a prepararse y responder a los riesgos de MDM: el Guía de inicio de la página de control de rumores y el Planificación de MDM y respuesta a incidentes Guía para funcionarios electorales. El Grupo de trabajo conjunto sobre información errónea/desinformación proporciona un foro a través del cual el subsector puede continuar identificando desafíos para contrarrestar el MDM, y continuará produciendo recursos para abordar dichos desafíos.

Otro enfoque que ha adoptado el subsector para abordar el MDM es promover la adopción del .gov nivel dominio superior, disponible exclusivamente para los gobiernos de EE. UU. Obtener información de un sitio web .gov o una dirección de correo electrónico le permite al público tener la confianza de que la información que está viendo proviene de una fuente oficial del gobierno. A partir de abril de 2021, el programa .gov es administrado por CISA y está disponible sin costo alguno. Finalmente, los mecanismos de intercambio de información que se analizan a continuación brindan información y herramientas para crear conciencia sobre las narrativas de MDM y contrarrestarlas.

[3] Consejo Nacional de Inteligencia,Amenazas extranjeras a las elecciones federales de EE. UU. de 2020. Evaluación de la comunidad de inteligencia, ICA 2020-00078D, 10 de marzo de 2021, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections.

Intercambio de información a niveles clasificados y no clasificados

Desde sus inicios, los objetivos y logros iniciales del Consejo Coordinador del Subsector se centraron en mejorar el intercambio de información. El CCG estableció elInformación de Infraestructura Electoral Centro de intercambio y análisis (EI-ISAC) para respaldar la respuesta a incidentes, el análisis de tendencias y el intercambio de información en todo el subsector. Los miembros del SCC pertenecen a EI-ISAC como miembros de apoyo y se benefician del intercambio de información que proporciona. Un objetivo continuo de GCC y SCC es aumentar la membresía en EI-ISAC entre las jurisdicciones electorales pequeñas y medianas y los proveedores de la industria. La membresía de EI-ISAC ha superado las 3000 entidades y continúa creciendo.

El Grupo de Interés Especial de la Industria Electoral (EI-SIG) fue formado por separado por creadores de tecnología de la industria en 2018 a través del Centro de Análisis e Intercambio de Información de Tecnología de la Información (IT-ISAC). El EI-SIG continúa sirviendo como un vehículo importante para el intercambio de información, la capacitación y las iniciativas de seguridad centradas en la industria, incluida la adopción de políticas organizativas coordinadas de divulgación de vulnerabilidades.

Los miembros del subsector reciben regularmente información sobre amenazas de la comunidad de inteligencia de EE. UU. a través de ISAC y otras vías, como informes clasificados y no clasificados. Estos informes del DHS y sus socios federales, incluida la Oficina Federal de Investigaciones (FBI) y la Oficina del Director de Inteligencia Nacional (ODNI), permiten a los funcionarios electorales y proveedores de la industria mantenerse actualizados sobre las amenazas a la seguridad cibernética e influir en las operaciones de adversarios extranjeros. El subsector continúa agregando funcionarios electorales y proveedores de la industria al Programa de Autorización del Subsector de Infraestructura Electoral para que tengan acceso a las sesiones informativas clasificadas apropiadas.

Aunque tanto el Programa de Autorización del Subsector de Infraestructura Electoral como el EI-ISAC ayudan a distribuir información, el GCC y el SCC continúan abogando para que la comunidad de inteligencia rebaje rápidamente y comparta inteligencia procesable. Los informes y documentos no clasificados o solo para uso oficial se pueden compartir de manera más amplia dentro del subsector, especialmente con los funcionarios electorales locales, la gran mayoría de los cuales no tienen autorización de seguridad pero necesitan acceso a la información para proteger sus sistemas y personal. Las sesiones informativas no confidenciales también permiten que la comunidad electoral se beneficie de la experiencia del sector privado, lo que puede brindar una perspectiva diferente a la del gobierno federal.

El subsector busca cada vez más formas de compartir información sobre amenazas a la seguridad física de la infraestructura electoral, los lugares de votación y el personal. A medida que se acercan las elecciones intermedias de 2022, los Consejos de Subsector reconocen una necesidad continua de mejora relacionada con el intercambio de información de seguridad física, incluido el desarrollo de protocolos de intercambio de información.

El GCC continúa alentando el uso de sus protocolos voluntarios de intercambio de información sobre amenazas e informes de incidentes en todo el subsector. Estos protocolos aseguran que la información se comparta adecuadamente entre jurisdicciones para que cuando una jurisdicción se enfrente a una amenaza, las otras jurisdicciones puedan monitorear la misma amenaza. Los protocolos también orientan a los funcionarios electorales sobre los recursos de respuesta a incidentes.

El SCC actualizó su informe de incidentes de orientación general para las organizaciones miembro en 2021 y continúa utilizando este marco sujeto a todos los requisitos federales, estatales y locales para tales notificaciones.

Recursos para mejorar la seguridad electoral, incluida la ciberseguridad y los ataques de ransomware

Aunque el subsector se enfrenta a amenazas cada vez mayores de seguridad física y MDM, la ciberseguridad sigue siendo una prioridad constante. El GCC y el SCC tienen un enfoque sostenido en aumentar la disponibilidad y el uso de recursos, servicios y capacitación en seguridad cibernética de CISA, EI-ISAC y otros.

CISA, con la ayuda de GCC y SCC, alienta a los funcionarios electorales y proveedores de la industria a continuar utilizando sus evaluaciones de ciberseguridad y servicios de detección y prevención incluidos nuevos servicios que son más escalables para aumentar su alcance en más de 10,000 jurisdicciones electorales y proveedores de la industria. Además, además de aumentar su membresía para optimizar el intercambio de información, EI-ISAC está ampliando la participación en sus servicios agregados más recientemente, como Bloqueo de dominios maliciosos y Informes (MDBR).

El Grupo de trabajo de capacitación de GCC se amplió recientemente para incluir al SCC en un reconocimiento de la importancia de la capacitación en todo el subsector, no solo para los funcionarios electorales. El grupo de trabajo conjunto recientemente establecido asesora a CISA, EI-ISAC, EAC y otros en áreas donde faltan recursos de capacitación. Las capacitaciones sobre phishing y ransomware centradas en las elecciones, así como los cursos CISA para "construir confianza a través de seguridad prácticas son adiciones recientes creadas en base a los aportes del Grupo de Trabajo de Capacitación. Además, muchas oficinas electorales estatales se han asociado con el sector privado y la academia o han producido capacitación interna sobre seguridad cibernética para empleados y funcionarios electorales locales. La EI-SIG también ofrece formación en ciberseguridad a las empresas miembros y a sus empleados.

El GCC y el SCC continúan enfocándose en empoderar a sus miembros para administrar el riesgo de ciberseguridad y planificar posibles incidentes. Los miembros de los consejos de ambos subsectores proporcionaron información sobre el Herramienta de perfil del riesgo de seguridad electoral: organizado por EAC y creado por CISA, que ayuda a las partes interesadas de la administración electoral a evaluar su riesgo y priorizar sus recursos para mitigar el riesgo. El esfuerzo Last Mile de CISA es un esfuerzo de colaboración con los funcionarios electorales para producir productos personalizados (por ejemplo, carteles de instantáneas, guías de respuesta ante emergencias el día de las elecciones y otras plantillas) que abordan los riesgos cibernéticos y de infraestructura dinámicos o condicionales de los administradores electorales estatales y locales y los proveedores de la industria. Muchas oficinas electorales estatales han trabajado con sus socios del sector privado y otros para producir sus propios productos para mejorar la preparación a nivel estatal y ayudar a los funcionarios locales a prepararse para la respuesta a incidentes cibernéticos.