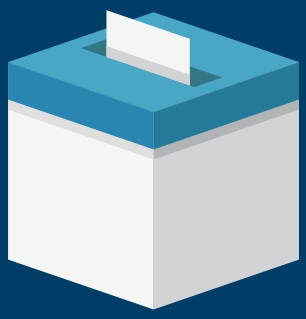
Moyens de sécurité

pour le sous-secteur de l'infrastructure électorale



L'Agence de la cybersécurité et de la sécurité des infrastructures (*ou Cybersecurity and Infrastructure Security Agency, CISA*) et le Federal Bureau of Investigation (*FBI*) ont préparé un récapitulatif de certaines des ressources disponibles au sein du gouvernement fédéral pour les fonctionnaires électoraux des États, locaux, territoriaux et tribaux (SLTT) et leurs partenaires du secteur privé, afin d'aider à répondre aux menaces qui pèsent sur le personnel, ainsi que des conseils sur l'évaluation et l'atténuation des risques pour leurs biens matériels.

Bien que bon nombre de ces ressources ne soient pas explicitement axées sur la sécurité électorale, il se peut que le sous-secteur de l'infrastructure électorale les trouve utiles dans le cadre de ses fonctions. Étant donné que la distinction entre la sécurité physique et la cybersécurité est de plus en plus floue, certaines ressources axées sur la cybersécurité ont également été incluses dans ce document. Toutes les ressources citées ici sont disponibles gratuitement pour l'utilisateur et peuvent être trouvées sur les sites Web énumérés ci-dessous.

Menaces contre les fonctionnaires électoraux et l'infrastructure

En réponse aux menaces accrues de violence contre les travailleurs électoraux à la suite du cycle électoral de 2020 aux États-Unis, le FBI et la CISA ont défini la priorité des efforts visant à lutter contre ces menaces. Le FBI et la CISA prennent toutes les menaces de violence au sérieux, y compris celles qui ciblent les travailleurs électoraux pour leur rôle crucial dans la sauvegarde du processus électoral pour tous les électeurs. Le Département de la Justice américain (*Department of Justice* ou *DOJ*) a créé le Groupe de travail sur la menace aux travailleurs électoraux afin d'enquêter activement sur ces menaces et de les poursuivre vigoureusement. Si vous êtes victime d'une menace en tant que travailleur électoral, veuillez prendre les mesures suivantes :

- S'il y a une menace imminente pour la vie, composez le 911 (Services d'urgence américains)
- Pour signaler les menaces, communiquez avec le Coordonnateur des crimes électoraux (*Election Crimes Coordinator*) au sein de votre bureau local du FBI (www.fbi.gov/contact-us/field-offices) ; soumettez un tuyau en ligne à tips.fbi.gov ; ou appelez le 1-800-CALL-FBI (225-5324), sélectionnez les instructions 1, puis les instructions 3. Communiquer avec le coordonnateur des crimes électoraux dans votre bureau local du FBI est la meilleure façon de signaler des menaces électorales
- Enfin, communiquez avec votre bureau régional de la CISA pour obtenir des conseils sur les risques liés à la sécurité physique qui soient adaptés à votre juridiction et à vos installations. Les conseillers en sécurité préventive (*Protective Security Advisors, PSA*) du CISA peuvent effectuer des évaluations, telles que l'« Outil d'évaluation de la sécurité et de la situation initiale » (*Security Assessment and First Entry*, *SAFE*), qui mettent en évidence les vulnérabilités de votre infrastructure électorale physique, dont les bureaux électoraux, les bureaux de traitement des bulletins de vote, les aires de stockage, les centres de vote et autres installations électorales. Trouvez votre conseiller local en sécurité préventive (PSA) ici : www.cisa.gov/cisa-regions

Protection de la sécurité physique : Documents d'orientation et autres ressources

- La *Préparation de la sécurité physique de la CISA dans les lieux de vote et les installations électorales* (*CISA Physical Security Preparedness at Voting Locations and Election Facilities*) fournit des étapes concrètes permettant aux responsables électoraux d'améliorer le dispositif de sécurité physique et d'accroître la résilience des opérations électorales dans leur juridiction : www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf
- Les *produits « Last Mile » de la CISA* sont des outils personnalisables que les responsables électoraux peuvent utiliser pour améliorer la sécurité de leur infrastructure. Parmi ces produits, mentionnons l'Aperçu de la planification de la sécurité électorale (*Election Security Planning Snapshot*), les Guides d'intervention d'urgence lors d'élections (*Election Emergency Response Guides*), les Mesures de protection des élections (*Election Safeguards*) et d'autres modèles. Pour plus d'informations et pour demander un produit Personnalisé « Last Mile », veuillez contacter : electionsecurity@hq.dhs.gov
- Le *Guide sur l'Aperçu du plan de sécurité et les ressources du CISA sur les cibles faciles et les lieux bondés* (*CISA Soft Targets and Crowded Places Security Plan Overview and Resource Guide*) fournit aux partenaires des secteurs public et privé des renseignements pertinents pour améliorer leur préparation et leur sécurité : www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf www.cisa.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf

- *Protéger l'infrastructure pendant les manifestations publiques du CISA* (*CISA Protecting Infrastructure During Public Demonstrations*) offre des recommandations de sécurité pour les entreprises pouvant être la cible d'actes illégaux lors de manifestations publiques : www.cisa.gov/sites/default/files/publications/protecting_infrastructure_during_public_demonstrations_508.pdf
- *L'Atténuation des répercussions du doxing sur les infrastructures essentielles de la CISA* (*CISA Mitigating the Impact of Doxing on Critical Infrastructure*) définit le doxing et en fournit des exemples, explique l'impact potentiel du doxing sur les infrastructures essentielles et offre des mesures de protection et de prévention, des options d'atténuation et des ressources supplémentaires pour les particuliers et les organisations : www.cisa.gov/sites/default/files/publications/cisa_insights_mitigating_the_impacts_of_doxing_508.pdf
- *Le Guide du contreterrorisme à l'intention du personnel de la sécurité publique du Bureau du directeur du renseignement national* (*Office of the Director of National Intelligence (ODNI) Counterterrorism Guide for Public Safety Personnel*) aide les premiers intervenants à reconnaître et à signaler les activités suspectes, à repérer les indicateurs de mobilisation à la violence et à réagir aux attaques terroristes et à les atténuer : www.dni.gov/nctc/jcat/index.html

Site Web clé/Coordonnées

- La page *Web de la CISA sur la sécurité électorale* (*CISA Election Security*) contient tous les outils et ressources en matière de sécurité électorale de la CISA, y compris toutes les ressources du gouvernement fédéral énumérées dans le présent document : www.cisa.gov/election-security
- Le site Web du programme de la CISA visant à *la Sécurité dans votre ville* (*CISA Hometown Security*) fournit des outils et des ressources pour appuyer la sécurité et la résilience de la collectivité : www.cisa.gov/hometown-security
- Le *Comité interinstitutions de la CISA* (*CISA Interagency Security Committee*) s'occupe de la sécurité continue à l'échelle du gouvernement pour les installations fédérales et a créé de nombreux documents sur les normes, les politiques et les pratiques exemplaires qui sont disponibles pour que les particuliers et les organisations les examinent à l'adresse suivante : www.cisa.gov/isc
- Le *Bureau de la CISA pour la Prévention des bombardements* (*CISA Office for Bombing Prevention, OBP*) fournit une variété de ressources, de formations, d'outils et de produits pour aider les autorités étatiques et locales, les partenaires privés et autres à comprendre et à atténuer la menace des engins explosifs improvisés (EEI) et à protéger les infrastructures essentielles : www.cisa.gov/obp
- *CISA Central* est la plateforme de la CISA pour que les partenaires et les intervenants en infrastructure essentielle puissent demander de l'aide et des services. CISA Central fonctionne 24h/24 et 7j/7 : Central@cisa.gov ou 888-282-0870
- Le Numéro vert du FBI (*FBI Tip Line*) est la plaque tournante du FBI pour signaler les menaces et les crimes électoraux et non électoraux : https://tips.fbi.gov ou 1-800-CALL-FBI (225-5324)
- La page Web du FBI sur *les Crimes électoraux et la sécurité* (*FBI Election Crimes and Security*) fournit des renseignements sur la compréhension et la déclaration des crimes électoraux : www.fbi.gov/elections
- *L'initiative « Paroles protégées » du FBI* (*FBI Protected Voices*) fournit des outils et des ressources aux campagnes politiques, aux entreprises et aux individus pour se protéger contre les opérations d'influence étrangère en ligne et les menaces de cybersécurité : www.fbi.gov/protectedvoices
- La *Boîte à outils des premiers intervenants du Centre national de lutte contre le terrorisme de l'ODNI* (*ODNI National Counterterrorism Center (NCTC) First Responder Toolbox*) fournit de l'information pour aider aux activités de préparation, de coordination, d'intervention, de sécurité et d'enquêtes entre les parties prenantes dans la lutte contre le terrorisme : www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox
- La *Commission d'assistance électorale des États-Unis* (US *Election Assistance Commission, CAE*) sert de centre national d'information sur l'administration électorale et dispose de ressources supplémentaires liées à la sécurité électorale, qui peuvent être trouvées ici : www.eac.gov/election-officials/election-security

Formations et exercices

- Les *Formations sur la sécurité électorale de la CISA (CISA Election Security Trainings) fournissent des* conseils supplémentaires aux intervenants électoraux pour gérer les risques et renforcer la résilience des infrastructures électorales. Pour planifier des

Alertes et annonces d'intérêt public

- Le *Centre d'échange et d'analyse de l'information sur l'infrastructure électorale (Elections Infrastructure Information Sharing and Analysis Center, EI-ISAC*) offre une série de ressources en matière de sécurité électorale, y compris des

formations ou pour en savoir plus à leur sujet, envoyez un courriel à : electionsecurity@hq.dhs.gov

- Le *Comité interinstitutions de la sécurité de la CISA* (*CISA's Interagency Security Committee, ISC*), qui met l'accent sur la sécurité de toutes les installations fédérales, offre des cours de formation en ligne et interactifs qui pourraient être utiles à la sécurisation de votre infrastructure physique : www.cisa.gov/interagency-security-committee-training
- *Le Bureau de la CISA pour la Prévention des bombardements* offre des formations d'études indépendantes en personne, virtuelles et sur le Web. Ces cours aident les parties prenantes publiques et privées à sensibiliser et à réagir aux menaces des engins explosifs improvisés (EEI) : tripwire.dhs.gov/training-education/counter-ied-training-0
  Les *Exercices de la CISA* (*CISA Exercises*), y compris des exercices sur table, offrent une formation axée sur des scénarios pour aider à cerner les domaines à *améliorer*, à partager les pratiques exemplaires et à améliorer la préparation aux menaces qui pèsent sur l'infrastructure et le personnel électoraux : www.cisa.gov/critical-infrastructure-exercises

produits de renseignement sur les menaces, une surveillance des menaces et de la vulnérabilité, une réponse à l'incidence et l'assainissement, ainsi que d'autres produits et services : www.cisecurity.org/ei-isac/

- Le *Centre pour les plaintes de crime sur Internet du FBI (FBI Internet Crime Complaint Center, IC3)* accepte les plaintes en ligne des victimes de crimes sur Internet et publie à la fois les alertes de l'industrie et des consommateurs sur les questions liées à la criminalité sur Internet : www.ic3.gov
- Le *Système national de cyber-sensibilisation du CISA* (*CISA National Cyber Awareness System, NCAS*) est un référentiel d'alertes du CISA concernant les problèmes de sécurité, les vulnérabilités et les exploits actuels : www.cisa.gov/uscert/ncas/alerts