



**MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES**

*Liberté
Égalité
Fraternité*

**Direction des Français à l'étranger
et de l'Administration consulaire (FAE)**

MEAE_23048_DFAE

ANNEXE 1 AU CCTP

Liste des audits effectués dans le cadre de la solution de vote par internet pour les élections des représentants
des Français établis hors de France

Type d'audit	Description sommaire
Audit de sécurité des systèmes d'information de l'environnement de vote par Internet des Français de l'étranger, et de conformité avec la délibération n° 2019-053 de la CNIL	<p>Cet audit comprend deux volets principaux : la partie « Sécurité » et la partie « Conformité à la délibération de la CNIL de 2019 ».</p> <ul style="list-style-type: none"> - <u>Sécurité</u> : Cet audit a pour objectif d'apprécier le niveau de sécurité des systèmes d'information, tant au niveau technique qu'organisationnel. Cet audit vise notamment à assurer les exigences de sécurité suivantes : <ul style="list-style-type: none"> - l'intégrité du vote ; - la confidentialité du vote ; - la disponibilité de la plateforme de vote ; - l'authentification de l'électeur qui ne doit pouvoir voter qu'une fois et uniquement blanc ou pour un seul candidat ; - l'anonymat de l'électeur. - <u>Conformité avec la délibération de la CNIL de 2019</u> : Cet audit vise également à établir les conformités avec la délibération de la CNIL n° 2019-053 du 25 avril 2019, portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. Cet audit de conformité s'appuie en particulier sur les 4 audits listés et détaillés ci-bas : <ul style="list-style-type: none"> - l'audit de sécurité sur l'architecture technique du système de vote ; - la revue des configurations ; - l'audit du code source de la solution de vote par internet ; - l'audit de sécurité portant sur les tests d'intrusion web.

Audit de sécurité sur l'architecture technique du système de vote électronique	<p>Audit de sécurité annexé à l'analyse de la conformité de la CNIL. Cet audit vise à analyser le niveau de sécurité de l'architecture technique du système de vote électronique.</p> <p>L'analyse de la sécurité de l'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés sur les plateformes de vote par rapport à l'état de l'art.</p>
Revue des configurations	<p>L'objectif de cet audit est d'évaluer le niveau de renforcement de différents éléments constitutifs de l'application de vote par internet.</p> <p>Dans ce cadre, le MEAE fait appel au titulaire pour la réalisation de revues de configurations, au regard des bonnes pratiques de sécurité, de l'état de l'art ainsi que des guides de renforcement de l'Agence Nationale de la Sécurité des Systèmes d'Information, conformément à l'objectif de sécurité n° 2-06 de la délibération n° 2019-053 du 25 avril 2019.</p>
Audit de code source cryptographique	<p>Les objectifs de cet audit sont :</p> <ul style="list-style-type: none"> - s'assurer de la bonne prise en compte des mécanismes de cryptographie dans le projet ; - identifier les vulnérabilités par des attaques réalistes et reproduisant des scénarios de menaces liés aux enjeux métiers du MEAE ; - évaluer le niveau de sécurité global ; - fournir des recommandations précises et un plan d'actions pragmatique adapté au contexte du MEAE. <p>Également, le MEAE demande au titulaire du marché de réaliser un audit des scripts utilisés pour réaliser les prises d'intégrité des éléments serveurs. Les objectifs de cet audit sont de contrôler que les outils de vérification d'intégrité implémentés déployés sur le serveur hébergeant l'application de vote par internet sont corrects.</p>

Audit de sécurité sur les tests d'intrusion web	<p>Les tests d'intrusion web menés par le titulaire ont pour objectifs de :</p> <ul style="list-style-type: none"> - Tester la robustesse des mécanismes d'identification et d'authentification ; - Vérifier le cloisonnement entre les profils ; - S'assurer de la confidentialité du vote et des données ; - Confirmer l'efficacité des mécanismes de surveillance et de traçabilité des actions ; - Valider la conformité de la solution avec les objectifs de sécurité de la CNIL pour les systèmes de vote électronique.
Audits différentiels	<p>Le ministère demande au titulaire du marché de réaliser des audits différentiels pour compléter les différents audits de sécurité réalisés, sur les nouvelles versions développées par le titulaire du marché VPI.</p> <p>Ces audits différentiels peuvent concerner une partie ou l'ensemble des audits listés dans ce document.</p>
Audit complémentaire sur les constats et recommandations, suite à l'organisation d'un scrutin	<p>A l'issue d'un scrutin mettant en œuvre le système de vote par internet, cet audit complémentaire vise à réaliser un bilan global des opérations, au regard de l'audit de sécurité et de conformité à la CNIL réalisé en amont.</p> <p>Cet audit porte également sur le mode opératoire appliqué, dont la gestion du matériel et des fichiers, le déroulé des opérations ainsi que la gestion des incidents et des opérations.</p>

Analyse de risque	Le but de l'analyse de risque est d'identifier les menaces portant sur le projet, de déterminer les mesures de sécurité adaptées à la menace, et de mettre en place le cadre de suivi et d'amélioration continue. Cette analyse de risque doit être réalisée avec la méthode EBIOS.
Analyse d'impact sur la protection des données	Ce document regroupe les éléments de l'analyse d'impact relative à la protection des données à caractère personnel concernant le traitement automatisé de données à caractère personnel prévu à l'article R.176-3 du code électoral pour l'élection de députés par les Français établis hors de France.
Audit d'accessibilité - RGAA	L'audit RGAA permet de contrôler l'accessibilité d'un site et de ses contenus suivant les normes internationales de l'accessibilité numérique connues sous l'appellation de WCAG .