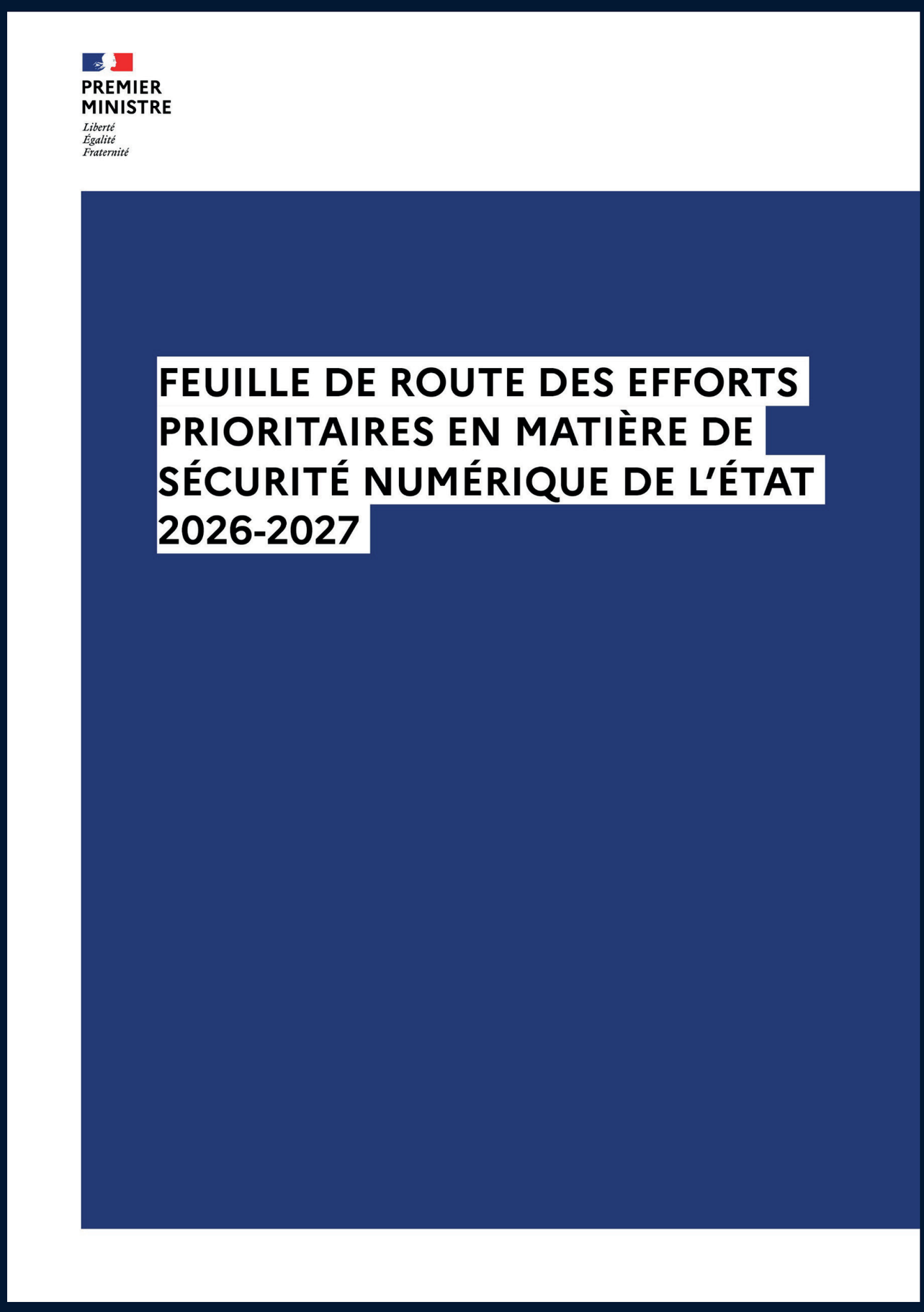
HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

FEUILLE DE ROUTE DES EFFORTS PRIORITAIRES EN MATIÈRE DE SÉCURITÉ NUMÉRIQUE DE L'ETAT 2026-2027



ÉCHÉANCES À RETENIR

D’ICI AU 30 JUIN 2026

[Action 1.c]
Avoir recueilli auprès des établissements publics les rapports annuels prévus par le décret 2019-1088.

[Action 1.d]
Produire une déclinaison ministérielle de la présente feuille de route cyber et s’assurer de sa bonne intégration dans la feuille de route numérique du ministère.

[Action 1.g]
Avoir formalisé une politique d’audit et de contrôle des systèmes d’information (la mise en oeuvre étant attendue pour décembre 2026).

[Action 2.a]
Avoir mis à jour l’inventaire des systèmes d’information en identifiant ceux à enjeux.

[Action 2.b]
Avoir formalisé une première politique d’hébergement dans le cloud.

[Action 3.b]
Avoir mis en place une politique de contrôle de la chaîne d’approvisionnement.

[Action 4.a]
Définir des procédures d’installation des correctifs de sécurité (leur mise en oeuvre étant prévue pour décembre 2026).

[Action 4.b]
Avoir défini et mis en oeuvre des procédures permettant de prendre connaissance et de traiter les alertes.

[Action 6.b]
Mettre en place des revues des droits d’accès au moins une fois par an pour les SI à enjeux, en commençant par les comptes d’administration technique.

[Action 6.d]
Définir un calendrier de généralisation de ProConnect comme mécanisme de fédération des identités.

[Action 6.e]
Avoir supprimé les comptes génériques ou, si cela s’avère impossible, renforcer leur traçabilité.

[Action 7.c]
Porter et maintenir la sécurité des annuaires importants pour la cybersécurité des ministères au niveau 3 de l’indicateur ADS.

[Action 9.b]
Réaliser un premier test des sauvegardes des systèmes d’information à enjeux (l'année 2026 est implicite au vu de la période couverte et de la mention du précédent jalon en mars 2025).

DE SEPTEMBRE A DECEMBRE 2026

SEPTEMBRE 2026

[Action 5.a]

Avoir renforcé d'ici au 30 septembre 2026 la sécurité de leur DNS, notamment par un recours accru au service interministériel DNS.

DÉCEMBRE 2026

[Action 1.g]

Mettre en oeuvre d'ici le 31 décembre 2026 la politique d'audit et de contrôle des systèmes d'information (qui doit être formalisée d'ici juin 2026).

[Action 2.c]

Avoir homologué d'ici au 31 décembre 2026 l'ensemble des systèmes d'information (SI) soutenant les missions essentielles.

[Action 3.a]

S'assurer que les documents contractuels intègrent bien les exigences de cybersécurité avant le 31 décembre 2026 pour les marchés numériques.

[Action 4.a]

Mettre en oeuvre avant le 31 décembre 2026 les procédures d'installation des correctifs de sécurité (qui doivent être définies d'ici juin 2026).

[Action 4.c]

Mettre en oeuvre un processus de remplacement des éléments obsolètes au fil de l'eau, en donnant la priorité aux briques de sécurité d'ici le 31 décembre 2026.

[Action 4.d]

Avoir remplacé les équipements de sécurité obsolètes d'ici le 31 décembre2026.

[Action 5.b]

Renforcer la sécurité de leurs systèmes de messagerie avant le 31 décembre 2026.

[Action 6.a]

Déploiement sur un premier périmètre comprenant des SI à enjeux d'ici le 31 décembre 2026 (concernant la gestion automatique du cycle de vie des identités et des accès).

[Action 6.b]

Mettre en place des revues des droits d'accès au moins une fois par an pour les comptes d'administration fonctionnelle avant le 31 décembre 2026.

[Action 6.d]

Déploiement de ProConnect sur un premier périmètre comprenant des SI à enjeux d'ici le 31 décembre 2026.

[Action 7.a]

Mettre en place d'ici le 31 décembre 2026 une authentification multi-facteur de l'ensemble des administrateurs de systèmes d'information.

[Action 7.b]

Administrer les systèmes d'information à partir de postes dédiés d'ici le 31 décembre 2026 pour l'administration des SI à enjeux et des SI nationaux.

[Action 8.a]

Améliorer la capacité de collecte, de centralisation et d'analyse des traces d'ici le 31 décembre 2026.

[Action 8.b]

Déployer d'ici le 31 décembre 2026 des dispositifs avancés de détection des attaques (EDR ou XDR) sur l'ensemble des postes de travail et sur l'ensemble des serveurs (priorité aux SI à enjeux).

[Action 8.c]

Consolider les CSIRT ministériels et leur mise en réseau avec le CERT-FR d'ici le 31 décembre 2026.

2027 / 2028 ET AU DELÀ

FÉVRIER 2027

[Action 6.c]
[28 février 2027]
Déployer une authentification multi-facteur des utilisateurs sur l'ensemble des SI à enjeux.

DÉCEMBRE 2027

[Action 3.a]
[31 décembre 2027]
S'assurer que les documents contractuels intègrent bien les exigences de cybersécurité pour les marchés ayant une composante numérique ou nécessitant l'échange d'information sensible.

[Action 6.a]
[31 décembre 2027]
Étendre le périmètre de la gestion automatique du cycle de vie des identités et des accès.

[Action 7.b]
[31 décembre 2027]
Administrer les systèmes d'information à partir de postes dédiés pour l'administration des SI des services déconcentrés (hors ceux non soumis à NIS 2).

FIN 2027

[Action 10.b]
[Avant fin 2027]
Identifier les briques techniques impliquées (chiffrement, signature…) dans le cadre de la transition vers la cryptographie post-quantique.

FÉVRIER 2028

[Action 6.c]
[28 février 2028]
Déployer une authentification multi-facteur des utilisateurs sur l'ensemble des SI de l'État

[Action 6.d]
[28 février 2028]
Achever le déploiement de ProConnect (comme mécanisme de fédération des identités) sur l'ensemble des SI.

MARS 2028

[Action 4.d]
[1er mars 2028]
Avoir remplacé les autres éléments obsolètes (hors sécurité) des SI à enjeux.

DÉCEMBRE 2028

[Action 2.c]
[31 décembre 2028]
Homologuer les "autres" systèmes d'information (SI) à enjeux (ceux ne soutenant pas directement les missions essentielles, qui doivent l'être dès 2026).

2030 ET AU-DELÀ

[Action 10.c]
[Avant fin 2030]
Déployer de la cryptographie post-quantique pour tous les systèmes d'information traitant d'information Diffusion Restreinte.

[Action 10.c]
[À partir de 2030]
Ne déployer que des produits de chiffrement qui intègrent de la cryptographie post-quantique.

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

LES RÉPONSES EXISTENT DÉJÀ DANS L'ÉCOSYSTÈME HEXATRUST :

GOUVERNANCE,
ZERO TRUST,
SUPERVISION, POST-QUANTIQUE :

LES ACTEURS FRANÇAIS & EUROPÉEN SONT PRÊTS.

L'union
fait la force