PREMIER
MINISTRE

Liberté
Égalité
Fraternité

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

La feuille de route de la sécurité numérique de l'État prévue par l'instruction générale interministérielle n° 1337 est établie annuellement, validée en comité stratégique de la sécurité numérique (COSINUS), puis par une concertation interministérielle.

Le document pour la période 2025-2026 avait été rédigé dans la perspective de la mise en conformité des administrations de l'État à la directive de l'Union européenne 2022/2555, dite directive NIS 2, qui prévoit dans son article 2 l'inclusion des administrations publiques dans le périmètre des entités régulées.

La plupart des objectifs de la feuille de route 2025-2026 correspondent aux objectifs généraux fixés par les articles 20 et 21 de la directive NIS 2 et les mesures préconisées rejoignent les exigences requises par le référentiel en préparation dans le cadre de la transposition de cette directive. Une priorité a été donnée aux systèmes d'information à enjeux des ministères[1].

Les multiples intrusions et fuites de données qui ont affecté en 2025 les systèmes d'information des ministères et des établissements dont ils ont la tutelle rappellent la persistance de vulnérabilités graves dans l'ensemble de ces infrastructures. La présente feuille de route, pour la période 2026-2027, vise à répondre à ces vulnérabilités. Elle prend néanmoins en compte les contraintes budgétaires qui ont pesé sur la mise en œuvre de la précédente. Elle en reprend les actions, affermit certaines échéances et la complète par une préparation à la transition vers la cryptographie post-quantique.

En effet, la sécurité numérique est fondée sur des mécanismes cryptographiques qui deviendraient inopérants avec les capacités de calcul d'un ordinateur quantique capable de les faire effondrer. Le chantier de transition vers des algorithmes résistants à cette menace est long et doit par conséquent être anticipé et engagé dès à présent. Ce document fixe deux premières étapes d'inventaire (2026 et 2027) et des objectifs de mise en œuvre à horizon 2030.

Dans un contexte de hausse générale de la menace et d'une situation géopolitique dégradée, il est important que les nouvelles échéances soient tenues et qu'un pilotage renforcé soit mis en place sur l'ensemble des actions, avec une priorisation sur certaines.

[1] Les systèmes d'information (SI) à enjeux sont définis comme les SI soutenant les missions essentielles du ministère ou traitant de données sensibles, sélectionnés en fonction d'une évaluation des besoins de sécurité et des impacts potentiels d'un incident de sécurité.

1. Renforcer la gouvernance

L'organisation de la sécurité des systèmes d'information de l'État et de ses établissements publics fait l'objet de l'instruction générale interministérielle (n° 1337/SGDSN/ANSSI). Pour que cette instruction soit pleinement appliquée, il importe que les sujets de cybersécurité soient suivis au plus haut niveau, mais également que chaque ministère pilote la cybersécurité des établissements publics dont il a la tutelle. Chaque ministère devra donc :

[Action 1.a] Désigner un conseiller numérique chargé des sujets de la sécurité du numérique au sein du cabinet du ministre dans le mois suivant la nomination du ministre ;

[Action 1.b] S'assurer que la cybersécurité soit prise en compte dans les conventions passées avec les établissements publics au fur et à mesure de leur renouvellement ;

[Action 1.c] Avoir recueilli d'ici au 30 juin 2026 auprès des établissements publics les rapports annuels prévus par le décret 2019-1088[2] ;

[Action 1.d] Produire une déclinaison ministérielle de la présente feuille de route cyber avant le 30 juin 2026 et s'assurer de sa bonne intégration dans la feuille de route numérique du ministère ;

[Action 1.e] Intégrer la problématique de la cybersécurité dans les lettres de mission des directeurs d'administration centrale pour s'assurer de l'alignement des priorités et de sanctions en cas de manquement ;

[Action 1.f] Mobiliser les corps d'inspection pour assurer un contrôle de la mise en œuvre des feuilles de route (ministérielle et interministérielle) ;

[Action 1.g] Avoir formalisé d'ici au 30 juin 2026 une politique d'audit et de contrôle des systèmes d'information et la mettre en œuvre d'ici le 31 décembre 2026.

Par ailleurs, la politique de sécurité des systèmes d'information de l'État sera mise à jour pour intégrer en anticipation le référentiel de règles ayant vocation à s'appliquer aux entités essentielles que créera NIS 2, au plus tard au premier trimestre 2027.

2. Homologuer les systèmes d'information

L'homologation des systèmes d'information de l'État est une obligation réglementaire au titre de l'article 4-3 du décret 2019-1088 : « *les infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'État mentionné à l'article 1er du présent décret font l'objet, préalablement à leur mise en œuvre, d'une homologation de sécurité* ». Certaines composantes peuvent néanmoins être dispensées d'homologation[3].

Les ministères devront donner la priorité aux systèmes d'information à enjeux et aux nouveaux systèmes d'information.

Tout système faisant l'objet d'une migration sur le cloud devra être considéré comme un nouveau système d'information et donc faire l'objet d'une homologation. Aussi, en cohérence avec la doctrine cloud au centre et les recommandations de l'ANSSI en la matière, les ministères devront élaborer une politique d'hébergement dans le cloud des systèmes

[2] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique.

[3] Arrêté du 31 juillet 2025 relatif aux dispenses d'homologation de sécurité des infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat.

d'information à enjeux garantissant la prise en compte de la cybersécurité dans les sélections d'offres cloud.

Il est donc demandé aux ministères :

[Action 2.a] D'avoir mis à jour d'ici au 30 juin 2026 l'inventaire des systèmes d'information en identifiant ceux à enjeux ;

[Action 2.b] D'avoir formalisé une première politique d'hébergement dans le cloud d'ici au 30 juin 2026 ;

[Action 2.c] D'avoir homologué d'ici au 31 décembre 2026 l'ensemble des systèmes d'information (SI) soutenant les missions essentielles et d'homologuer les autres SI à enjeux avant le 31 décembre 2028 ;

[Action 2.d] D'homologuer tous les nouveaux systèmes d'information faisant l'objet de l'obligation réglementaire ;

[Action 2.e] De s'assurer de la transparence des risques résiduels pendant les commissions d'homologation en présentant systématiquement les limites dues aux objectifs de la feuille de route non atteints, tels que le déploiement des correctifs de sécurité, les revues de comptes, les tests de restauration des sauvegardes ou des plans de reprise informatique.

3. Maîtriser l'écosystème dans lequel les systèmes d'information sont mis en œuvre

L'État a recours à un grand nombre de prestataires et de fournisseurs pour la mise en œuvre de ses systèmes d'information. Si les marchés passés font bien l'objet de clauses générales de sécurité, des clauses spécifiques doivent être prévues en cas de recours à un cloud ou en cas d'interconnexion avec un système d'information sur site.

Les ministères devront s'assurer que leurs prestataires et fournisseurs offrent un niveau de cybersécurité au moins équivalent à celui qui est exigé sur site.

A cet effet, ils devront :

[Action 3.a] S'assurer que les documents contractuels intègrent bien les exigences de cybersécurité, avec un niveau proportionné à la criticité des systèmes mis en œuvre :

- Avant le 31 décembre 2026 pour les marchés numériques ;
- Avant le 31 décembre 2027 pour les marchés ayant une composante numérique ou nécessitant l'échange d'information sensible ;

[Action 3.b] Avoir mis en place d'ici au 30 juin 2026 une politique de contrôle de la chaîne d'approvisionnement.

4. Assurer le maintien en condition de sécurité des systèmes d'information

Le maintien en condition de sécurité des systèmes d'information est un élément important de la cybersécurité. L'atteinte de cet objectif suppose comme prérequis que les ministères disposent au d'une cartographie de leurs systèmes d'information suffisamment détaillée.

Dans le cadre de la feuille de route, cet objectif est décliné en deux sous-objectifs.

D'une part, il s'agit d'assurer les mises à jour de sécurité des systèmes d'information.

A ce titre, il est demandé aux ministères :

[Action 4.a] De définir et mettre en œuvre des procédures d'installation des correctifs de sécurité, en proportionnant les exigences en fonction de la criticité des systèmes mis en œuvre :

- Définition : l'action est à réaliser d'ici au 30 juin 2026 ;
- Mise en œuvre : avant le 31 décembre 2026 ;

[Action 4.b] D'avoir défini et mis en œuvre d'ici au 30 juin 2026 des procédures permettant de prendre connaissance et de traiter les alerter.

D'autre part, il convient de réduire l'obsolescence des systèmes d'information de l'Etat. Les ministères devront :

[Action 4.c] Mettre en œuvre 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] Dresser un inventaire des éléments obsolètes des SI à enjeux et établir un calendrier de remplacement qui sera intégré dans la feuille de route ministérielle afin d'avoir :

- Remplacé les équipements de sécurité obsolètes d'ici le 31 décembre 2026 ;
- Remplacé les autres éléments obsolètes des SI à enjeux avant le 1er mars 2028 ;

[Action 4.e] En cas d'impossibilité de mise à jour des ressources, mettre en œuvre des mesures d'atténuation pour réduire les risques liés à l'utilisation d'une version comportant des vulnérabilités connues ou d'une version obsolète d'un applicatif, en application des recommandations de l'ANSSI, dans les mêmes délais.

5. Sécuriser les services exposés sur Internet

Les cyberattaques contre l'Etat exploitent de manière privilégiée les vulnérabilités du DNS (*Domain Name System*) et de la messagerie pour introduire des codes malveillants dans les systèmes d'information. Ces points de vulnérabilité doivent faire l'objet d'une attention particulière. Les ministères devront :

[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 ;

[Action 5.b] Renforcer la sécurité de leurs systèmes de messagerie avant le 31 décembre 2026.

6. Renforcer l'authentification et la gestion des accès

Dans une situation où les systèmes d'information de l'État sont de plus en plus répartis sur un grand nombre d'environnements, sur différents sites ou sur différentes formes de cloud, les processus d'identification, d'authentification et d'autorisation dans l'accès aux systèmes d'information prennent une importance croissante pour la cybersécurité. Ils sont à la base des démarches *Zéro Trust* préconisées dans les entités les plus matures. Afin de fiabiliser et d'améliorer l'efficience de la gestion des droits d'accès, il est nécessaire de mettre en place des mécanismes automatiques s'appuyant notamment sur les bases de données des ressources humaines. Il est important que l'ensemble des ministères s'engage dans cette perspective.

Les ministères devront donc :

[Action 6.a] Gérer de manière automatique le cycle de vie des identités et des accès et mettre en place des accès aux systèmes d'information en fonction de l'identité, de l'authentification et des rôles associés :

- Déploiement sur un premier périmètre comprenant des SI à enjeux d'ici le 31 décembre 2026 ;
- Extension du périmètre (qui sera précisée en 2026 lors de groupes de travail) d'ici le 31 décembre 2027 ;

[Action 6.b] Mettre en place des revues des droits d'accès au moins une fois par an pour les SI à enjeux :
- Comptes d'administration technique : d'ici le 30 juin 2026 ;
- Comptes d'administration fonctionnelle : avant le 31 décembre 2026 ;

[Action 6.c] Déployer une authentification multi-facteur des utilisateurs sur le système d'information et de communication de l'Etat[4] :
- Sur l'ensemble des SI à enjeux avant le 28 février 2027 ;
- Sur l'ensemble des SI avant le 28 février 2028 ;

[Action 6.d] Généraliser ProConnect comme mécanisme de fédération des identités des services numériques, en remplacement des comptes locaux et permettant une révocation homogène des accès :
- Définition d'un calendrier de généralisation d'ici le 30 juin 2026 ;
- Déploiement sur un premier périmètre comprenant des SI à enjeux d'ici le 31 décembre 2026 ;
- Déploiement sur l'ensemble des SI d'ici le 28 février 2028.

[Action 6.e] Avoir supprimé d'ici au 30 juin 2026 les comptes génériques ou, si cela s'avère impossible pour des impératifs techniques, renforcer leur traçabilité.

7. Renforcer la sécurité de l'administration des systèmes d'information

Les entités et personnes chargées de l'administration des systèmes d'information des ministères disposent de droits élevés qui requièrent une attention particulière. Il importe donc que les systèmes d'administration soient sécurisés dans les règles de l'art, en conformité avec les recommandations de l'ANSSI en la matière.

Les ministères devront en conséquence :

[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 (les SI propres aux services déconcentrés ne sont pas dans le périmètre, les SI qui ne seront pas soumis aux règles de NIS 2 sont également exclus) ;
- D'ici le 31 décembre 2027 pour l'administration des SI des services déconcentrés (à l'exception des SI n'étant pas soumis à NIS 2) ;

[Action 7.c] Porter d'ici au 30 juin 2026 et maintenir la sécurité des annuaires importants pour la cybersécurité des ministères au niveau assurant la protection contre les vulnérabilités connues, soit au niveau 3 de l'indicateur ADS.

[4] Au sens du décret n° 2019-1088 du 25 octobre 2019.

8. Améliorer la supervision et la réponse à incidents

La nécessité d'améliorer la supervision et la réponse à incidents a conduit les ministères à se doter d'outils de collecte, de centralisation et d'analyse des traces, ainsi que d'outils de surveillance en continu des infrastructures. Par ailleurs, le projet TEMPO mené dans le cadre du plan France Relance a permis de compléter la couverture des ministères par un réseau de CSIRT ministériels (centres d'alerte et de réactions aux cyberattaques). Toutefois, ces CSIRT sont à des niveaux de maturité variables et certains ne sont pas encore tout à fait opérationnels. Il est proposé d'approfondir la démarche, notamment en termes d'articulation avec le CERT-FR (centre de réponse à incident national et gouvernemental porté par l'ANSSI) et l'activité de détection de l'ANSSI.

Dans ce but, les ministères s'attacheront à :

[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, en donnant la priorité aux systèmes d'information à enjeux ;

[Action 8.c] Consolider les CSIRT ministériels et leur mise en réseau avec le CERT-FR d'ici le 31 décembre 2026 ;

[Action 8.d] Permettre aux CSIRT ministériels de partager au sein du réseau des CSIRT de l'État, et en premier lieu au CERT-FR, toute information utile à la gestion d'un incident sans validation préalable d'autres entités de leur ministère ;

[Action 8.e] Renforcer l'articulation entre les chaînes SSI et les DNUM au sein des ministères, en matière de gestion d'incidents.

En cas d'incident important, le ministère aura pour obligation de suivre les recommandations de l'ANSSI, puis 6 mois après l'incident d'adresser un point de suivi à l'ANSSI, au corps d'inspection et au Premier ministre.

9. Intégrer la cybersécurité dans les plans de reprise d'activité

Il est important pour l'État de renforcer sa résilience afin d'être en mesure de faire face aux incidents significatifs. Si ses capacités de gestion de crise ont été améliorées dans le cadre de la préparation des Jeux olympiques et paralympiques de Paris 2024, il reste une marge d'amélioration importante des plans de reprise d'activité en matière de cybersécurité.

Dans ce but, il est demandé aux ministères de :

[Action 9.a] Tester au moins une fois par an les plans de reprise ;

[Action 9.b] Tester régulièrement les sauvegardes des systèmes d'information à enjeux - un premier test était précédemment prévu à partir du 31 mars 2025, un test devra être réalisé d'ici au 30 juin.

10. Préparer la transition vers la cryptographie post-quantique

Les nouvelles capacités de calcul que permettrait l'apparition d'un ordinateur quantique capable de faire effondrer les mécanismes cryptographiques actuels bouleverseraient immédiatement le champ de la sécurité numérique en rendant ces mécanismes caducs. Parallèlement, certaines attaques consistent à capter dès à présent de l'information durablement sensible et de la conserver afin de la déchiffrer lorsque les capacités seront disponibles Des algorithmes dits « post-quantiques » permettent de se protéger contre ces attaques, actuelles ou futures, mais la transition à l'échelle d'un ministère s'inscrit dans le temps. L'enjeu et la durée du chantier rendent nécessaire d'engager dès à présent cette transition.

Dans ce but, il est demandé aux ministères de :

[Action 10.a] Faire l'inventaire, d'ici la fin 2026, de leurs données durablement sensibles pour lesquelles une mise en place de la cryptographie post-quantique sera prioritaire ;

[Action 10.b] Identifier avant la fin 2027 les briques techniques impliquées (chiffrement, signature…) ;

[Action 10.c] Déployer de la cryptographie post-quantique pour tous les systèmes d'information traitant d'information *diffusion restreinte* avant fin 2030 ;

[Action 10.d] A partir de 2030, ne déployer que des produits de chiffrement qui intègrent de la cryptographie post-quantique.