GOUVERNEMENT
Liberté
Égalité
Fraternité

bpifrance

FRANCE 2030

Stratégie Nationale pour la Cybersécurité

« Développement de technologies cyber innovantes critiques »

L'appel à projets est ouvert jusqu'au 23 avril 2025 à 12h00 (midi, heure de Paris).

Les dossiers peuvent être déposés selon le calendrier de relève suivant :

- 30 janvier 2025 à 12h00 (midi heure de Paris),
- 23 avril 2025 à 12h00 (midi heure de Paris).

En cas d'épuisement des moyens financiers affectés à cet appel à projets, celui-ci peut être arrêté de manière anticipée par arrêté du Premier Ministre pris sur avis du Secrétariat général pour l'investissement (SGPI).

Les porteurs de projets sont invités à déposer leur dossier de candidature en ligne sur la plateforme de Bpifrance : https://www.picxel.bpifrance.fr/accueil

APPEL À PROJETS
Octobre 2024

Sommaire

2– Sommaire

3– Contexte et objectifs de l'AAP
- _ Le plan d'investissement France 2030
- _ La stratégie nationale pour la cybersécurité
- _ Contexte de l'appel à projets
- _ Objectifs de l'appel à projets

6– Projets attendus
- _ Nature des projets candidats
- _ Nature des porteurs de projets

7– Critères et processus de sélection
- _ Critères d'éligibilité
- _ Critères de sélection
- _ Labellisation
- _ Processus de sélection

9– Données
- _ Protection et respect de la réglementation
- _ Production, stockage et valorisation de données d'intérêt cyber
- _ Accès aux données d'expérimentation

10– Conditions et nature du financement
- _ Aides proposées pour les activités économiques
- _ Aides proposées pour les activités non-économiques
- _ Coûts et dépenses éligibles
- _ Conditions de retour à l'Etat

14– Mise en œuvre, allocation des fonds et suivi des projets
- _ Contractualisation
- _ Suivi des projets et allocation de fonds
- _ Confidentialité et communication
- _ Conditions de *reporting*

Contexte et objectifs de l'appel à projets

Le plan d'investissement France 2030

- **Traduit une double ambition** : transformer durablement des secteurs clefs de notre économie (énergie, automobile, aéronautique ou encore espace) par l'innovation technologique, et positionner la France non pas seulement en acteur, mais bien en leader du monde de demain. De la recherche fondamentale, à l'émergence d'une idée jusqu'à la production d'un produit ou service nouveau, France 2030 soutient tout le cycle de vie de l'innovation jusqu'à son industrialisation.

- **Est inédit par son ampleur** : 54 Md€ seront investis pour que nos entreprises, nos universités, nos organismes de recherche, réussissent pleinement leurs transitions dans ces filières stratégiques. L'enjeu est de leur permettre de répondre de manière compétitive aux défis écologiques et d'attractivité du monde qui vient, et faire émerger les futurs champions de nos filières d'excellence. France 2030 est défini par deux objectifs transversaux consistant à consacrer 50 % de ses dépenses à la décarbonation de l'économie et 50% à des acteurs émergents porteurs d'innovation, et à intervenir sans engager de dépenses défavorables à l'environnement (au sens du principe Do No Significant Harm).

- **Sera mis en œuvre collectivement** : pensé et déployé en concertation avec les acteurs économiques, académiques, locaux et européens pour en déterminer les orientations stratégiques et les actions phares. Les porteurs de projets sont invités à déposer leur dossier via des procédures ouvertes, exigeantes et sélectives pour bénéficier de l'accompagnement de l'Etat.

- **Est piloté par le Secrétariat général pour l'investissement** pour le compte du Premier ministre et mis en œuvre par l'Agence de la transition écologique (ADEME), l'Agence nationale de la recherche (ANR), la Banque publique d'investissement (Bpifrance) et la Caisse des dépôts et consignations (CDC).

La stratégie nationale pour la cybersécurité

Le numérique est aujourd'hui présent dans tous les pans de la vie des Français. Support de nombreuses innovations, bénéficiant à chacun, il induit également de nouveaux risques en matière de sécurité et de souveraineté. Ainsi le développement du télétravail durant la crise sanitaire a contribué à rendre plus ténue la frontière entre les outils informatiques professionnels et personnels, augmentant d'autant la vulnérabilité des systèmes. Les tensions internationales causées, entre autres, par l'invasion de l'Ukraine par la Russie ont également entraîné une hausse du niveau des menaces dans le cyberespace.

Dans ce cadre, le Gouvernement a souhaité, *via* la stratégie nationale pour la Cybersécurité, accompagner le développement de la filière française de la cybersécurité. La stratégie vise ainsi à faire émerger des champions français de la cybersécurité, tant pour accompagner le développement d'une filière au potentiel économique important que pour garantir à notre pays la maîtrise des technologies essentielles à la garantie de sa souveraineté.

À l'horizon 2025, l'objectif assigné à cette stratégie est l'atteinte d'un chiffre d'affaires de 25 milliards d'euros pour la filière, un total de 75 000 emplois et l'émergence de scale-ups françaises en cybersécurité. Pour cela, la stratégie s'articule autour de 5 axes :

1. Développer des solutions souveraines et innovantes de cybersécurité ;
2. Renforcer les liens et synergies entre les acteurs de la filière ;
3. Soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales ;
4. Former plus de jeunes et professionnels aux métiers de la cybersécurité, actuellement fortement déséquilibrée ;
5. Soutenir le développement des entreprises *via* des investissements en fonds propres.

Cet appel à projets s'inscrit dans l'axe 1 de la stratégie et vise à soutenir le développement de briques technologies innovantes et critiques en cybersécurité. Il participera aussi à l'atteinte des objectifs de l'axe 2 de la stratégie, puisqu'il permettra le financement de projets collaboratifs entre les acteurs de la filière.

Pour en savoir plus : https://www.gouvernement.fr/cybersecurite.

Contexte de l'appel à projets

L'offre française en cybersécurité comporte des lacunes en ce qui concerne la maîtrise de certaines technologies clés, comme en font état plusieurs initiatives (action « technologies clés » de la revue stratégique de cyberdéfense, feuille de route du projet « cybersécurité et sécurité de l'IoT » du Comité Stratégique de Filière « Industries de sécurité », étude interne « Perspectives cyber 2030 » du GT Veille et Anticipation, feuille de route interne de l'ANSSI[1] par exemple).

Les technologies ainsi identifiées sont critiques du fait de leur sensibilité en termes de sécurité et appellent autant que possible des solutions souveraines. En outre, elles représentent un marché potentiel de taille pour les acteurs français.

Objectif de l'appel à projets

Le développement de solutions innovantes de confiance et souveraines est une priorité de la stratégie nationale. Cet appel à projets (AAP) y répond en cofinançant des projets de recherche et développement portant sur des briques technologiques innovantes et critiques en cybersécurité.

L'appel porte sur l'une des clés contribuant à la souveraineté numérique : **la protection des données stockées, transmises, ou calculées**. Que ce soit pour renforcer les défenses de systèmes face à des capacités étatiques, d'assurer la sécurité des échanges au sein d'une chaine d'approvisionnement, ou de minimiser des dépendances aux couches matérielles et logicielles sous-jacentes ; que ce soit pour une application à des systèmes embarqués, des installations industrielles, des centres de traitement de données ou de l'informatique grand public, la protection des données permet d'établir une périmètre de confiance clair, et robuste à des catégories d'attaques bien identifiées.

Les composants, services et infrastructures de protection des données au sens large doivent aujourd'hui faire face à de nombreuses évolutions :

- une tendance croissante d'externaliser les données sur le cloud avec un besoin de protection adapté ;
- des besoins de partage de l'information entre tiers en maintenant la confidentialité des données pour chaque partie prenante ;
- l'usage de l'intelligence artificielle qui se démultiplie avec des enjeux de protection des données d'apprentissage et des modèles ;
- l'émergence de la menace quantique qui nécessite d'anticiper la transition. A noter que le développement d'une offre de cryptographie post-quantique a déjà été adressé par un appel à projet dédié, ce volet n'est donc pas couvert par le présent appel ;
- une diversification des modèles d'attaquants qui amènent un intérêt à renforcer les modèles classiques de protection périphérique avec des approches de protection au niveau des données ;
- des attaques qui s'étendent aux chaînes de production logicielle de la chaîne d'approvisionnement qu'il faut donc mieux protéger ;
- une pénurie de méthodes et d'outils pour aider au déploiement de mécanismes de protection de données, y compris l'inventaire des biens et les aides à la décision.

Par ailleurs, la protection des données est un élément fondamental de l'élargissement du spectre législatif, porté par exemple par le « Cyber Resilience Act »[2]. Ce dernier constituera, d'ici quelques mois, un différenciant majeur de la politique industrielle européenne. Il y a donc un enjeu à pré-positionner des acteurs très innovants dans ce domaine, et de porter le développement de standards internationaux.

Cet appel à projets doit contribuer à répondre à l'ampleur des évolutions en cours et de permettre l'émergence de solutions innovantes pour la protection des données. Pour ce faire, une liste de thématiques de travail a été constituée (voir annexe 1). A terme, l'ambition est de renforcer l'autonomie de la France et de l'Union Européenne face à la diversité des environnements de stockage, de calcul, et de communication.

[1] Liée notamment à la qualification de produits et services.

[2] Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

Prioritairement, la thématique ciblée est la protection des données. Cependant, la thématique d'évaluation de la cybersécurité de l'AAP « Développement de technologies cyber innovantes critiques – 3 » publié en juin 2023 reste éligible.

Projets attendus

Nature des projets candidats

Les projets attendus présentent une assiette de dépenses totales d'un montant supérieur à **1 million d'euros à la fois pour les projets individuels et pour les projets collaboratifs**. Par exception, ce seuil est abaissé à 500 000 euros pour les projets individuels portés par les jeunes pousses au sens de la définition adoptée pour le régime exempté relatif aux aides en faveur des petites et moyennes entreprises (SA.111728). Plus généralement, la participation d'acteurs émergents[3] et en particulier de Très Petites Entreprises (TPE) et Petites et Moyennes Entreprises (PME) dans les projets est encouragée.

La réalisation de ces projets doit porter sur des travaux fortement innovants de recherche et développement en cybersécurité réalisés en France et s'inscrire dans une ou plusieurs des thématiques techniques identifiées dans l'annexe 1. Les projets attendus auront un niveau initial de TRL (Technology Readiness Level) égal au moins à 4 et viseront un niveau de TRL en fin de projet au moins égal à 7.

Les projets causant un préjudice important du point de vue de l'environnement seront exclus (application du principe DNSH – *Do No Significant Harm*[4] ou « absence de préjudice important »). Les projets devront le cas échéant, justifier la neutralité pour l'environnement des applications de la solution proposée ou s'inscrire dans une démarche d'amélioration vis-à-vis d'une solution de référence pertinente (produits/procédés/services comparable).

Les projets contribuants ou créant des composants « Open Source » démontreront une attention particulière à favoriser leur pérennité et leur valorisation.

Les projets auront une durée indicative comprise entre **12 et 36 mois.** Les dépenses liées au projet déposé dans le cadre du présent AAP sont éligibles à une aide seulement à compter de la date à laquelle le dossier est considéré comme complet par Bpifrance après la relève.

Nature des porteurs de projets

Le projet est porté par une entreprise unique, quelle que soit sa taille, immatriculée en France au registre du commerce et des sociétés (RCS) à la date de dépôt du dossier.

Le projet peut également être porté par un consortium identifiant une entreprise « cheffe de file » pouvant impliquer des partenaires industriels et/ou des partenaires de recherche, et le cas échéant, un ou plusieurs utilisateurs finaux de la solution.

[3] Entreprises de moins de 12 ans d'ancienneté, ou réalisant un pivot stratégique radical (le CA attendu du projet représente plus de 50% du CA total), ou en hypercroissance (le CA progresse de 20% au moins durant les 3 dernières années), ou en partenariat avec une startup, ou en build-up (achat d'une startup-up réalisé il y a moins de 3 ans).

[4] Règlement (UE) 2020/852 sur l'établissement d'un cadre visant à favoriser les investissements durables, en mettant en place un système de classification (ou « taxonomie ») pour les activités économiques durables sur le plan environnemental, publié au journal officiel de l'UE le 22 juin 2020.

Critères et processus de sélection

Critères d'éligibilité

Pour être éligible, un projet doit remplir l'ensemble des conditions suivantes :

- être complet au sens administratif lors du dépôt du dossier ;
- satisfaire les contraintes indiquées, notamment en termes de montant d'assiette de dépenses ;
- avoir pour objet le développement d'un ou plusieurs produits, procédés, solutions ou services, non-disponibles sur le marché et à fort contenu innovant ;
- être composé uniquement de partenaires éligibles à recevoir des aides publiques (en particulier, ne pas faire l'objet d'une procédure judiciaire, ne pas avoir le statut d'entreprise en difficulté) ;
- lister l'ensemble des aides accordées ou sollicitées sur les trois dernières années pour les projets de R&D menés par chaque partenaire et soutenus par la puissance publique (européenne, nationale, territoriale), en précisant les montants des programmes de R&D et les montants des aides accordées, afin d'apprécier la capacité financière des partenaires à mener à bien le projet ;
- présenter les éléments d'évaluation de la performance environnementale du projet avec la grille d'impact fournie dans le dossier de candidature.

Les projets ne respectant pas l'un des critères d'éligibilité sont écartés du processus de sélection.

Critères de sélection

Pour être sélectionnés, les projets éligibles sont instruits notamment sur la base des critères suivants :

- adéquation avec les thématiques détaillées dans le cahier des charges ;
- caractère innovant et valeur ajoutée du projet ;
- niveau de maturité préexistant et faisabilité technique du projet ;
- insertion du projet dans l'écosystème de la cybersécurité ;
- retombées économiques pour le territoire national, chiffrées et étayées en termes d'emplois (notamment : accroissement, maintien de compétences), d'investissements (notamment : renforcement de sites industriels, accroissement de la R&D), de valorisation d'acquis technologiques (brevet, propriété intellectuelle, notamment), de développement d'une filière ou d'anticipation de mutations économiques ou sociétales ;
- taille des marchés visés, impact économique et social du projet ;
- cohérence entre la situation financière de l'entreprise et l'importance des travaux proposés dans le cadre du ou des projets présentés ;
- capacité du consortium à mener à bien le projet et à assurer le cas échéant le déploiement ou l'industrialisation de la solution développée ;
- caractère stratégique à l'échelle nationale, régionale, ou européenne, existence d'une collaboration structurée ou d'un effet diffusant au sein d'une filière ou d'un écosystème, en particulier pour les entreprises impliquées ;
- adéquation avec les priorités de politique publique ;
- prise en compte des menaces cyber dans les phases de conception et de développement ;
- performance environnementale.

Labellisation

Le projet peut être labellisé, au choix du porteur, par un ou plusieurs pôles de compétitivité. Cette labellisation est facultative pour répondre au présent appel à projets.

La labellisation constitue un acte de reconnaissance par un pôle de compétitivité de l'intérêt du projet par rapport aux axes stratégiques du pôle, à l'écosystème et à ses cibles marché. La labellisation permet de confronter la pertinence du projet à la vision d'experts reconnus. Elle peut aussi permettre un accompagnement du porteur du projet dans sa démarche de définition et de structuration du projet et améliorer ses chances de succès.

La labellisation du projet par un pôle de compétitivité est une information prise en compte dans le processus de présélection des projets et portée à la connaissance des membres du jury. La labellisation et le rapport du comité de labellisation du pôle doivent être réalisées selon les critères du présent cahier des charges.

Critères de performance environnementale et impact socio-économique

Le présent appel à projets vise à sélectionner des projets démontrant une réelle prise en compte de la transition écologique. Les effets positifs attendus et démontrés du projet à cet égard, de même que les risques d'impacts négatifs, sont utilisés afin de sélectionner les meilleurs projets parmi ceux présentés et peuvent amener à moduler le niveau d'intervention publique accordé au projet. Chaque projet doit expliciter sa contribution à la transition écologique, en présentant les effets, quantifiés autant que faire se peut, directs ou indirects, positifs ou négatifs, estimés pour les objectifs décrits en Annexe 2.

L'évaluation portera également sur les impacts socio-économiques anticipés et le caractère souverain de la solution, en particulier les retombées économiques pour le territoire national, chiffrées et étayées en termes d'emplois (accroissement, maintien de compétences, etc.), d'investissements (renforcement de sites, accroissement de la R&D, etc.), de valorisation d'acquis technologiques (brevet, propriété intellectuelle, etc.), de développement d'une filière ou d'anticipation de mutations économiques ou sociétales.

Processus de sélection

Le canevas du dossier de candidature est disponible sur la page internet de l'appel à projets. Il doit être déposé de manière dématérialisée sur la plateforme de dépôt dédiée : https://www.picxel.bpifrance.fr/accueil.

Une première phase de présélection, sur la base du dossier de candidature complet, permet de décider du passage en audition ou non du projet selon les critères d'éligibilité et les critères de sélection (voir ci-dessus). Les auditions, organisées en distanciel, se tiennent sur la base d'une présentation du projet sous forme de diapositives et permettent de décider de l'entrée, ou non, du projet en instruction. Le jury d'audition est composé d'experts indépendants, d'experts Bpifrance, d'experts ANSSI et/ou Direction Générale de l'Armement, et pourra être complété d'experts ministériels.

Pour les projets en instruction il sera demandé au porteur, et aux partenaires, le cas échéant, d'apporter des éléments complémentaires au dossier de candidature dans un délai d'un mois maximum à compter de la date de notification. L'instruction des projets est conduite par Bpifrance qui pourra mobiliser des experts indépendants.

La décision finale d'octroi de l'aide est prise par le Premier Ministre, sur avis du Secrétariat général pour l'Investissement (SGPI) après avis du comité de pilotage ministériel à la suite de la présentation des conclusions del'instruction effectuée par Bpifrance. Les projets lauréats de cet appel à projets pourront faire l'objet d'une publication sur les sites internet du Gouvernement et de Bpifrance.

Données

Le partage de données entre les acteurs d'une filière est un élément essentiel à sa structuration, axe fort de la stratégie nationale pour la cybersécurité. **Dans le plein respect du droit de propriété des producteurs des données**, cet appel à projets introduit certaines exigences qui doivent faciliter leur partage. Ces exigences seront valables pour tous les projets recevant des financements étatiques dans le cadre de la stratégie nationale pour la cybersécurité.

Protection et respect de la réglementation

Il est essentiel que les données produites ou manipulées dans le cadre des projets financés par la stratégie

nationale, que ce soit lors de la phase de développement, d'expérimentation ou ultérieurement en production, soient protégées au bon niveau en fonction de leur sensibilité. Les objectifs sont à la fois de veiller à la protection de la propriété intellectuelle, d'éviter l'appauvrissement informationnel (typiquement contractuel) et de prévenir au mieux les fuites massives de données.

Dans cette optique, un travail d'analyse préalable est demandé aux porteurs de projets pour déterminer le niveau de sensibilité des différentes catégories de données du projet. Les mesures de sécurité qui en découleront (et qui devront être implémentées dans le cadre du projet) pourront faire intervenir la protection des communications de bout en bout (cryptographie) lors du transfert des données, un stockage sécurisé (chiffré et sauvegardé), un contrôle d'accès adéquat ainsi que des mesures juridiques ou contractuelles appropriées. Le cas échéant, le respect de la réglementation applicable (règlement général sur la protection des données, par exemple) sera le point de départ de cette analyse et de ces travaux.

Production, stockage et valorisation de données d'intérêt cyber

Dans le cadre des projets candidats, il est également demandé aux porteurs de capitaliser sur les opportunités de production de données d'intérêt cyber (de toutes natures). Cela implique de mettre en place les mécanismes *ad-hoc* de captation, de prétraitement (notamment de labélisation ou de normalisation) et de stockage de ces données, même s'il s'agit de données annexes non essentielles au projet.

Les réflexions sur un modèle économique autour de ces données sont fortement encouragées.

Dans le cas d'une abondance trop importante de données ou de contraintes spécifiques, une priorisation sur les données à stocker pourra être effectuée lors du suivi du projet. De même, la durée de stockage est à déterminer en fonction de la typologie des données concernées.

Le non-respect de cet aspect impactera négativement le dossier lors du processus de sélection et pourra *in fine* aboutir à une réduction du taux d'aide.

Accès aux données d'expérimentation

Les données générées dans le cadre du paragraphe précédent restent la propriété de leur producteur. Néanmoins, il est demandé aux porteurs bénéficiant d'une aide d'Etat dans le cadre de la stratégie nationale pour la cybersécurité de s'engager à mettre à disposition ces données gracieusement de manière ponctuelle dans le cadre d'expérimentations techniques non commerciales sous réserve de la compatibilité avec la réglementation et avec la non-concurrence des acteurs. Dans les deux cas d'exception, les données pourront éventuellement être mise à disposition si des traitements permettent de s'affranchir de ces contraintes (par exemple par de la cryptographie homomorphe, de l'anonymisation, de l'échantillonnage, etc.).

Conditions et nature du financement

L'intervention publique s'effectue dans le respect de la réglementation de l'Union européenne applicable en matière d'aides d'État (articles 107 à 109 du Traité sur le Fonctionnement de l'Union européenne).

Il est **notamment** fait application des régimes d'aide suivants, adoptés sur la base du règlement général d'exemption par catégorie n° 651/2014 de la Commission européenne publié au JOUE du 26 juin 2014 et ses modifications :

- régime cadre exempté n° SA.111723 relatif aux aides à la recherche, au développement et à l'innovation (RDI) pour la période 2024-2026 ;
- régime cadre exempté n° SA.111728, relatif aux aides en faveur des PME pour la période 2024-2026 ;
- régime cadre exempté n° SA.111729, relatif aux aides en faveur de l'accès des PME au financement pour la période 2024-2026 ;
- régime cadre exempté n° SA.111726, relatif aux aides à la protection de l'environnement pour la période 2024-2026.

Les régimes d'aides sont disponibles sur le site : (https://www.europe-en-france.gouv.fr). Ils détaillent les conditions d'application du présent dispositif pour assurer sa compatibilité avec le droit de l'Union européenne.

La liste des présents régimes cadre peut être complétée selon l'évolution des cadres de régimes d'aides européens.

Aides proposées pour les activités économiques

Sont considérées comme « économiques » les activités des entités, généralement des entreprises, consistant à offrir des biens ou services sur un marché potentiel, avec l'espérance de retours financiers basés sur les résultats du projet.

Le taux de l'aide s'applique sur les dépenses éligibles et dans la limite des intensités maximales permises par les régimes d'aides évoqués ci-dessus. S'agissant du régime cadre exempté relatif aux aides à la recherche, au développement et à l'innovation (RDI), les taux maximums applicables aux entités sont les suivants :

Type d'entreprise **Type de recherche**	**Petite entreprise(PE)**	**Entreprise moyenne (ME)**	**Grande entreprise(GE et ETI)**
Recherche industrielle	70%	60%	50%
- dans le cadre d'une collaboration effective (1)	80%	75%	65%
Développement expérimental	45%	35%	25%
- dans le cadre d'une collaboration effective (1)	60%	50%	40%

(1) une collaboration effective existe :

a. entre des entreprises parmi lesquelles figure au moins une PME et aucune entreprise unique ne supporte seule plus de 70% des dépenses éligibles ;

b. entre une entreprise et un ou plusieurs organismes de recherche et de diffusion de connaissances si ce ou ces derniers supportent au moins 10% des dépenses éligibles et ont le droit du publier les résultats de leurs propres recherches.

L'aide apportée aux activités économiques sera constituée d'une part de subvention et d'une part d'avance remboursable. Dans le cas général, la part de subvention sera de 60% au maximum.

Les dépenses qualifiées de « recherche industrielle » doivent faire l'objet d'une justification étayée de la part du demandeur. A défaut, ces dépenses pourront être requalifiées en « développement expérimental » et soutenues selon les modalités correspondantes.

Aucune aide de moins de 500 000 € ne sera attribuée à une entreprise relevant de la catégorie « Grande entreprise ». Toute dérogation à cette règle devra faire l'objet d'une demande préalable soumise à l'avis du Comité de pilotage ministériel.

Aides proposées pour les activités non économiques

Sont considérées comme « non économiques », les activités des entités, généralement des établissements de recherche, quel que soit leur statut, remplissant une mission d'intérêt général en consacrant une part prépondérante de leur activité à la R&D. Les activités relevant de prérogatives de puissance publique lorsque les entités publiques agissent en leur qualité d'autorité publique sont également considérées comme « non économiques ».

Pour les activités non économiques, l'aide sera apportée sous forme de subventions selon les modalités suivantes :

Type d'acteur	**Intensité de l'aide**
	100% des coûts marginaux

Organismes de recherche et assimilés (au choix de l'entité)	50% des coûts complets[5]
Collectivités locales et assimilées	50% des coûts complets

Toute dépense d'un organisme de recherche et assimilés liée à des travaux applicatifs pour le développement d'une solution portée par un des membres du consortium est à considérer en sous-traitance de ce dernier.

Travaux et dépenses éligibles

Les dépenses liées au projet sont à présenter hors taxe et selon la ventilation requise dans l'annexe financière du projet présente dans le dossier de candidature.

Les dépenses éligibles sont directement affectées au projet (hormis les frais connexes qui sont calculés par un forfait). Dans le cas général (Régime cadre exempté de notification n° SA.111723 relatif aux aides à la recherche, au développement et à l'innovation), la nature des dépenses éligibles est précisée ci-dessous :

Type de dépenses	Principes
Salaires et charges	Salaires chargés du personnel du projet (non environnés) appartenant aux catégoriessuivantes : chercheurs (post-doc inclus), ingénieurs, techniciens.
Frais connexes	Montant forfaitaire (20%, et 40% pour les laboratoires de recherche) des dépenses de personnel (salaires chargés non environnés)
Coûts de sous-traitance	Coûts de prestations utilisées exclusivement pour l'activité du projet (plafond à 30%). Les acteurs ou les projets développant la filière française seront privilégiés.
Contribution aux amortissements	Coûts d'amortissements comptables des instruments et du matériel de R&D auprorata de leur utilisation dans le projet. *Exemple : pour un équipement amorti de façon linéaire sur une durée de 10 ans, et utilisé durant 2 ans pour le projet, le montant éligible à une aide sera égal à 2/10e dumontant total de l'investissement dans cet équipement.*
Frais de mission	Frais réels des déplacements liés à la réalisation du projet.
Autres coûts	Autres frais d'exploitation directement liés à l'activité du projet. (Consommables nonamortis dans les comptes)

Conditions de retour pour l'Etat

Le montant de l'aide attribuée fait suite à une instruction approfondie sur la base des dépenses prévisionnelles présentées et des régimes d'aides associés.

L'aide apportée aux activités économiques sera constituée d'une part de subvention et d'une part récupérable. Les modalités de remboursement des avances récupérables accordées aux entreprises sont précisées dans les conventions prévues entre Bpifrance et les bénéficiaires des aides. Le remboursement des avances prend en règle générale la forme d'un échéancier forfaitaire sur plusieurs annuités, tenant compte des prévisions d'activité du bénéficiaire.

Le montant des échéances de remboursements intègre un taux d'actualisation, basé sur le taux de référence et d'actualisation fixé par la Commission européenne à la date de la décision d'octroi des aides, lequel est majoré de 100 points de base. Ce taux peut être ajusté à la hausse en cas d'évolution des modalités de remboursement.

Lorsque le comité interministériel en charge du suivi du dispositif constate, en fin de projet, une création effective et satisfaisante d'emplois sur le territoire dans le secteur cyber, il peut être décidé de renoncer à tout ou partie du remboursement.

Les modalités plus précises concernant le remboursement de la part remboursable seront précisées dans les conventions prévues entre Bpifrance et les bénéficiaires des aides.

[5] Les entités souhaitant se voir financer sur la base des coûts complets devront posséder une comptabilité analytique.

Mise en œuvre, allocation des fonds et suivi des projets

Contractualisation

Chaque bénéficiaire signe une convention avec Bpifrance. Cette convention précise notamment l'utilisation des crédits, le contenu du projet, le calendrier de réalisation, les modalités de pilotage du projet, le montant des tranches et les critères de déclenchement des tranches successives, les prévisions de cofinancement des projets, les conditions de retour financier pour l'Etat, les modalités de restitution des données nécessaires au suivi et à l'évaluation des investissements, et les modalités de communication.

La convention d'aide est signée dans le cas général dans un délai d'environ 4 mois à compter de la décision du Premier Ministre, sous peine de perte du bénéfice de la décision d'aide.

Suivi des projets et allocation de fonds

Le bénéficiaire met en place un tableau de bord comportant des indicateurs de suivi de l'avancement des projets et des résultats obtenus. Il le transmet régulièrement à Bpifrance selon les modalités prévues par la convention. Pour chaque projet soutenu, une réunion d'avancement est prévue, au moins annuellement. Organisée par Bpifrance, elle associe le SGPI et l'ensemble des ministères concernés. Cette réunion a pour objet de suivre la mise en œuvre du projet et notamment le niveau d'exécution budgétaire, l'avancement des opérations financées et le respect du planning.

Confidentialité et communication

Bpifrance s'assure que les documents transmis sont soumis à la plus stricte confidentialité et ne sont communiqués que dans le cadre de l'expertise et de la gouvernance de France 2030. L'ensemble des personnes ayant accès aux dossiers de candidature est tenu à la plus stricte confidentialité.

Une fois le projet sélectionné, chaque bénéficiaire soutenu par France 2030 est tenu de mentionner ce soutien dans ses actions de communication ou la publication des résultats du projet, avec la mention unique : « Ce projet a été soutenu par le plan France 2030 », accompagnée du logo de France 2030. L'État se réserve le droit de communiquer sur les objectifs généraux de l'action, ses enjeux et ses résultats, le cas échéant à base d'exemples anonymisés et dans le respect du secret des affaires. Toute autre communication est soumise à l'accord préalable du bénéficiaire.

Les projets lauréats de cet appel à projets font l'objet d'une publication sur les sites internet www.entreprises.gouv.fr et www.bpifrance.fr. Une notification individuelle est également adressée aux porteurs de projets.

Conditions de *reporting*

Le bénéficiaire est tenu de communiquer régulièrement à Bpifrance et à l'Etat les éléments d'informations nécessaires à l'évaluation de l'avancement du projet (impact social, économique, sociétal, environnemental et numérique) ainsi qu'à l'évaluation *ex post* du projet. Ces éléments, et leurs évolutions, sont précisés dans conditions générales de la convention d'aide entre Bpifrance et le bénéficiaire.

Contacts

Les renseignements concernant le processus administratif (constitution du dossier,démarches en ligne, précisions cahier des charges) pourront être obtenus auprès de Bpifrance par courriel en mentionnant en objet du message « Technos critiques 3 » à l'adresse suivante :

strategies-acceleration@bpifrance.fr

Pour toute question relative à la Stratégie Nationale cyber ou dépassant le cadre de cet appel à projets, le coordinateur de la Stratégie peut être contacté directement

:

strategie.cyber@pm.gouv.fr

Annexe 1 : Thématique des projets attendus

Développement de solutions innovantes de protection des données

Au travers de cet AAP, la stratégie d'accélération cybersécurité souhaite soutenir des projets visant à développer de nouvelles approches et de nouveaux moyens de protection des données, tout au long de leur cycle de vie. En particulier, les projets pourront adresser une ou plusieurs des thématiques suivantes :

- Axe 1 : protection des données utilisées dans des **infrastructures et services non maîtrisés** par les clients et/ou qui ne peuvent être considéré de confiance, et en particulier mécanismes indépendants à la main des utilisateurs et potentiellement en-dehors de l'exploitation des fournisseurs de services (exemple : FHE, Confidential Computing, etc.)
- Axe 2 : protection des **données partagées, ou exploitées par des tiers** :
    - maintien de la confidentialité des données pour chaque partie prenante dans le cadre de mutualisation et de partage de l'information (détection de fraude, prise de décision, apprentissage profond, etc.) (exemple : MPC) ;
        - Les cas d'usage envisagés peuvent notamment couvrir : remontées de capteurs de systèmes embarqués, logs d'activité de grandes infrastructures, transfert sécurisé de documents, dématérialisation des échanges (signatures et transfert de documents contractuels, factures, obligations déclaratives, etc.), données de santé (du laboratoire au cabinet du praticien médical en passant par les établissements de santé).
    - utilisation de techniques de Data Masking dans le but de protéger en confidentialité un sous-ensemble de données transmises à un tiers (exemples de cas d'usage : partage des données de santé à des fins de recherche) ;
    - recherche dans des données chiffrées, ou détection dans des flux de données chiffrées de marqueurs ou d'identifiants spécifiques sans avoir à déchiffrer les données. Par exemple, recherche d'une chaîne de caractères spécifique dans un flux chiffré de logs d'activités avec une technologie de type FHE ou *searchable encryption*.
- Axe 3 : facilitation et accélération des **cas d'usage autour de l'IA** :
    - protection des données d'apprentissage pour l'IA durant la phase d'entraînement, mais également au travers de l'usage du modèle final (inférence) ;
    - protection des données traitées par les modèles d'IA (exemple : les prompts des utilisateurs) ;
    - protection des modèles d'IA (intégrité et confidentialité).
- Axe 4 : outils d'aide à la **transition post-quantique**[6] :
    - outils permettant l'automatisation de l'inventaire des biens cryptographiques (souvent appelés « Discovery ») :
        - sondes réseaux (analyse / inspection des flux permettant d'identifier les vulnérabilités),
        - analyse des applications / des binaires pour détecter la cryptographie vulnérable,
        - outils de gestion du cycle de vie des certificats (CLM) appliqués à la menace quantique ;
    - outils d'aide à la décision, d'identification des biens vulnérables à la menace quantique et devant être mis à jour ou remplacés : à partir des inventaires des applications, des équipements, des systèmes réalisés par les outils d'inventaire automatisé, les actions de migration sont proposées par ordre de priorité ;
    - innovations dans les outils d'analyse de risque pour permettre la prise en compte des scénarios de menace quantique.
- Axe 5 : ***Data Centric Security*** (DCS) : techniques permettant de transporter le contrôle d'accès de la donnée, avec la donnée. Approches s'inscrivant dans le prolongement du *Zero Trust* et reposant sur la mise en place de labels définissant conditions d'accès (profils, localisation, droits, …) et de cryptographie.
- Axe 6 : protection de **l'intégrité des données de la chaîne de production logicielle** avec des moyens innovants permettant de :
    - protéger l'intégrité de la chaîne de production logicielle contre des attaques ;
    - améliorer les méthodes de détection à chaque étape de la transformation des sources en logiciel ;
    - mettre en place des actions de remédiation afin de limiter les impacts et permettre un retour rapide à l'état de fonctionnement nominal.
- Axe 7 : autres.

[6] Le développement d'une offre de cryptographie post-quantique a déjà été adressé par un appel à projet dédié « Cryptographie Post-quantique », ce volet n'est donc pas couvert par le présent appel.

- L’identité numérique européenne va générer de nouveaux usages dans lesquels le **partages d’attributs** seront nécessaires (majorité, nationalité, …). L’accès et la délivrance de ces attributs doivent protéger les données d’identité. L’approche *Zero Knowledge Proof* peut être un exemple de mise en œuvre de ce partage. De même, les services de confiance reposant sur l'utilisation de registres électroniques (*ledgers*) doivent pouvoir être évalués et supervisés.
- **Protection des sauvegardes et archives** (immutabilité, WORM *Write Once Read Many*) : amélioration des techniques de protection en intégrité et en disponibilité des outils de sauvegardes et des supports associés (cas d’usage : se protéger d’une attaque rançongiciel visant à détruire le système de sauvegarde).
- Toute innovation portant sur la sécurisation (protection, vérification, preuve, détection, analyse d’impacts …) de *smart contracts*, et des effets induits par leurs déclenchements automatiques.
- **Fuites de données** : la détection, mais aussi le traitement des fuites de données ou des reventes de données suites à une exfiltration malveillante. Par exemple : aide à la minimisation des données personnelles ou sensibles dans les traitements, marquage solide des données, systèmes de supervision de bases de données, outils permettant d'exploiter voire de partager de façon sécuriser les informations issues des fuites de données sans exposer les données confidentielles ou personnelles pour se protéger pour l'avenir (alerter les victimes, éviter la réutilisation de données d'identification révélées, etc.).

De manière transverse, les projets attendus sont encouragés à :

- favoriser l'émergence et la **consolidation de méthodes, de formats de données, d'outils et d'infrastructures** permettant de mutualiser les efforts et d'automatiser de plusieurs ordres de magnitude les tâches des architectes des systèmes d’information ;
- favoriser l’émergence d’un ensemble de pratiques innovantes pour le développement et l’intégration de chaînes de traitement de données **sûres-par-construction et sûres-par-configuration** ;
- Concevoir des principes novateurs de **gouvernance des déploiements de systèmes de protection de données** entre fournisseurs de technologies, fournisseurs de services, et utilisateurs finaux ;
- Développer des solutions qui prennent en compte les contraintes des **petites entités**.

Les projets souhaitant cibler l’aspect « évaluation de cybersécurité » sont renvoyés au cahier des charges de l’AAP « Développement des technologies cyber innovantes critiques » publié en juin 2023.

Annexe 2 : Critères de performance environnementale

Les projets causant un préjudice important du point de vue de l'environnement seront exclus (application du principe DNSH – Do No Significant Harm ou « absence de préjudice important ») au sens de l'article 17 du règlement européen sur la taxonomie[7].

En créant un langage commun et une définition claire de ce qui est « durable », la taxonomie est destinée à limiter les risques d'écoblanchiment (ou "greenwashing") et de distorsion de concurrence, et à faciliter la transformation de l'économie vers une durabilité environnementale accrue.

Ainsi, la taxonomie définit la durabilité au regard des six objectifs environnementaux suivants :

- l'atténuation du changement climatique ;
- l'adaptation au changement climatique ;
- l'utilisation durable et la protection des ressources aquatiques et marines ;
- la transition vers une économie circulaire ;
- la prévention et la réduction de la pollution ;
- la protection et la restauration de la biodiversité et des écosystèmes.

Les efforts des porteurs de projets en matière d'écoconception, de maitrise des émissions de CO2, des consommations énergétiques et de ressources ainsi que de lutte contre l'obsolescence pourront être plus particulièrement considérés dans l'évaluation.

Pour l'évaluation technique de l'impact du projet vis-à-vis de chaque objectif environnemental, le déposant doit renseigner le document dédié disponible sur le site de l'appel à projets (dossier de candidature) et le joindre au dossier de candidature.

Il s'agira d'autoévaluer les impacts prévisibles de la solution proposée (faisant l'objet de l'aide) par rapport à une solution de référence explicite, pertinente et argumentée. Cette analyse tient compte du cycle de vie des processus et du ou des produits ou livrables du projet, suivant les usages qui en sont faits. En tant que de besoin, ces estimations pourront être étayées par des analyses en cycle de vie plus complètes. La présentation au dossier d'éléments concrets sur la façon dont les porteurs de projet contribuent ou s'engagent à contribuer, dans le cadre du projet, voire dans l'ensemble de leurs activités, sera prise en compte positivement dans l'évaluation.

[7] Règlement (UE) 2020/852 sur l'établissement d'un cadre visant à favoriser les investissements durables, en mettant en place un système de classification (ou « taxonomie ») pour les activités économiques durables sur le plan environnemental, publié au journal officiel de l'UE le 22 juin 2020