Investissements d'Avenir – Développement de l'Économie Numérique

Cœur de filière numérique

Sécurité numérique

2013

IMPORTANT

ADRESSES DE PUBLICATION DE L'APPEL A PROJETS

http://cdcinvestissementsdavenir.achatpublic.com

www.dgcis.gouv.fr/secteurs-professionnels/economie-numerique/securite-numerique-aap

DEMANDES DE RENSEIGNEMENTS

Vous pouvez poser vos questions directement en sélectionnant cet appel à projets sur le site des consultations de la Caisse des Dépôts **jusqu'au 31 octobre 2013 à 12h00 :**
http://cdcinvestissementsdavenir.achatpublic.com

Ou par courrier à l'adresse suivante :

Caisse des Dépôts
Département Développement Numérique des Territoires
FSN – Appel à projets « *Cœur de filière numérique – Sécurité numérique* »
72, avenue Pierre Mendès-France
75914 Paris Cedex 13

CLÔTURE DE L'APPEL A PROJETS

Les projets doivent être déposés sous forme électronique, impérativement avant la clôture de l'appel à projets, la date et l'heure de réception faisant foi :

le 29 novembre 2013 à 12 heures 00 (heure de Paris)
sur le site des consultations de la Caisse des dépôts
http://cdcinvestissementsdavenir.achatpublic.com

Les modalités détaillées de soumission sont précisées au § 4.2.

SOMMAIRE

1 CADRE DE L'APPEL A PROJETS : CONTEXTE, ENJEUX ET OBJECTIFS 4

2 CHAMP DE L'APPEL A PROJETS 5

2.1 TYPE DE PROJETS 5
2.2 AXES TECHNOLOGIQUES 5
2.3 POINTS D'ATTENTION COMMUNS 9

3 DISPOSITIONS GENERALES POUR LE FINANCEMENT 9

3.1 AIDES AUX PROJETS DE R&D 9
3.2 DEPENSES ELIGIBLES POUR LES PROJETS DE R&D 10

4 MODALITES DE MISE EN ŒUVRE 11

4.1 PROCESSUS DE PRESELECTION ET D'ATTRIBUTION DE FINANCEMENTS 11
4.1.1 Phase 1 : Présélection des projets 11
4.1.2 Phase 2 : Décision de financement 11
4.2 MODALITE DE REMISE DU DOSSIER DE SOUMISSION 12
4.3 CONTENU DU DOSSIER DE SOUMISSION 12
4.4 REGLES D'ELIGIBILITE DES PROJETS 12
4.5 REGLES D'ELIGIBILITE DES PARTENAIRES 13
4.6 CRITERES D'EVALUATION POUR LA PRESELECTION 14

1 Cadre de l'appel à projets : Contexte, enjeux et objectifs

Dans le cadre de la réorientation du Programme d'Investissements d'Avenir décidée par le Gouvernement début 2013, une priorité a été donnée au développement et à la diffusion des technologies génériques, et plus particulièrement le développement de la R&D sur les technologies « cœur de filière du numérique », pour lequel un budget global de 150 M€ a été alloué.

Par cœur de filière du numérique, sont désignées les technologies numériques stratégiques, dont la maîtrise par les entreprises est susceptible d'être une source de différentiation majeure, d'en accroitre la compétitivité, de créer de nouvelles activités industrielles ou de services et d'en favoriser le développement.

En pratique, le cœur de filière du numérique recouvre les quatre thèmes suivants :

- l'informatique en nuage et le *big data* ;
- le calcul intensif et la simulation numérique ;
- le logiciel embarqué et les objets connectés ;
- la sécurité numérique.

Le présent document constitue le cahier des charges de l'appel à projets liés à la sécurité numérique.

A contrario des deux précédents appels à projets « sécurité et résilience des réseaux » organisés dans le cadre des investissements d'avenir, qui fixaient des priorités et visaient alors essentiellement à favoriser le développement de l'économie numérique par la mise en place d'un espace de confiance, seront privilégiés, cette fois-ci, des projets adressant spécifiquement les domaines de la cybersécurité, dans ses aspects protection et défense des systèmes d'information.

La place et le rôle des technologies de l'information dans les sociétés développées ne sont plus à présenter. Une part croissante de la compétitivité globale d'un pays tient à sa capacité à intégrer ces technologies dans le fonctionnement de l'État, des administrations et des entreprises comme d'en assurer l'accès le plus large aux citoyens.

S'est ainsi créé un cyberespace résultant de l'essor concomitant des technologies de l'information, favorisé par la convergence IP, de celui des infrastructures numériques et du fort taux d'équipement des entreprises, comme de celui des particuliers, entrainant de nouveaux usages. Ce cyberespace s'intègre chaque jour davantage à l'économie, à la vie quotidienne des Français et au fonctionnement du pays.

Le cyberespace est soumis à des menaces croissantes portées par des individus, des organisations criminelles ou des États, qui peuvent mettre en danger les fonctions portées par les systèmes d'information qui le constituent, voire des vies humaines en cas d'actions de sabotage, ou causer des accidents technologiques ou environnementaux. L'état de cybersécurité visé pour le cyberespace implique, à côté de la lutte contre la cybercriminalité, la mise en œuvre de principes et de méthodes, l'utilisation de technologies et de moyens destinés à protéger sa disponibilité, son intégrité et la confidentialité des données traitées. Elle est à même de concilier les enjeux économiques, sociétaux, stratégiques, d'indépendance et de souveraineté nationale, tels que définis à la fois par le Livre blanc de la défense et de la sécurité nationale et par la Feuille de route du numérique élaborée par le Gouvernement.

2 Champ de l'appel à projets

2.1 Type de projets

Les projets de R&D doivent correspondre à des activités de recherche industrielle et/ou de développement expérimental.

L'appel vise des projets de R&D menés par au moins deux partenaires dont une entreprise, à fort caractère innovant et concentrés sur le thème de la cybersécurité définie au paragraphe précédent.

Les conditions précises d'éligibilité des projets et des partenaires sont détaillées respectivement en § 4.4 et § 4.5. Les critères d'évaluation des projets soumis sont détaillés dans le paragraphe §4.6.

Les points d'attention mentionnés au §2.3, lorsque pertinents, seront également examinés en tant que critères d'évaluation des projets.

2.2 Axes technologiques

Compte-tenu des objectifs du présent appel à projets en matière de cybersécurité, à savoir essentiellement la protection des infrastructures (réseaux, OIV, etc.), il est attendu que les projets de R&D proposés dans le cadre du présent appel portent sur l'un ou plusieurs des cinq axes technologiques suivants[1] :

- **Axe technologique n°1 : Terminaux mobiles sécurisés et applications de confiance**

Face à la menace d'interception des communications, démultipliée par le développement des usages connectés et de la mobilité, le besoin de solutions commerciales sécurisées pour la protection des informations sensibles (c'est-à-dire de niveau équivalent à « confidentiel industrie » pour le secteur industriel ou « diffusion restreinte » pour l'Administration) est avéré.

Or les offres commerciales existantes ne permettent pas aujourd'hui de concilier des niveaux sécurité et d'ergonomie satisfaisants :

- soit les terminaux sont exclusivement dédiés à des applications professionnelles, extrêmement bridés et donc très loin de l'ergonomie attendue des *smartphones* modernes ;
- soit ils n'offrent qu'un cloisonnement applicatif léger des applications professionnelles / personnelles, au détriment du niveau de sécurité souhaité pour les applications professionnelles.

L'enjeu est de concevoir et développer à partir de terminaux existants ou adaptés une offre de type *smartphones* et tablettes professionnels (c'est-à-dire fournis par l'entreprise à ses employés), les moyens de gestion de parc associés, ainsi que l'infrastructure nécessaire de raccordement au système d'information de l'entreprise. Ces terminaux présenteront une ergonomie conforme aux standards du marché, en vue de faciliter leur acceptabilité par les utilisateurs, et permettront d'exécuter à la fois, dans des contextes fortement isolés l'un par rapport à l'autre :

[1] Bien que l'appel à projets privilégie les cinq axes technologiques décrits au présent paragraphe, les projets portant plus généralement sur le développement d'une technologie, d'un équipement, d'un service ou d'une solution dont l'application principale est la cyber-sécurité ou la sécurité de systèmes d'information, pourront être examinés.

- des applications professionnelles sécurisées (protection des données, des applications, des canaux d'échange avec l'entreprise) ;
- des applications personnelles « classiques ».

Un axe complémentaire sera l'étude et la réalisation des moyens techniques permettant d'évaluer et de maîtriser la sécurité d'applications tierce partie, afin de faciliter leur qualification en vue de leur mise à disposition de l'utilisateur.

- **Axe technologique n°2 : Solutions de protection des infrastructures et dispositifs voix/visiophonie sur IP**

Face à la migration vers le « tout IP », la satisfaction des besoins spécifiques de protection des flux voix et visio pose aujourd'hui deux types de problèmes insuffisamment couverts par les offres commerciales :

- celui d'intégrer « proprement » ces flux dans les systèmes d'information, dès lors que l'on estime que les solutions (terminaux) de voix et visio intégrés dans ces systèmes peuvent bénéficier des mesures de protection offertes par ces systèmes (chiffrement IP, notamment) ;
- celui d'offrir des services intégrés de sécurité, tels que le chiffrement de bout en bout de la voix ou de la visio, dès lors que de tels services sont estimés nécessaires et ne sont pas rendus par l'environnement.

En complément, la question de l'interopérabilité entre les différentes solutions se pose, qu'il s'agisse de l'interopérabilité technique entre équipements (terminaux fixes sécurisés entre eux, passerelles avec des équipements de chiffrement IP, terminaux fixes avec terminaux mobiles sécurisés…) ou de l'interopérabilité opérationnelle (gestions d'annuaires, de clés, révocations…).

L'enjeu est de concevoir et développer :

- des architectures et des solutions de filtrage adaptées permettant d'intégrer des flux voix et visio dans des systèmes d'information sécurisés sans remettre en cause les propriétés de sécurité de ces derniers ;
- une gamme de terminaux matériels (téléphones IP sécurisés) ou logiciels (*softphones* sécurisés sur PC) et d'équipements d'infrastructure associés, pour offrir une sécurisation des flux de bout en bout.

Le choix de protocoles permettant de garantir tant l'interopérabilité technique qu'opérationnelle des offres et ce, dans un objectif d'interopérabilité à l'échelle internationale, constituera un point d'attention particulier, de même qu'une ergonomie des solutions proche de celle des standards du marché, en vue de faciliter leur acceptabilité par les utilisateurs.

Les travaux pourront par ailleurs déboucher, au-delà de l'offre produits, sur une offre de services mettant en œuvre les produits développés.

- **Axe technologique n° 3 : Outils passifs de détection et de corrélation à haut débit, outils d'investigation après incidents**

Face aux menaces de plus en plus élaborées pesant sur les systèmes d'information sensibles, les mesures d'hygiène et de prévention adoptées sur ces systèmes ne suffisent généralement plus en raison, notamment, de l'ouverture desdits systèmes vis-à-vis du reste du monde via des interconnexions : des moyens de plus en plus efficaces, performants et robustes, de détection et de corrélation sont en conséquence nécessaires.

Il s'agit de développer des moyens de détection d'attaques par le réseau et de corrélation d'alertes, visant à rendre un service passif (sans action dynamique sur le réseau sur lesquels on les place), permettant :

- de récupérer en temps réel les métadonnées pertinentes issues du trafic réseau, d'analyser ces données pour y détecter d'éventuelles attaques et de remonter des alertes dans un format normalisé ;
- de corréler à grande échelle les alertes remontées par un ensemble de capteurs, afin par exemple de mettre en correspondance des événements concomitants et d'élever au besoin le niveau d'alerte ;
- de réaliser l'analyse de grands volumes d'alertes par des techniques de data-mining adaptées ;
- de recevoir et de protéger des signatures d'attaques qui peuvent provenir de plusieurs sources (ouvertes, internes de l'éditeur, externes) et peuvent elles-mêmes être sensibles.

On attend de ces solutions :

- des performances de traitement supportant de très hauts débits de l'ordre de 10 à 100 Gb/s ;
- et une richesse fonctionnelle couvrant à la fois la détection de compromission, d'attaques et tentatives d'intrusion, d'exfiltration, ainsi que les services de recherche de vulnérabilités (cartographie, reconnaissance).

En compléments, ces travaux pourront être accompagnés de développement des outils d'investigation nécessaires aux prestataires de traitement d'incidents.

- **Axe technologique n°4 : Solutions de protection des dispositifs SCADA**

La sécurité des systèmes de commande/contrôle industriels (ICS – Industrial Control Systems), en particulier mais pas seulement de type SCADA (Supervisory Control and Data Acquisition), est un enjeu majeur, qui va nécessiter un investissement important dans des solutions de sécurité adaptées à ces environnements.

Or, en matière de produits, l'offre commerciale, pourtant riche en dispositifs de protection efficaces adaptés aux systèmes d'information classiques, est aujourd'hui pratiquement inexistante en matière de dispositifs adaptés aux systèmes ICS.

Il s'agit de développer des gammes de moyens de protection, que ce soit en matière d'IDS/IPS (détection) ou de pare-feu (filtrage) :

- prenant en compte les protocoles spécifiques des systèmes industriels ;
- conformes aux normes industrielles, afin de permettre leur mise en œuvre dans les conditions des systèmes industriels (contraintes spécifiques de température, de résistance mécanique, de sureté de fonctionnement…).

Un axe important sera le choix des standards de sécurité permettant une reconnaissance internationale de la qualité et de performance des produits.

En complément, un travail est attendu sur les procédures spécifiques d'évaluation de ces gammes de produits, tant sous l'angle de leur sécurité, sur leur cycle d'intégration dans les systèmes concernés, que de leur couplage avec les moyens de supervision de la sécurité mis plus généralement en place par les prestataires de SOC (security operations center).

- **Axe technologique n°5 : Solutions de supervision de la sécurité (SIEM) maîtrisées.**

Face aux multiples formes que peuvent prendre les attaques sur les systèmes d'information, des outils d'analyse et de corrélation de journaux d'événements de type SIEM (*Security Information Event Management*) s'avèrent indispensables.

Cependant, les offres commerciales existantes ne permettent pas aujourd'hui de concilier les niveaux de confiance et de performance attendus pour un déploiement dans des systèmes d'information sensibles (entreprises, OIV, Administration).

L'enjeu consiste donc à enrichir l'offre de manière à disposer de solutions de type SIEM qui soient à la fois :

- de confiance, c'est-à-dire maîtrisées;
- multimodales, c'est-à-dire capable de gérer une grande variété de données issues de capteurs hétérogènes avec les connecteurs appropriés et de développer de nouveaux capteurs, par exemple des capteurs associés aux postes de travail ;
- disposant d'une forte capacité de corrélation (traitement à très haut débit d'événements, analyse *big data* de bases de données volumineuses, intégration de signatures pertinentes de scénarios d'attaque) ;
- évolutives, par la simplicité de l'ajout d'un nouveau type de donnée à mesurer ou à prendre en compte et par la *scalabilité* du déploiement ;
- conçues et développées pour offrir une résistance aux attaques en confidentialité, intégrité et disponibilité sur la fonctionnalité de SIEM ;
- ergonomiques en offrant des interfaces pertinentes et une représentation de la situation adaptées à différents niveaux d'opérateurs tels que : veilleur « fiche réflexe », analyste, expert *forensic*, responsable SSI, etc ;
- dotées d'une capacité débrayable à proposer des actions automatisées en réponse à des scénarios d'attaque reconnus.

En complément, un travail est attendu sur les procédures spécifiques d'évaluation de performances de ces outils de type SIEM.

2.3 Points d'attention communs

Les projets, si l'objet des travaux de R&D s'y prête, devront montrer leur prise en compte des trois points d'attention suivants :

- **Un fort niveau de confiance** : Conformément au niveau de confiance déjà mentionné, ces solutions doivent être conçues et développées de manière à permettre la protection d'informations et de systèmes sensibles notamment des opérateurs, de l'industrie et de son patrimoine, et de l'administration. En particulier, elles doivent émaner de développeurs soucieux de soumettre leur réalisation, en toute transparence, à un processus d'évaluation sous le contrôle de l'autorité SSI nationale.

- **Une grande facilité d'emploi** : Il est essentiel de bien veiller à la simplicité du déploiement et de l'exploitation des solutions proposées, ainsi qu'à une ergonomie adaptée aux besoins et aux usages des utilisateurs, facteurs essentiels d'une bonne acceptation.

- **Un soin marqué pour la standardisation** *:* Les solutions proposées devront tenir compte, dans toute la mesure du possible, des normes et standards en usage ; à défaut, une démarche pour leur standardisation devra être prévue.

3 Dispositions générales pour le financement

3.1 Aides aux projets de R&D

Les dépenses éligibles du projet sont susceptibles d'être soutenues par des financements de nature subventionnelle (subventions et, le cas échéant, avances remboursables) aux taux maximaux suivants, étant précisé que seulement les « dépenses éligibles » au sens de l'article 3.2 ci-dessous seront prises en compte pour le calcul de ces taux maximaux :

- 45% pour les micro-, petites et moyennes entreprises[2] ;
- 30% pour les entreprises intermédiaires[3] ;
- 25 % pour les grandes entreprises ;
- 40% des coûts analytiques liés au projet pour les autres partenaires (établissements de recherche[4], associations)[5].

Les soutiens aux entreprises feront l'objet d'un intéressement de l'Etat aux résultats du projet sous la forme d'un retour financier. Les modalités précises de ces retours seront déterminées en phase d'instruction des projets sélectionnés, avec un objectif d'intéressement de 33% des aides allouées aux entreprises, en moyenne pour le projet, sur la base de simulations issues d'un scénario économique médian. L'intéressement pourra consister en :

- des redevances sur le chiffre d'affaires découlant des résultats du projet (licences, ventes de systèmes…), lorsque ce chiffre d'affaires est identifiable ;

[2] Cf. définition en annexe

[3] Cf. définition en annexe

[4] Cf. définition en annexe

[5] Certains établissements de recherche peuvent toutefois opter pour un financement sur la base d'une aide à un taux maximum de 100 % des seuls coûts additionnels (hors salaires et charges des personnels et autres moyens statutaires). Dans ce dernier cas, l'établissement de recherche devra évaluer l'ensemble des moyens statutaires qu'il engage sur le projet, ces derniers devant être au moins du même ordre de grandeur que la subvention reçue.

ou

- un financement partiellement sous forme d'avance remboursable en cas de succès technique.

Le niveau de l'intéressement pour chaque partenaire pourra tenir compte de son rôle dans le projet et de la valorisation prévue des résultats du projet. Lorsque l'intéressement pour un partenaire atteint au moins 33% de l'aide allouée à celui-ci sur la base de simulations issues d'un scénario économique médian, le comité d'engagement pourra décider d'augmenter le taux de soutien maximal d'au plus 5% par rapport aux taux prévus ci-dessus.

3.2 Dépenses éligibles pour les projets de R&D

Seules sont éligibles les dépenses réelles spécifiques au projet de R&D faisant l'objet de la demande d'aide. Elles seront précisées dans les conventions d'aides et s'inscrivent dans les catégories admissibles suivantes :

Pour toutes les entreprises :

Les coûts admissibles qui relèvent de la réalisation du projet de R&D :

- Les frais de personnels (chercheurs, techniciens et autres personnels d'appui s'ils sont employés pour le projet de recherche).

- Les coûts des instruments et du matériel dans la mesure où et aussi longtemps qu'ils sont utilisés pour le projet de recherche. Si ces instruments et ce matériel ne sont pas utilisés pendant toute leur durée de vie pour le projet, seuls les coûts d'amortissements correspondant à la durée de projet, calculés conformément aux bonnes pratiques comptables sont jugés admissibles ;

- Les coûts de la recherche contractuelle, des connaissances techniques et des brevets ou licences d'exploitation acquis auprès de sources extérieures au prix du marché, lorsque l'opération a été réalisée dans le respect du principe de pleine concurrence et en l'absence de tout élément de collusion, ainsi que les coûts de services de conseil et équivalents utilisés exclusivement aux fins de l'activité de recherche. En particulier, les dépenses d'évaluation de produits, si elles sont justifiées par l'objet du projet et dans la limite de 10% de l'ensemble des dépenses.

- Les frais généraux supplémentaires encourus directement du fait du projet de recherche, dans des limites précisées dans les conventions d'aide.

- Les autres frais d'exploitation, notamment les coûts des matériaux, fournitures et produits similaires, supportés directement du fait de l'activité de recherche.

Pour les PME :

En plus des catégories de coûts éligibles ci-dessus les coûts supportés par PME énoncés ci-après sont éligibles dès lors qu'ils permettent d'assurer la protection d'un résultat direct résultat du projet de R&D financé et que cette protection bénéficie uniquement à la PME.

Les coûts admissibles sont :

- Tous les coûts antérieurs à l'octroi des droits dans la première juridiction, y compris les coûts d'élaboration, de dépôt et de suivi de la demande, ainsi que les coûts de renouvellement de la demande avant l'octroi des droits.

- Les frais de traduction et autres liés à l'obtention ou à la validation des droits dans d'autres juridictions.

- Les coûts liés à la défense de la validité des droits dans le cadre du suivi officiel de la demande et d'éventuelles procédures d'opposition, même s'ils sont exposés après l'octroi des droits.

Les organismes de recherche peuvent bénéficier des financements publics sur la base des coûts éligibles définis pour toutes les entreprises à l'exclusion de ceux prévus pour les PME.

Pour les établissements de recherche bénéficiant d'aides aux coûts additionnels (cf. §3.1 2ème alinéa), les salaires et charges des personnels statutaires ne peuvent pas être retenus dans les dépenses éligibles, mais doivent néanmoins être explicités dans le dossier (annexe technique).

4 Modalités de mise en œuvre

4.1 Processus de présélection et d'attribution de financements

Le processus de présélection des projets et de décision de financement, piloté par le comité d'engagement « subventions – avances remboursables » du FSN, s'effectue **en deux phases successives** :

4.1.1 Phase 1 : Présélection des projets

- L'examen des propositions (éligibilité et évaluation) est mené par un comité d'experts sur la base du dossier remis à l'occasion du présent appel à projets.
- La présélection des projets est menée par le comité d'engagement « subventions – avances remboursables » du FSN, sur la base de l'évaluation du comité d'experts. La décision de présélectionner un projet pourra être accompagnée de conditions particulières émises par le comité d'engagement.

4.1.2 Phase 2 : Décision de financement

Cette phase inclut les étapes suivantes :

- instruction détaillée du dossier en vue de la décision de financement ; au cours de cette phase, des informations complémentaires sur les partenaires du projet et le projet lui-même peuvent être demandées ;
- discussion et finalisation avec les partenaires du projet de convention de soutien, notamment concernant les modalités et le niveau d'intéressement de l'Etat aux résultats du projet ;
- préparation des annexes techniques et financières des conventions de soutien;
- soumission du dossier de financement au comité d'engagement du FSN ;
- décision du Comité d'engagement – ou, le cas échéant, du Premier Ministre – d'attribuer le financement, et conditions d'attribution.

4.2 Modalité de remise du dossier de soumission

Le dossier de soumission doit être déposé sur le site CDC des consultations investissements d'avenir :

Site CDC des consultations investissements d'avenir
http://cdcinvestissementsdavenir.achatpublic.com

Si les documents de soumission ne contiennent pas de signature électronique, leur dépôt en ligne doit être complété par la transmission des documents originaux signés. Ces derniers doivent être remis contre récépissé ou envoyés par pli recommandé avec avis de réception postal au plus tard dix (10) jours ouvrés après la date de clôture à :

Caisse des Dépôts
Département du développement numérique des territoires
FSN - Appel à Projets « *Cœur de filière – sécurité numérique* »
72, avenue Pierre Mendès-France
75914 Paris Cedex 13

Tout dossier reçu au-delà de la période de dix jours ouvrés indiquée ci-dessus ou transmis uniquement en version papier ne sera pas étudié.

4.3 Contenu du dossier de soumission

Le dossier de soumission est téléchargeable aux adresses de publication de l'appel à projets.

Le dossier de soumission doit contenir les éléments listés ci-dessous pour lesquels les modèles à utiliser sont à télécharger sur les sites de publication de l'appel à projet (cf. page 2).

Les dossiers de soumission des projets de R&D sont composés :

- des pièces relatives au projet, listées dans le document « 1 - liste_dossier_projet_complet » ;
- des pièces relatives à chaque partenaire, selon son type, listées dans les documents
  - « 1 - liste_dossier_complet_entreprise »,
  - « 1 - liste_dossier_complet_etablissement_public »,
  - « 1 - liste_dossier_complet_association_GIP ».

L'utilisation des modèles fournis est obligatoire.

4.4 Règles d'éligibilité des projets

Un projet est éligible au présent appel aux conditions suivantes :

- **il s'inscrit dans un ou plusieurs des axes technologiques** précisés en §2.2 ou tout au moins a pour objet principal le développement d'une technologie, d'un équipement, d'un service ou d'une solution dont l'application principale est la cyber-sécurité ou la sécurité de systèmes d'information. Les propositions qui couvrent les axes technologiques devront les indiquer explicitement ;

- il est **à fort contenu innovant** ;

- le financement demandé porte sur des **travaux de R&D réalisés en France, de type « recherche industrielle » ou « développement expérimental »**, au sens des définitions européennes[6] ;

- **le projet est coopératif au sens des règles européennes**[7] ;

- **le consortium est conduit, dans le cas où le projet est coopératif, par une entreprise chef de file** ; la contribution des entreprises partenaires aux coûts du projet représente la majorité des dépenses prévisionnelles de R&D ;

- **les travaux n'ont pas commencé** avant que la demande d'aide ait été soumise ;

- **l'assiette éligible des travaux ne fait pas déjà l'objet d'un autre financement** par l'État, les Collectivités Territoriales, l'Union européenne ou leurs agences[8] ;

- le projet présente des **perspectives de retombées économiques** pour le territoire national en termes d'emploi (accroissement, maintien de compétences), d'investissement, de structuration d'une filière ou d'anticipation de mutations économiques ;

- **le dossier de candidature (cf. §4.3) est complet** et remis avant la date de clôture de l'AAP (cf. conditions en page. 2).

Les projets ne respectant pas l'un de ces critères seront écartés du processus de sélection, sans recours possible.

4.5 Règles d'éligibilité des partenaires

Pour être éligible à une aide, le partenaire d'un projet éligible doit :

- être une entreprise, un établissement de recherche ou une association ;

- ne pas être en difficulté au sens des lignes directrices communautaires concernant les aides d'Etat au sauvetage et à la restructuration d'entreprises en difficulté ;

- ne pas faire l'objet d'une injonction de récupération suivant une décision antérieure de la Commission européenne déclarant des aides illégales et incompatibles avec le marché intérieur ;

- avoir la capacité financière d'assurer, pour les travaux qu'il prévoit d'engager, la part des coûts restant à sa charge après déduction de l'aide ;

- avoir une feuille de route technologique cohérente avec les objectifs du projet ;

6 Cf. définition en annexe

7 Cf. définition en annexe

8 L'appréciation de ce critère d'éligibilité tiendra compte de la nature des financements en question. Sous réserve de l'examen détaillé de la situation de l'entreprise, ce critère n'exclut pas les financements de nature non subventionnelle apportés par des établissements bancaires ou des organismes tels qu'Oseo pour financer la part des dépenses de R&D de l'entreprise non couverte par l'aide sollicitée De plus, ce critère n'exclut pas le co-financement du projet par les collectivités territoriales, dans la limite du taux d'aide global prévu au §3.1.

- avoir un plan de valorisation des résultats du projet (sauf laboratoire public).

En outre, dans le cadre d'un projet de R&D, les grandes entreprises doivent démontrer le caractère incitatif de l'aide demandée (l'aide accroît la taille, la portée, le budget ou le rythme des activités de R&D).

4.6 Critères d'évaluation pour la présélection

Cette présélection s'appuiera sur les critères suivants :

- **Adéquation aux objectifs de l'appel à projets**, notamment prise en compte des axes technologiques prioritaires décrits au § 2.2 et des points d'attention communs détaillés au §2.3 ;

- **Pertinence technologique et industrielle :**

  - **Ambition technologique,** rupture et originalité par rapport à une simple incrémentation des technologies, eu égard à l'état de l'art européen et mondial ; potentiel en matière de normalisation ;

  - **Maturité industrielle**, à savoir la mise à disposition des ressources et des moyens nécessaires pour développer des produits dans un degré d'aboutissement relativement élevé (TRL au moins égal à 7), visant à répondre à des besoins effectifs du marché, notamment s'agissant de grandes organisations pour lesquelles la sécurité numérique est un enjeu clé (Etat, administrations, grandes entreprises), et offrant de bonnes perspectives commerciales dans un avenir relativement proche ;

- **Impact économique :**

  - **Nature stratégique du projet** pour les partenaires impliqués dans le projet (le projet devra s'inscrire, pour chaque partenaire industriel, dans une stratégie technologique et industrielle de moyen terme, accompagnée d'informations sur le marché visé, de la position concurrentielle des acteurs et les perspectives de revenus pour chaque entreprise impliquée) ;

  - **Retombées en matière de création de valeur, d'activités** (perspectives économiques et commerciales et volume des marchés visés, compte tenu du positionnement des partenaires sur ces marchés), **d'emplois** (création d'emplois de personnel de R&D à court terme, développement potentiel de l'emploi dans la phase d'industrialisation et de déploiement commercial…) ;

  - **Positionnement concurrentiel** par rapport à l'offre internationale existante et aux futurs marchés pressentis en termes de performances, de fonctionnalités et de prix.

- **Partenariat :**

  - **Qualité du consortium** : présence de partenaires-clés du domaine, complémentarité technologique entre les partenaires, présence de la masse critique vis-à-vis des verrous

technologiques visés, complémentarité, notamment entre fournisseurs de technologies et utilisateurs ;

- **Structuration de l'écosystème**, notamment présence de PME ou d'établissements de recherche ; l'attribution d'un label par un ou plusieurs pôles de compétitivité sera, à ce titre, un élément favorable d'appréciation ;
- **Gestion du projet** (organisation des travaux, règles de gouvernance entre les partenaires, gestion des risques, livrables, planification...).

La qualité des informations apportées par les partenaires sur la pertinence de leur projet vis-à-vis de ces différents critères sera déterminante dans l'évaluation. Ils sont ainsi encouragés à présenter des informations précises et si possible quantifiées (dimension des marchés, perspectives d'augmentation du volume d'affaires, création d'emploi etc.).

ANNEXE 1 : Définitions

Un projet est au **coopératif** au sens communautaire notamment lorsque :

i) le projet repose sur une coopération effective entre au moins deux entreprises indépendantes l'une de l'autre et les conditions suivantes sont remplies :
   - aucune entreprise ne supporte seule plus de 70 % des coûts admissibles du projet de coopération,
   - le projet prévoit une coopération avec au moins une PME,

ou :

ii) le projet repose sur une coopération effective entre une entreprise et un organisme de recherche et les conditions suivantes sont remplies :
   - l'organisme de recherche supporte au moins 10 % des coûts admissibles du projet, et
   - l'organisme de recherche a le droit de publier les résultats des projets de recherche dans la mesure où ils sont issus de recherches qu'il a lui-même effectuées.

« **Développement expérimental** », l'acquisition, l'association, la mise en forme et l'utilisation de connaissances et de techniques scientifiques, technologiques, commerciales et autres existantes en vue de produire des projets, des dispositifs ou des dessins pour la conception de produits, de procédés ou de services nouveaux, modifiés ou améliorés. Il peut s'agir notamment d'autres activités visant la définition théorique et la planification de produits, de procédés et de services nouveaux, ainsi que la consignation des informations qui s'y rapportent. Ces activités peuvent porter sur la production d'ébauches, de dessins, de plans et d'autres documents, à condition qu'ils ne soient pas destinés à un usage commercial. La création de prototypes et de projets pilotes commercialement exploitables relève également du développement expérimental lorsque le prototype est nécessairement le produit fini commercial et lorsqu'il est trop onéreux à produire pour être utilisé uniquement à des fins de démonstration et de validation. En cas d'usage commercial ultérieur de projets de démonstration ou de projets pilotes, toute recette provenant d'un tel usage doit être déduite des coûts admissibles. La production expérimentale et les essais de produits, de procédés et de services peuvent également bénéficier d'une aide, à condition qu'ils ne puissent être utilisés ou transformés en vue d'une utilisation dans des applications industrielles ou commerciales Le développement expérimental ne comprend pas les modifications de routine ou périodiques apportées à des produits, lignes de production, procédés de fabrication, services existants et autres opérations en cours, même si ces modifications peuvent représenter des améliorations.

Entreprise intermédiaire : au sens du présent appel à projets, entreprises non PME qui n'emploient pas plus de 2000 personnes et n'appartiennent pas, du fait de relations de détention de capital à hauteur d'au moins 50% en amont ou en aval, à un ensemble employant plus de 2000 personnes au total.

Établissement de recherche : entité, telle qu'une université, un organisme, une fondation de coopération scientifique ou un institut de recherche, quel que soit son statut légal (organisme de droit public ou privé) ou son mode de financement, ayant pour mission d'exercer les activités de recherche fondamentale ou de recherche industrielle ou de développement expérimental et de diffuser leurs résultats par l'enseignement, la publication ou le transfert de technologie ; les profits sont intégralement réinvestis dans ces activités, dans la diffusion de leurs résultats ou dans l'enseignement ; les entreprises qui peuvent exercer une influence sur une telle entité, par exemple en leur qualité d'actionnaire ou de membre, ne bénéficient d'aucun accès privilégié à ses capacités de recherche ou aux résultats qu'elle produit.

La catégorie des **micro-, petites et moyennes entreprises** (PME) est constituée des entreprises qui occupent moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total du bilan annuel n'excède pas 43 millions d'euros.» Extrait de l'article 2 de l'annexe à la recommandation 2003/361/CE. Pour plus de renseignements, consulter : http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_fr.pdf

« Recherche industrielle », la recherche planifiée ou des enquêtes critiques visant à acquérir de nouvelles connaissances et aptitudes en vue de mettre au point de nouveaux produits, procédés ou services, ou d'entraîner une amélioration notable de produits, procédés ou services existants. Elle comprend la création de composants de systèmes complexes, nécessaire à la recherche industrielle, notamment pour la validation de technologies génériques, à l'exclusion des prototypes visés au point g).

ANNEXE 2 : MODALITES DE SOUMISSION

Comme indiqué plus haut, les porteurs de projets sont invités à déposer leur dossier sur le site Caisse des Dépôts des consultations Investissements d'avenir accessible à l'adresse suivante :
http://cdcinvestissementsdavenir.achatpublic.com

Le site des consultations Investissements d'avenir de la Caisse des Dépôts offre une plate-forme et des échanges sécurisés.

Il est dès lors nécessaire :

- d'installer l'environnement d'exécution Java pour déposer le projet ; un lien permettant l'installation gratuite du logiciel est proposé lors du téléchargement ; le soumissionnaire contactera son service informatique si celui-ci a la responsabilité de contrôler l'installation de nouveaux logiciels ;

- d'ouvrir un compte sur le site de la consultation ;

- de prendre en considération le fait que la durée du téléchargement est fonction du débit de l'accès internet du soumissionnaire et de la taille des documents à transmettre, et **de ne pas attendre la date limite de dépôt des projets pour la transmission des fichiers de réponse par voie électronique**. Seule l'heure de fin de réception fait foi : la date et l'horodatage proviennent de la plate-forme et le soumissionnaire remettant un pli électroniquement en accepte explicitement l'horodatage ;

- de prévoir les modalités de signature des documents par le coordonnateur du projet et ses partenaires [certificat électronique de signature avec utilisation de la fonction « gestion de parapheur (onglet « outils), ou bien scannage des signatures avec alors, en plus, envoi postal en pli recommandé avec accusé de réception (cf. point 4.2. de l'appel à projets)] ; le certificat de signature est donc facultatif ;

- de se reporter pour plus de détails au guide d'utilisation accessible sur le site des consultations et d'appeler en cas de problème l'assistance téléphonique au 0 892 23 21 20.

Les porteurs de projet qui souhaiteraient, en amont du dépôt réel de leur dossier de réponse, tester cette procédure sont invités à se connecter sur le site de formation mis à leur disposition à l'adresse URL suivante :

https://formation-empruntnational.achatpublic.com/ecole-sdm/ent/gen/ent_detail.do?PCSLID=CSL_2011_JGR3SUMn3B&v=1&selected=0

Ils devront télécharger la consultation test, puis déposer une réponse fictive en suivant les instructions données. Ce dépôt ne pourra en aucun cas être considéré comme une réponse valide au présent appel à projets.