18.xxx

Message concernant le crédit d'engagement pour le système national d'échange de données sécurisé

du ...

Monsieur le Président,
Madame la Présidente,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'un arrêté fédéral concernant le crédit d'engagement pour le système national d'échange de données sécurisé, en vous proposant de l'adopter.

Nous vous prions d'agréer, Monsieur le Président, Madame la Présidente, Mesdames, Messieurs, l'assurance de notre haute considération.

…

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

Condensé

Au quotidien, mais surtout en cas de catastrophe et en situation d'urgence, les organes de conduite de la Confédération, des cantons et des communes, les autorités et les organisations d'intervention responsables de la sécurité et du sauvetage et les exploitants d'infrastructures critiques doivent échanger des informations de manière rapide et sûre. L'exercice du réseau national de sécurité 2014 a permis de constater que les systèmes de communication civils seraient indisponibles ou que leur fonctionnement serait fortement limité en cas de pénurie d'électricité. Le rapport final relatif à l'exercice souligne en outre l'absence de vue d'ensemble illustrée et de suivi coordonné de la situation et la nécessité d'y remédier. Ces constatations ont été confirmées lors de l'exercice de conduite stratégique 2017. En vue de combler cette faille de sécurité, le Conseil fédéral demande, par le présent message, un crédit d'engagement de 150 millions de francs pour le développement et l'acquisition d'un système national d'échange de données sécurisé.

Contexte

L'évolution des risques et des menaces pose de nouveaux défis en matière de protection de la population. Nous avons toujours davantage besoin d'un approvisionnement électrique fiable en toute situation. En cas de panne d'électricité, les systèmes de télécommunication sont hors service. En outre, des risques surgis récemment, comme les cyberattaques dirigées contre la population ou les exploitants d'infrastructures critiques, gagnent en importance à l'échelle mondiale et la menace terroriste s'est aggravée.

Des failles de sécurité sont apparues dans les systèmes de télécommunication actuels. L'exercice du réseau national de sécurité 2014 a permis de constater que ces systèmes seraient indisponibles ou que leur fonctionnement serait fortement limité en cas de pénurie d'électricité. Ce problème est notamment dû au fait que les réseaux commerciaux utilisés sont peu fiables en temps de crise, voire pas du tout. Or des systèmes dont les fonctionnalités sont limitées ne permettent pas un flux de données et d'informations suffisamment stable, rapide et fiable. De plus, il manque un système à même de garantir une vue d'ensemble d'une situation complexe en cas de tremblement de terre, d'accident dans une centrale nucléaire ou d'attaque terroriste. Ces constatations ont été confirmées lors de l'exercice de conduite stratégique 2017.

En cas de catastrophe et de situation d'urgence, les organes de conduite, les autorités et les organisations concernées ainsi que les exploitants d'infrastructures critiques ont besoin de systèmes de communication efficaces et d'une vue d'ensemble consolidée de la situation afin de transmettre l'alarme, d'assurer des prestations vitales et de prendre des mesures de sécurité permettant de protéger la population. Il leur faut impérativement être informés à tout moment et dans tous les cas de figure de l'évolution de la situation et de systèmes de conduite afin d'être en possession de toutes les informations nécessaires et de garantir la mise en œuvre des mesures de protection.

Pour combler les failles de sécurité mises au jour, il faut fournir de nouveaux systèmes de télécommunication aux organes de conduite de la Confédération, des cantons et des communes, aux autorités et organisations d'intervention chargées du sauvetage et de la sécurité et aux exploitants d'infrastructures critiques. Le 18 décembre 2015, le Conseil fédéral a ainsi chargé le Département fédéral de la défense, de la protection de la population et des sports (DDPS) d'effectuer une évaluation des projets de télécommunications importants pour la protection de la population suisse. Le rapport met notamment en évidence les systèmes qui sont indispensables pour protéger efficacement la population de notre pays et qui doivent donc être réalisés ou améliorés à court terme. Le DDPS a mis le projet de rapport en consultation auprès des cantons, des organes fédéraux concernés, des exploitants d'infrastructures critiques et d'autres organisations entre septembre et décembre 2016 et a reçu 72 avis en retour. La consultation a montré qu'une priorité absolue devait être accordée à un système d'échange de données par câble sécurisé, qui soit renforcé contre les pannes d'électricité et protégé des cyberattaques. Cet avis est partagé par les services de la Confédération, les cantons et les exploitants d'infrastructures critiques.

Pour améliorer la sécurité des systèmes de télécommunication et l'échange à large bande d'informations et de données entre les organes de conduite, les autorités actives dans le domaine de la sécurité, les organisations d'intervention et les exploitants d'infrastructures critiques et pour augmenter la protection contre les cyberattaques, le présent projet prévoit de créer un système national d'échange de données sécurisé réunissant la Confédération, les cantons et des tiers.

Les compétences et le financement du système entre la Confédération, les cantons et les tiers sont présentés dans le message concernant la révision totale de la loi sur la protection de la population et sur la protection civile (LPPCi). Cette dernière est soumise au Parlement dans un message distinct. Le Conseil fédéral entend mettre en vigueur la nouvelle loi révisée le 1er janvier 2020, sous réserve de la décision du Parlement. La solution proposée est le fruit d'un large consensus entre la Confédération et les cantons.

Le développement et l'acquisition du système national d'échange de données sécurisé tel qu'il est proposé contribuera à combler la faille de sécurité identifiée et donc à améliorer la protection de la population.

Contenu du projet

En adoptant l'arrêté fédéral, le Parlement accorde un crédit d'engagement d'un montant de 150 millions de francs. Ce montant sera libéré en trois tranches: la première, de 14,7 millions de francs, est libérée avec l'arrêté fédéral; la deuxième, de 83,6 millions de francs, et la troisième, de 51,7 millions de francs, seront libérées sur décision du Conseil fédéral en fonction de l'avancement du projet.

Les investissements seront échelonnés jusqu'en 2027. L'Office fédéral de la protection de la population (OFPP) est responsable de la direction et de la gestion du projet et se voit également déléguer la responsabilité des acquisitions. Le crédit d'engagement inclut la gestion du projet, les travaux de développement,

l'acquisition du matériel et des logiciels, les licences, les infrastructures et les prestations de gestion et de maintenance du réseau.

L'exploitation et la maintenance du système d'échange de données sécurisé auront pour effet d'augmenter les dépenses annuelles de fonctionnement de l'OFPP 100 000 francs en 2020, de 600 000 francs en 2021, de 1,5 million de francs en 2022, de 7 millions de francs en 2023, de 10 millions de francs en 2024, de 12 millions de francs en 2025, de 13,9 millions de francs en 2026 et de 15 millions de francs à partir de 2027, frais de personnel non compris. Ces dépenses incluent des prestations de maintenance et d'exploitation du réseau de base et des 120 emplacements utilisateurs prévus, y compris la gestion de l'exploitation d'urgence 24 heures sur 24. La mise hors service du système de transmission de messages Vulpus entraînera, à partir de 2026, une diminution annuelle des frais d'exploitation de 1,5 million de francs.

Pour que le projet puisse être réalisé dans les délais impartis en respectant les prescriptions financières et qualitatives et pour garantir une exploitation sécurisée du système, jusqu'à 30 postes supplémentaires à plein temps sont nécessaires au DDPS, dont 15 durant la phase de projet. Sur ces 15 postes supplémentaires, 10 seront maintenus après la clôture du projet (postes à durée indéterminée) pour l'exploitation et l'entretien des installations techniques, la maintenance annuelle et la gestion des bénéficiaires de prestations.

Table des matières

Condensé **2**

1 Contexte et conditions-cadres **7**
1.1 Contexte 7
1.2 Motif de la demande de crédit 7
1.3 Intérêt du projet dans l'absolu 9
1.4 Intérêt du projet pour la Confédération 10
1.5 Enjeux pour l'avenir 11
1.6 Implication des milieux intéressés 12

2 Contenu de l'arrêté de crédit **13**
2.1 Proposition du Conseil fédéral 13
2.2 Description détaillée du projet 13
2.2.1 Le réseau de données sécurisé 13
2.2.2 Le système d'accès aux données 14
2.2.3 Le remplacement du système Vulpus et le réseau de suivi de la situation 15
2.2.4 Investissements 16
2.2.5 Échelonnement et libération 18
2.2.6 Exploitation et entretien 20
2.2.7 Réglementation des compétences et financement 21

3 Conséquences **23**
3.1 Conséquences pour la Confédération 23
3.1.1 Conséquences financières 23
3.1.2 Conséquences sur l'état du personnel 26
3.2 Conséquences pour les cantons 31
3.3 Conséquences économiques 31
3.4 Conséquences sociales 31
3.5 Conséquences environnementales 32

4 Relation avec le programme de la législature et les stratégies du Conseil fédéral **32**
4.1 Relation avec le programme de la législature 32
4.2 Relation avec les objectifs 2018 du Conseil fédéral 32
4.3 Relation avec les stratégies du Conseil fédéral 33

5 Aspects juridiques **35**
5.1 Constitutionnalité 35
5.2 Forme de l'acte à adopter 35
5.3 Frein aux dépenses 35

Liste des abréviations utilisées **36**

Arrêté fédéral concernant le crédit d'engagement pour le système national d'échange de données sécurisé *(projet)* **00**

Message

1 Contexte et conditions-cadres

1.1 Contexte

Il est primordial que les organes de conduite, les autorités en charge de la sécurité et du sauvetage, les organisations d'intervention et les exploitants d'infrastructures critiques puissent communiquer de façon sûre et échanger de façon protégée des informations et des vues d'ensemble de la situation afin de gérer efficacement les événements et garantir la sécurité et la protection de la population en toute situation.

Actuellement, la Confédération et les cantons passent par le réseau national des autorités de la Confédération et des cantons (KomBV-KTV), par les réseaux des polices cantonales ou par les réseaux des fournisseurs commerciaux pour échanger de grandes quantités de données ou utiliser des applications.

Les systèmes de communication et d'information civils actuellement utilisés présentent des failles de sécurité. L'exercice du réseau national de sécurité 2014 (ERNS 14) a permis de constater que le fonctionnement de ces systèmes serait fortement limité en cas de pénurie d'électricité, ce qui compromettrait la maîtrise d'une situation complexe. Les réseaux utilisés ne garantissent pas un flux de données et d'information en temps réel, fiable et régulier. Lors d'un événement, ils peuvent en effet tomber en panne en raison d'une surcharge, d'une défaillance du réseau électrique ou d'une cyberattaque. De plus, il manque un système à même de garantir une vue d'ensemble d'une situation complexe en cas de tremblement de terre, d'accident dans une centrale nucléaire ou d'attaque terroriste. Ces insuffisances au niveau de la sécurité ont été confirmées par l'exercice de conduite stratégique 2017 (ECS 17). Le rapport d'évaluation du 9 mai 2018 sur l'ECS 17[1] relève notamment l'absence d'une représentation commune de la situation, ce qui constitue une lacune fondamentale de la gestion des crises au niveau national. Il faut non seulement prendre des mesures afin de permettre une appréhension commune de la situation, mais aussi impérativement optimiser les outils technologiques. Par conséquent, les efforts consentis jusqu'ici afin de mettre en place une vue d'ensemble illustrée s'appuyant sur la présentation électronique de la situation (PES) et la coordination du suivi au profit de l'évaluation de la situation doivent demeurer prioritaires.

1.2 Motif de la demande de crédit

Le 1er décembre 2017, le Conseil fédéral a pris connaissance d'une évaluation des projets de télécommunications importants pour la protection de la population. Le

[1] Le rapport peut être consulté à l'adresse suivante: www.chf.admin.ch > Documentation > Conduite stratégique > Exercice de conduite stratégique (ECS).

rapport du 29 septembre 2017[2] met notamment en évidence les systèmes indispensables pour protéger efficacement la population suisse et détermine lesquels doivent être réalisés ou améliorés à court terme. L'évaluation de 72 prises de position a montré qu'une priorité absolue devait être accordée à un système d'échange de données par câble sécurisé, qui soit renforcé contre les pannes d'électricité et protégé des cyberattaques, ainsi qu'au remplacement du système de transmission de messages Vulpus, devenu obsolète. Cet avis est partagé par les services de la Confédération, (notamment fedpol, le Service de renseignement de la Confédération [SRC], l'Administration fédérale des douanes [AFD], MétéoSuisse, l'Office fédéral de l'environnement, l'Office fédéral de l'énergie, l'État-major fédéral Protection de la population [EMFP] et la Centrale nationale d'alarme [CENAL]), par les cantons et par les exploitants d'infrastructures critiques (notamment Swissgrid SA, CFF SA et la Banque nationale suisse), qui souhaitent avoir le plus vite possible accès à ce nouveau système.

La numérisation des communications entre les autorités et la population s'accompagne aussi de nouvelles vulnérabilités. Nous avons toujours davantage besoin d'un approvisionnement électrique fiable en toute situation. En cas de panne d'électricité, qu'elle soit due à un problème technique ou un événement naturel, les systèmes de télécommunication sont hors service. En outre, des risques surgis récemment, comme les cyberattaques contre les autorités et les exploitants d'infrastructures critiques, gagnent en importance à l'échelle mondiale et la menace terroriste s'est aggravée. Parallèlement, la maintenance des technologies analogiques n'est plus assurée, ce qui signifie par exemple que le système Vulpus des autorités civiles chargées de la sécurité en Suisse ne peut plus être utilisé et doit être remplacé par un nouveau système.

Lors de sa séance du 1er décembre 2017, le Conseil fédéral a constaté qu'il fallait améliorer la disponibilité des systèmes de télécommunication, donc leur résilience, et l'échange de données à large bande entre les organes de conduite, les autorités en charge de la sécurité et les exploitants d'infrastructures critiques, tout en améliorant la protection contre les cyberattaques. La création d'un système national d'échange de données sécurisé vise à atteindre ces objectifs.

Le système national d'échange de données sécurisé doit, d'une part, assurer la liaison à large bande entre les organes fédéraux, les cantons et les exploitants d'infrastructures critiques pendant au moins deux semaines, même en cas de pénurie d'électricité prolongée, de panne de courant ou de défaillance des réseaux publics de communication et, d'autre part, renforcer sensiblement l'intégrité et la protection des communications et des échanges de données en cas de cyberattaque. Ce système se composera d'un réseau de données sécurisé, d'un système d'accès aux données et d'un système qui garantit l'échange d'informations, images comprises, afin d'obtenir une vue d'ensemble de la situation (réseau de suivi de la situation). Ce

[2] Le rapport peut être consulté (en allemand uniquement) à l'adresse suivante : www.admin.ch > Documentation > Communiqués > Protection de la population : l'avenir des systèmes d'alarme et de communication (dans « Organisations », sélectionner « Département fédéral de la défense, de la protection de la population et des sports » et insérer « 01.12.2017 » dans les champs « De » et « À »).

dernier remplacera le système de transmission de messages Vulpus, devenu obsolète.

Reposant essentiellement sur l'infrastructure renforcée (emplacements, fibre optique) du réseau de conduite suisse, le système national d'échange de données sécurisé reliera à large bande quelque 120 emplacements utilisateurs et emploiera à cet effet une autre infrastructure de fibre optique existante qui appartient aux pouvoirs publics (directement ou au sens large).

Le système Vulpus est aujourd'hui exploité par l'armée. Il pourra être supprimé une fois que le système national d'échange de données sécurisé et le réseau de suivi de la situation entreront en service. L'abandon du système obsolète Vulpus au profit d'un réseau national de suivi de la situation permettra aux organes de conduite, aux autorités chargées de la sécurité, aux organisations d'intervention et aux exploitants d'infrastructures critiques de disposer d'une vue d'ensemble illustrée de la situation. Celle-ci représente un instrument de conduite déterminant pour maîtriser rapidement et efficacement des événements aux conséquences complexes, intercantonales, nationales ou internationales.

À l'avenir, le système national d'échange de données sécurisé constituera, lors de la transmission d'importantes quantités de données, le socle de tous les systèmes de télécommunication prioritaires pour la politique de sécurité, devenant ainsi le réseau de communication central servant à transmettre en toute situation, y compris en cas d'attentat, des données et des informations en faveur de la protection de la population et de la gestion de crises à l'échelon national. Il est ainsi prévu d'intégrer au futur système les réseaux de sécurité Polycom et Polyalert et la radio d'urgence IPCC. Aussi les autorités pourront-elles s'en servir au quotidien pour l'échange d'informations concernant la politique de sécurité. De même, le KomBV-KTV pourra avoir recours à l'infrastructure du système national d'échange de données sécurisé, alors même qu'il demeurera un réseau de communication distinct, ce qui permettra d'optimiser la sécurité de l'alimentation électrique des éléments utilisés en commun.

Selon la planification actuelle, 120 emplacements utilisateurs seront réalisés auprès de la Confédération, des cantons et des exploitants d'infrastructures critiques. D'autres pourront l'être au besoin, dans la mesure où les conditions de raccordement seront remplies.

1.3 Intérêt du projet dans l'absolu

La vulnérabilité de l'échange à large bande de données et d'informations entre les organes de conduite, les autorités en charge de la sécurité, les organisations d'intervention et les exploitants d'infrastructures critiques constitue un risque important pour la sécurité.

La communication et la présentation rapide et sûre de la situation générale avec des illustrations jouent un rôle prépondérant pour une gestion efficace des événements. Les événements de grande ampleur survenus en Suisse au cours des dernières années (Vivian en 1990 ou Lothar en 1999, canicule en 2003 et 2015, crues en 2005 et

2007, panne d'électricité des CFF en 2005, grippe porcine en 2009, incendie de forêt à Viège en 2011, éboulement à Bondo en 2017) ont montré l'importance croissante de la collaboration entre les autorités, les forces d'intervention et les exploitants d'infrastructures critiques. Assurer cette collaboration requiert une bonne interopérabilité et l'échange d'informations sur la situation entre tous les acteurs. L'ERNS 14 et l'ECS 17 ont confirmé cette nécessité.

Des expériences faites à l'étranger ont montré qu'il n'est possible de gérer efficacement et rapidement des événements aux conséquences complexes (p. ex. séismes, attaques terroristes) et d'éviter des blessés, des morts et des dégâts que si tous les acteurs impliqués disposent dans les plus brefs délais d'un aperçu de la situation complet. C'est précisément l'utilité d'un réseau de suivi de la situation rassemblant les systèmes de la Confédération, des cantons et des exploitants d'infrastructures critiques et réunissant automatiquement les informations issues de ces différents systèmes au sein d'une présentation générale de la situation, avec des illustrations. Un tel système permet également de remplacer le système de transmission de messages Vulpus, devenu obsolète.

La mise en place du système national d'échange de données sécurisé permettra d'éliminer les lacunes en matière de sécurité lors de l'échange d'informations et d'aperçus de la situation entre les organes concernés, de réduire dans une mesure importante le risque de panne des systèmes et d'améliorer la sécurité de la population. Ce système améliorera aussi énormément la sécurité. Par exemple, il sera possible d'échanger facilement et avec un niveau de sécurité nettement plus élevé les informations de MétéoSuisse nécessaires à l'exploitation des aéroports.

1.4 Intérêt du projet pour la Confédération

La Confédération, les cantons et d'autres organes œuvrent ensemble, dans le cadre de leurs compétences respectives, pour la protection de la population, notamment dans le domaine des systèmes d'alarme et de communication. Il est de l'intérêt de tous de veiller à l'interopérabilité de ces systèmes et des connexions sécurisées entre ces organes. En mettant à disposition des composants centraux pour le système national d'échange de données sécurisé, la Confédération garantit l'interopérabilité des systèmes, offre la possibilité aux organes fédéraux, aux cantons et aux exploitants d'infrastructures critiques de raccorder leurs propres systèmes à un système global et pose les bases d'une connexion à large bande sécurisée. Par exemple, la Banque nationale suisse, qui a pris position dans le cadre de l'évaluation des systèmes de télécommunication importants pour la protection de la population, voit dans la réalisation du système national d'échange de données sécurisé une contribution déterminante à la résilience opérationnelle de la place financière suisse. La réalisation de ce nouveau système, couplée avec celle du réseau de suivi de la situation, permettra aussi de remplacer le système de transmission de messages Vulpus, devenu obsolète.

La Confédération assume la responsabilité de la conduite en cas de catastrophe et en situation d'urgence de portée nationale. Pour remplir efficacement cette tâche, elle doit pouvoir compter sur une connexion sécurisée avec les organes de conduite

cantonaux et les exploitants d'infrastructures critiques et disposer d'un aperçu consolidé de la situation.

1.5 Enjeux pour l'avenir

La mise en place du système national d'échange de données sécurisé favorisera l'introduction de moyens numériques pour la gestion des événements. Un système renforcé contre les pannes d'électricité et protégé contre les cyberrisques permet de mieux exploiter, au profit de la sécurité, les avantages des développements numériques dans le domaine de la communication et de l'échange d'informations grâce à une meilleure résilience. On améliore ainsi l'efficacité des interventions et la protection de la population.

Il est possible que le système de communication Polycom soit remplacé par un système mobile de communication de sécurité à large bande dès que les applications de radiocommunication à large bande seront standardisées. Afin de répondre aux exigences d'une communication sécurisée et résiliente des données jusqu'aux terminaux mobiles des organisations d'intervention sur l'ensemble du territoire national, une extension mobile à capacité limitée du système national d'échange de données sécurisé serait envisageable selon les besoins. Étant donné que ce nouveau système sera protégé contre les pannes d'électricité et les cyberattaques, les utilisateurs disposeront d'un réseau de transmission sûr, doté d'une composante mobile et donc disponible en toute situation.

Le système national d'échange de données sécurisé constitue une valeur ajoutée pour les autres usagers qui accordent une grande importance à la disponibilité en cas de pannes d'électricité ou de défaillances informatiques. Il peut servir de plate-forme de transmission pour d'autres systèmes et améliorer dans une mesure importante leur fiabilité.

La disponibilité du système national d'échange de données sécurisé permet aussi d'évaluer et, si nécessaire, d'éliminer les redondances avec d'autres réseaux. Dans certains secteurs, comme l'approvisionnement en énergie et la place financière suisse, le système pourrait être utilisé comme réseau de communication de données redondant et améliorer ainsi la résilience de ces secteurs critiques. Il existe en outre de nombreuses autres possibilités d'utilisation dans le domaine de la sécurité.

La nécessité de prendre périodiquement des mesures de maintien de la valeur à caractère d'investissement sur certains éléments du système ne fait pas l'objet du présent message. Ces mesures sont à la charge de la Confédération, conformément au règlement financier proposé dans le message du … concernant la révision totale de la LPPCi[3]. Un nouveau crédit d'engagement sera demandé en temps voulu.

3 FF **2018** …

1.6 Implication des milieux intéressés

Aux termes de l'art. 2, al. 1, de la loi du 18 mars 2005 sur la consultation[4], la procédure de consultation vise à associer les cantons, les partis politiques et les milieux intéressés à la définition de la position de la Confédération et à l'élaboration de ses décisions. Bien que l'on soit en présence d'un projet d'une grande portée financière, aucune procédure de consultation n'a eu lieu. En effet, de nombreux avis ont été recueillis préalablement au sujet des systèmes projetés, de sorte qu'une consultation supplémentaire n'aurait sans doute pas apporté d'enseignements nouveaux.

Dans le cadre de l'élaboration du rapport sur l'avenir des systèmes de télécommunication de la protection de la population et de la procédure de consultation menée à cette occasion, les services fédéraux et cantonaux concernés, les exploitants d'infrastructures critiques, les associations et les organisations de la société civile ont été invités à donner leur avis sur l'ordre de priorité à établir. En tout, 72 prises de position ont été remises. Il en est ressorti que la priorité devait être accordée au système d'échange de données sécurisé, au remplacement du système obsolète de transmission de messages Vulpus et à la mise en place d'un réseau de suivi de la situation. Les participants ont demandé que les coûts de ces projets soient définis de manière plus précise dès qu'une décision politique de principe aura été prise sur leur réalisation.

Différents travaux et études ont été effectués durant la phase d'initialisation du projet de réseau de suivi de la situation, avec le concours des organes fédéraux et cantonaux intéressés. Un questionnaire a ainsi été soumis à 18 services fédéraux et 59 services cantonaux. Les attentes et les exigences générales par rapport au système ont été discutées et analysées lors de cinq ateliers ayant réuni plus de 100 participants. Les résultats ont été consignés dans une étude. Une description des aspects techniques de l'architecture du système et un document faisant la synthèse des objectifs ont en outre été rédigés. Un plan de mise en œuvre décrit le projet au niveau stratégique. Enfin, l'OFPP a procédé à un sondage auprès des fournisseurs potentiels concernant la création du réseau. Le projet a été jugé tout à fait réalisable et judicieux des points de vue technique, opérationnel et organisationnel.

Les examens menés ont montré que le remplacement du système de transmission de messages Vulpus et la mise en place d'un réseau de suivi de la situation présentaient un important potentiel de synergies. Une solution moderne pour le remplacement de Vulpus correspondrait largement aux fonctionnalités exigées par un réseau de suivi de la situation.

Le chef du DDPS et les présidents de la Conférence des directeurs des départements cantonaux de justice et police (CCDJP) et de la Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers (CG MPS) ont mis en place, le 10 janvier 2017, un groupe de travail composé de représentants de la Confédération et des cantons afin de définir les compétences et de régler les questions financières. Les travaux de ce groupe ont permis de dégager un consensus et de convenir d'un principe de financement avec les cantons.

4 RS **172.061**

2 Contenu de l'arrêté de crédit

2.1 Proposition du Conseil fédéral

Le système national d'échange de données sécurisé constitue un projet clé de la Confédération dans le domaine des technologies de l'information et de la communication. Pour le réaliser, le Conseil fédéral demande un crédit d'engagement de 150 millions de francs. La Confédération prend ainsi à sa charge les investissements en matière de développement et d'acquisition des composants centraux du futur système, accessibles à tous les utilisateurs (organes fédéraux, cantons, exploitants d'infrastructures critiques).

Le crédit d'engagement sera libéré en trois tranches. En l'adoptant, les Chambres fédérales libéreront la première tranche de 14,7 millions de francs. La deuxième tranche, de 83,6 millions de francs, et la troisième tranche, de 51,7 millions de francs, seront libérées sur décision du Conseil fédéral en fonction de l'avancement du projet.

2.2 Description détaillée du projet

Le système national d'échange de données sécurisé comprend :

a. le réseau de données sécurisé ;

b. le système d'accès aux données ;

c. le réseau de suivi de la situation destiné à remplacer le système de transmission de messages Vulpus, devenu obsolète.

2.2.1 Le réseau de données sécurisé

En tant que réseau de transmission (couches 1 et 2) pour la communication de données à large bande, le réseau de données sécurisé constituera la base de tous les systèmes de télécommunication de la protection de la population utilisés pour la politique de sécurité. Il devra assurer de manière autonome la liaison à large bande entre les organes fédéraux, les cantons et les exploitants d'infrastructures critiques pendant au moins deux semaines, même en cas de pénurie d'électricité prolongée, de panne de courant ou de défaillance des réseaux de communication commerciaux. Le crédit d'engagement permettra de raccorder 120 emplacements utilisateurs à ce réseau. Chaque emplacement sera relié à au moins deux nœuds renforcés. Quarante raccordements sont prévus pour les organes fédéraux, dont fedpol, le SRC, l'AFD, le Corps des gardes-frontière (Cgfr), MétéoSuisse, l'EMFP et la CENAL; 44 sont planifiés pour les exploitants d'infrastructures critiques tels que les aéroports, les CFF SA, Swissgrid SA, la Banque nationale suisse, les stations de radio et de télévision, les coopératives Migros et Coop SA et pour des tiers, par exemple la Principauté de Liechtenstein, et 36 pour les cantons (au moins un par canton). Les raccordements cantonaux seront généralement installés dans les centrales d'alarme et

d'intervention cantonales de la police qui sont déjà protégées contre les pannes d'électricité.

Selon leurs besoins et à condition de respecter les exigences en matière de sécurité, les utilisateurs pourront connecter à leurs raccordements leurs propres réseaux, par exemple cantonaux. Plusieurs services spécialisés au sein d'un cercle d'utilisateurs pourront ainsi avoir accès au système, par exemple un canton, une entreprise ou une unité administrative. Les utilisateurs sont eux-mêmes responsables de la conception de ces composants décentralisés et de la sécurité de l'alimentation électrique des services concernés.

Selon la décision du Conseil fédéral du 20 mai 2015, l'infrastructure physique du réseau de conduite suisse doit être utilisée dans la mesure du possible pour la réalisation du réseau de données sécurisé, à savoir la fibre optique et les emplacements protégés. La circulation des données de l'armée sur le réseau de conduite suisse doit être totalement séparée physiquement du système national d'échange de données sécurisé, afin de tenir compte des exigences de l'armée et des utilisateurs du système. Pour raccorder les emplacements utilisateurs, on recourra en plus aux infrastructures de fibre optique de la Confédération (p. ex. celles posées le long des routes nationales), des cantons ou des exploitants d'infrastructures critiques. De nouvelles lignes de fibre optique seront posées là où il sera impossible de connecter les emplacement utilisateurs directement au réseau existant. Lors de la planification, on prendra notamment en compte les infrastructures réseau répondant déjà aux exigences de sécurité en cas de panne d'électricité, à savoir celles qui disposent de groupes électrogènes de secours. Dans les autres cas, on vérifiera, et on améliorera le cas échéant, la sécurité d'alimentation électrique de réseaux tiers. La réalisation du système sur un réseau commercial entraînerait des coûts très élevés, car tous les nœuds intégrés dans le réseau et une partie des lignes en fibre optique devraient être renforcés et il faudrait procéder à d'importants travaux d'épissure (assemblage de câbles). Il est possible d'utiliser des synergies et de mettre en place un réseau à un coût relativement modeste et conforme aux exigences en matière de sécurité contre les pannes d'électricité en utilisant les infrastructures physiques du réseau de conduite suisse, lequel bénéficie d'ores et déjà d'une grande robustesse et d'une large autonomie énergétique, et en se connectant à d'autres réseaux à fibres optiques appartenant aux pouvoirs publics.

2.2.2 Le système d'accès aux données

Le système d'accès aux données est un réseau d'utilisateurs fermé (couche 3). On entend par là un réseau logique isolé dépourvu de connexion avec Internet ou d'autres réseaux. Ce système garantira aux utilisateurs un accès sûr en toute situation aux systèmes d'alarme et de télécommunication exploités pour la protection de la population. L'utilisation des applications se fait à l'aide de terminaux dédiés. Étant donné qu'il s'agit d'un réseau fermé, aucune coordination avec d'autres réseaux n'est requise. Toutes les applications nécessaires à la protection de la population, existantes et futures, pourront être utilisées en toute sécurité et en toute situation sur le réseau de données sécurisé, en combinaison avec le système d'accès aux données.

Les applications de ce réseau sont par exemple Polycom pour le système radio et Polyalert pour l'alarme ainsi que d'autres systèmes et applications importants pour la sécurité. La résilience par rapport aux cyberattaques est sensiblement augmentée par l'isolement vis-à-vis des autres réseaux (p. ex. Internet).

2.2.3 Le remplacement du système Vulpus et le réseau de suivi de la situation

Pour simplifier, le réseau sécurisé est constitué du matériel tandis que le système d'accès aux données correspond au système d'exploitation. Pour la communication des données, il faudra développer une application destinée à remplacer le système Vulpus, devenu obsolète. Vulpus est un système protégé servant à la transmission de messages entre les autorités civiles de la Confédération, des cantons et des tiers, utilisé par quelque 70 organes. Il est employé depuis une trentaine d'années pour échanger des informations (principalement des messages texte) entre les autorités et organisations suivantes: Ministère public de la Confédération, polices cantonales, police municipale de Zurich, Cgfr, Sécurité militaire, CENAL, SRC, différents états-majors spéciaux du Conseil fédéral, OFPP et diverses formations d'alarme. Actuellement, Vulpus est utilisé pour l'alarme, pour des opérations de recherche et pour transmettre les messages d'alerte en cas de danger naturel qui sont émis par la Confédération et impliquent les médias (stations radio). Il est employé quotidiennement par les autorités et organisations précitées. Il est actuellement exploité et entretenu par l'armée et par RUAG. Vulpus n'est pas protégé contre les pannes d'électricité et utilise le réseau de téléphonie de Swisscom. L'exploitation des raccordements de ce réseau peut être garantie jusqu'en 2025 au plus, moyennant différentes mesures. L'armée et le SRC n'ont plus besoin de Vulpus.

Les services apportés par Vulpus sont fondamentaux pour la communication des autorités. Ils doivent rester disponibles non seulement en temps normal, mais aussi en cas de catastrophe ou de situation d'urgence. En raison de son obsolescence, Vulpus doit être remplacé par un nouveau système permettant d'échanger des informations complexes sur la situation, des données et des aperçus de la situation afin de permettre une vue d'ensemble.

Non seulement le réseau de suivi de la situation peut remplacer les fonctions actuelles de Vulpus, mais il offre aussi la possibilité d'échanger des informations complexes, comme la présentation générale de la situation au moyen d'aperçus.

Les différentes organisations actives dans la maîtrise de catastrophes et de situations d'urgence utilisent déjà des systèmes électroniques de suivi de la situation (systèmes spécialisés et systèmes de conduite). C'est notamment le cas de la PES, exploitée par la CENAL (OFPP) et également utilisée principalement par le SRC, fedpol et des organes cantonaux. Si ces systèmes correspondent aux tâches et aux besoins spécifiques de chaque organisation, ils ne sont pas reliés entre eux ou le sont insuffisamment. En outre, de nombreuses organisations ne disposent pas de leur propre système électronique de suivi de la situation. Le réseau national de suivi de la situation sera réalisé sur la base du réseau de données sécurisé et du système d'accès aux données. La protection contre les pannes et les cyberattaques sera ainsi garantie et

sera même bien meilleure par rapport au système Vulpus. L'armée a besoin d'interfaces avec le réseau de suivi de la situation qui lui permettent notamment de disposer d'informations sur la situation dans le domaine civil et qui, en outre, améliorent sensiblement la collaboration entre militaires et civils, par exemple en cas d'attaque terroriste ou de catastrophe.

2.2.4 Investissements

La réalisation du système national d'échange de données sécurisé exige une étroite collaboration avec un grand nombre d'acteurs (services fédéraux, cantons, exploitants d'infrastructures critiques), fournisseurs et propriétaires de câbles à fibres optiques et d'immeubles. Le crédit d'engagement couvre aussi les investissements dans des mesures architecturales (essentiellement dans l'infrastructure du réseau et les emplacements utilisateurs de la Confédération). Ces mesures seront mises en œuvre en collaboration avec l'organe compétent de la Confédération en matière de constructions et de gestion immobilière.

Pour gérer les projets jusqu'à leur achèvement, le DDPS a donc besoin du soutien externe de différents experts. Ceux-ci appuieront l'OFPP, responsable du projet, durant la phase de développement, la coordination du projet, la planification et l'élaboration des produits (p. ex. les exigences, les plans de gestion des parties prenantes, les expertises juridiques, les contrats et les accords de niveau de service, les manuels relatifs au projet, les plans de sécurité, les états des lieux, les documents d'appels d'offres, la mise en place des structures de gouvernance pour la conduite dans la phase d'utilisation, l'exécution de tests, la réception de systèmes et les tâches de contrôle de gestion). Les coûts de gestion du projet budgétés sont relativement élevés par rapport à d'autres projets. Les raisons en sont les suivantes: d'une part, le projet compte un grand nombre de parties prenantes, qu'il s'agisse de services de la Confédération, des cantons ou de tiers; d'autre part, il vise à tirer profit d'importantes synergies avec le réseau de conduite suisse (réseau dorsal, liaisons de fibre optique, emplacements protégés, centre de contrôle du réseau [NCC], centre d'essai et de référence [PRZ], centre d'opérations et de sécurité [SOC]), ce qui réduit certes les coûts de l'infrastructure du réseau mais augmente ceux de la gestion.

La partie principale des travaux de développement comprend le développement de logiciels pour le réseau de suivi de la situation et la programmation des interfaces entre les composants centraux du système et les systèmes de présentation de la situation déjà utilisés par les cantons et les exploitants d'infrastructures critiques. La conception des nœuds et du réseau sera définie et un réseau IP sera mis en place pour le système d'accès aux données. En plus des travaux de développement technique, la phase de conception prévoit différentes analyses (système, technique, juridique, etc.) pour chacun des quatre projets. Ces analyses serviront de base à la mise au point des produits à livrer durant la phase de conception au sens de la méthode de gestion de projet Hermes et au développement de directives et de standards.

Pour réaliser le système, il faudra acquérir le matériel pour le NCC, le SOC et le PRZ. L'acquisition portera sur un logiciel configuré (système d'exploitation) pour le

système d'accès aux données et sur les licences relatives aux logiciels (p. ex. antivirus) nécessaires à l'exploitation du système d'accès aux données et du réseau de suivi de la situation. Les coûts d'acquisition sont bas par rapport aux coûts de développement en raison des synergies mises à profit avec le réseau de conduite suisse dans le domaine du matériel et des logiciels et de la possibilité d'acheter des produits disponibles sur le marché.

L'infrastructure du réseau de conduite suisse (réseau dorsal) sera complétée par une infrastructure réseau supplémentaire (composants actifs, p. ex. multiplexeurs, routeurs, commutateurs) pour le réseau de données et le système d'accès.

De nouvelles lignes de fibre optique seront posées afin d'assurer la liaison redondante entre les emplacements utilisateurs et le réseau de conduite suisse (réseau dorsal), en quelque sorte pour le « dernier kilomètre », étant donné l'impossibilité d'utiliser des lignes existantes sur ces tronçons.

Pour tous les projets, des composants de réseau (commutateurs, routeurs) seront installés aux 120 emplacements utilisateurs afin de garantir la transmission entre les composants centraux et les composants décentralisés (raccordements).

Dans la mesure où la disponibilité et la confidentialité devront être garanties pour l'infrastructure des emplacements utilisateurs de la Confédération, des investissements doivent être consentis afin de les sécuriser. L'alimentation en électricité devra en particulier être assurée à l'aide de deux lignes d'amenée indépendantes et un groupe électrogène devra garantir l'autonomie nécessaire. La Confédération financera elle-même la garantie de l'alimentation électrique à ses emplacements utilisateurs, cette tâche relevant des utilisateurs raccordés.

La gestion du réseau comprend la gestion des prestations, la gestion de la configuration et la gestion des erreurs. Pour fournir les prestations nécessaires, deux NCC redondants des points de vue technique, opérationnel et géographique seront nécessaires en tant qu'instances centrales pour la surveillance et le contrôle permanents et pour la coordination des processus et des fonctions. Il faudra déterminer dans le cadre de la phase de projet à partir de quels NCC existants cette redondance pourra être mise en place. L'identification et l'évaluation des éventuelles cyberattaques sera assurée par le SOC. Un centre de contrôle et de référence permettra de tester les modifications avant de les introduire au niveau opérationnel et de simuler l'élimination des défauts.

Du point de vue des technologies de l'information, le développement et la création du système national d'échange de données sécurisé se déroulent dans un laps de temps relativement long avec de nombreux utilisateurs. Des incertitudes planent donc sur la réalisation du projet. Selon la méthode de gestion de projet Hermes, celui-ci se trouve dans sa phase d'initialisation. L'OFPP ne dispose pas de crédits de planification permettant de réduire ces incertitudes. Les moyens nécessaires à la concrétisation durant la phase de projet, au cours de laquelle d'autres études seront menées, ne seront disponibles qu'ultérieurement, lorsqu'une décision politique aura été prise. Comme le projet n'en est pas encore à ce stade, la marge de risque est estimée à 15 % des coûts.

Le Conseil fédéral demande un crédit d'engagement de 150 millions de francs pour la période de 2020 à 2027 afin de financer les investissements visant à développer et à acquérir le système. Ce crédit est réparti comme suit:

Tableau 1

Dépenses d'investissement pour le développement et l'acquisition

	en millions de francs
Gestion du projet	29,5
Travaux de développement	17,7
Matériel informatique, logiciels, licences	14,8
Infrastructure du réseau: réseau dorsal	6,4
Infrastructure du réseau: emplacements utilisateurs	35,7
Gestion du réseau	8,3
Emplacements utilisateurs Confédération	18,0
Marge de risque (15 %)	19,6
Investissement pour le développement et l'acquisition	**150,0**

2.2.5 Échelonnement et libération

Le crédit d'engagement sera libéré en trois étapes, conformément aux recommandations faites au Conseil fédéral par le Contrôle fédéral des finances dans son rapport d'audit du 16 octobre 2015 sur le projet informatique clé de plateforme dédiée aux impôts à la consommation[5], à une exigence de la Délégation des finances de mars 2014 et à la décision du Conseil fédéral du 21 mai 2014 prise en conséquence.

La répartition en trois tranches permet de libérer uniquement les tranches pour la réalisation desquelles les conditions sont remplies. Le Conseil fédéral peut ainsi contrôler efficacement le financement du projet et libérer les moyens nécessaires à sa mise en œuvre en différentes étapes.

Le but de la première étape, de 2020 à 2021, est de réaliser les sous-projets. C'est durant cette étape que seront élaborés les produits à livrer de la phase de conception au sens de la méthode de gestion Hermes. Elle permettra notamment de confirmer la faisabilité, de préciser les coûts du système, des sous-systèmes et du personnel nécessaire et de réduire les risques. Le projet sera validé dans ce cadre («démonstration de validité»). Les conditions relatives à la sécurité des raccordements seront en outre définies. Le système Vulpus devant être désactivé à la fin de 2025 pour des

5 Le rapport peut être consulté à l'adresse suivante : www.cdf.admin.ch > Publications > Projets informatiques >Archives Projets informatiques.

raisons techniques, l'appel d'offres OMC nécessaire à son remplacement sera préparé durant la première étape afin que le marché puisse être attribué après la libération de la deuxième tranche.

Les Chambres fédérales se prononceront dans le cadre du présent arrêté sur la libération des moyens financiers correspondant à la première étape, dont les coûts se montent à 14,7 millions de francs.

La deuxième étape, de 2022 à 2024, a pour but d'effectuer un test d'exploitation, suivi de la mise en service du réseau. Le système d'accès aux données devra être développé et mis en service à cette fin. Les principaux utilisateurs de Vulpus seront raccordés au réseau en 2024 ou 2025 afin que son remplacement puisse être mis en place au début de 2026. Vulpus devrait être désactivé à la fin de 2025, à l'issue de la phase d'introduction du nouveau système et du fonctionnement en parallèle des deux systèmes prévu pendant un an pour des raisons de sécurité. Il est également nécessaire de désactiver Vulpus à la fin de 2025 parce que le système arrivera au terme de sa durée de vie. Une prolongation supplémentaire de son exploitation entraînerait des surcoûts disproportionnés. Les utilisateurs de Vulpus seront formés à l'utilisation du nouveau système en 2023 et 2024.

La demande de libération de la deuxième tranche, d'un montant de 83,6 millions de francs, sera soumise pour examen à la Conférence des secrétaires généraux, puis au Conseil fédéral, qui statuera. Les critères de libération sont les suivants:

- la phase de conception au sens de la méthode de gestion Hermes est achevée;
- la faisabilité est confirmée, les coûts du système, des sous-systèmes et du personnel nécessaire sont précisés et les risques liés à la mise en place sont évalués;
- le projet a fait l'objet d'une démonstration de validité en ce qui concerne le réseau et le système d'accès;
- les conditions de raccordement sont définies pour la Confédération, les cantons et les exploitants d'infrastructures critiques;
- l'appel d'offres OMC pour le remplacement du système Vulpus est lancé et l'attribution du marché est préparée.

Les dernières utilisatrices et les derniers utilisateurs seront raccordés durant la troisième étape, de 2025 à 2027, durant laquelle le système d'accès aux données sera développé. Des interfaces seront mises au point pour intégrer les différents systèmes de PES et les raccorder successivement au réseau de suivi de la situation. L'éventail des fonctionnalités de ce réseau sera en même temps élargi, par exemple à la présentation d'informations géographiques. Après l'achèvement du projet en 2027, d'indispensables travaux de clôture et de garantie auront encore lieu l'année suivante.

La demande de libération de la troisième tranche, d'un montant de 51,7 millions de francs, sera aussi soumise pour examen à la Conférence des secrétaires généraux, puis au Conseil fédéral, qui statuera. Les critères de libération sont les suivants:

- le réseau de données est opérationnel et les processus d'exploitation sont consolidés;

- l'infrastructure des emplacements d'origine des principaux utilisateurs du système Vulpus est sécurisée et raccordée au réseau;
- le remplacement du système Vulpus est mis en place;
- un premier ensemble de fonctionnalités du réseau de suivi de la situation est mis en œuvre et fait l'objet de tests.

Tableau 2

Répartition du crédit d'engagement entre les trois étapes (en millions de francs)

	Étape 1	Étape 2	Étape 3
Total	14,7	83,6	51,7

2.2.6 Exploitation et maintenance

Pour maintenir la disponibilité et la sécurité du système pendant toute sa durée de vie, il est nécessaire de l'entretenir et de l'adapter continuellement aux nouvelles normes. Ces travaux incluent la réparation et le remplacement de composants matériels (p. ex. à la suite de dommages dus à des éléments naturels ou de défauts techniques), des mises à jour de sécurité et des installations de nouvelles versions de logiciel. Les prestations correspondantes telles qu'inspections, maintenance, réparations, développements et mises à jour sont garanties en permanence dans toute la Suisse par des prestataires de services externes ou des organisations intervenant sur site. Les spécialistes travaillent selon les standards du secteur informatique et les exigences spécifiques au système.

Il est prévu de consacrer 15 % des dépenses annuelles d'exploitation et d'entretien aux réparations, à la maintenance, au remplacement de composants, aux nouvelles versions de logiciel, aux mises à jour, aux coûts de location, etc. durant le cycle de vie de chaque système. Quant aux coûts d'exploitation et de maintenance des différents éléments du réseau aux emplacements utilisateurs, ils sont estimés à 5 % de leur prix de base. Pour garantir une exploitation 24 heures sur 24, un service spécial sera mis en place. Il assumera différents rôles impliquant la conclusion de contrats de maintenance et d'assistance avec les fournisseurs de prestations ou de produits. La connexion des cantons et des tiers via la fibre optique nécessitera également des contrats étendus de gestion de réseau, de maintenance et d'assistance avec des fournisseurs de prestations ou de produits et une excellente coordination.

Conformément à la répartition des compétences et du financement, chaque utilisateur doit assumer lui-même les coûts d'exploitation des composants décentralisés. Pour la période de 2023 à 2027, un montant total de 13,5 millions de francs a été budgété afin d'assurer la maintenance des emplacements utilisateurs de la Confédération. Les moyens prévus permettront de couvrir les coûts de maintenance et d'exploitation spécifiques aux raccordements, par exemple l'entretien des interfaces entre les composants décentralisés et les composants centraux. À l'heure actuelle, on table sur 40 raccordements fédéraux. Les cantons (36 raccordements), les exploitants

d'infrastructures critiques (43) et la Principauté de Liechtenstein devront prendre à leur charge les coûts spécifiques à leurs emplacements utilisateurs.

L'exploitation et l'entretien du système d'échange de données sécurisé augmenteront les dépenses de fonctionnement de l'OFPP de 100 000 francs en 2020, 600 000 francs en 2021, 1,5 million de en 2022, 7 millions de francs en 2023, 10 millions de francs en 2024, de 12 millions de francs en 2025, 13,9 millions de francs en 2026 et 15 millions de francs par an à partir de 2027 (cf. tableau 4), charges de personnel non comprises. Le coût des postes de travail se montera au total à 1,7 million de francs de 2020 à 2028 (cf. tableau 4).

2.2.7 Réglementation des compétences et financement

Le système national d'échange de données sécurisé est un système coordonné reliant la Confédération, les cantons, les exploitants d'infrastructures critiques et les tiers. Dans les systèmes coordonnés, on distingue les composants centraux des composants décentralisés. Les composants centraux relient les utilisateurs et sont partagés entre eux. Les composants décentralisés permettent d'utiliser les composants centraux et sont utilisés par les organes fédéraux (p. ex. l'AFD), les cantons et les tiers qui les possèdent.

Pour définir les compétences et la répartition des coûts, le chef du DDPS et les présidents de la CCDJP et de la CG MPS ont institué, le 10 janvier 2017, un groupe de travail composé de représentants de la Confédération et des cantons. Les travaux de ce groupe ont permis de dégager un consensus et de convenir d'un principe de financement: les cantons commandent auprès de la Confédération 36 raccordements et s'entendent entre eux sur la répartition de ces raccordements ainsi que sur la répartition des coûts annuels d'exploitation et d'entretien. Les règles ci-après ont été définies.

La Confédération est responsable des composants centraux des systèmes coordonnés. Les composants décentralisés sont en revanche de la responsabilité de leur détenteur, à savoir la Confédération (organes fédéraux), les cantons, les exploitants d'infrastructures critiques et les tiers.

On entend par «investissement» toutes les dépenses nécessaires à la mise en place d'un nouveau système. Dans le cadre du système national d'échange de données sécurisé, par exemple, il s'agit notamment des investissements dans les bâtiments, les câbles, le matériel informatique, les logiciels, les génératrices de secours, les installations de climatisation (cf. tableau 4). Les composants centraux sont financés par la Confédération (dépense unique). Dans le cas du système d'échange de données, les investissements portent sur le réseau de base (réseau dorsal) jusqu'à l'interface avec un emplacement utilisateur (raccordement), le système d'accès aux données et le remplacement du système Vulpus (réseau de suivi de la situation). Les investissements dans les composants décentralisés sont financés par les cantons, les exploitants d'infrastructures critiques et les tiers. La sécurité électrique des emplacements utilisateurs raccordés en fait partie. Dans la mesure où les raccordements concernent des composants décentralisés d'organes fédéraux, les investissements

sont cependant à la charge de la Confédération. Le financement des dépenses qui y sont liées est compris dans la présente demande de crédit.

L'expérience nous montre qu'une fois arrivés au terme d'un cycle de vie, les éléments d'un système nécessitent des mesures de maintien de la valeur donnant lieu à des investissements. On entend ainsi par maintien de la valeur d'importants réinvestissements qui peuvent être indispensables six à huit ans après le premier investissement. Ces coûts représentent environ 60 % de ce premier investissement et sont assumés par la Confédération pour ce qui est des composants centraux. Les cantons et les tiers supportent pour leur part les coûts du maintien de la valeur des composants décentralisés. Lorsqu'ils disposent de composants décentralisés, les organes fédéraux doivent eux aussi assumer de tels réinvestissements.

On entend par coûts annuels d'exploitation et de maintenance les dépenses nécessaires au fonctionnement ininterrompu et sécurisé des systèmes, à savoir notamment la maintenance des systèmes, leur surveillance, la gestion des services et des urgences, la mise à jour des logiciels et les correctifs de sécurité. L'amortissement n'est pas inclus. On estime que les mesures de maintien de la valeur mises en œuvre durant le cycle de vie des systèmes représenteront 15 % des coûts annuels d'exploitation et de maintenance. Les coûts annuels d'exploitation et maintenance des composants centraux du système national d'échange de données sécurisé sont pris en charge par tous les utilisateurs connectés proportionnellement au nombre de leurs raccordements. L'exploitation et la maintenance des composants décentralisés sont financés par les cantons, les exploitants d'infrastructures critiques et les tiers ainsi que par la Confédération pour les organes fédéraux raccordés.

Les coûts annuels d'exploitation et de maintenance des composants centraux du réseau de données sécurisé, du systèmes d'accès aux données et du réseau de suivi de la situation destiné à remplacer le système Vulpus seront assurés à raison de 30 % par les cantons, d'environ 40 % par la Confédération et d'environ 30 % par les exploitants d'infrastructures critiques. Les cantons auront ainsi le droit de réaliser au maximum 36 raccordements à ce système. La Confédération, les exploitants d'infrastructures critiques et des tiers pourront de leur côté réaliser quelque 80 à 90 raccordements. Le financement est proportionnel au nombre de raccordements. En cas de raccordements supplémentaires par rapport aux 120 prévus, la clé de répartition des coûts sera adaptée en conséquence.

Tableau 3

Investissement, maintien de la valeur, exploitation et entretien

	Investissement	Maintien de la valeur (réinvestissement)	Exploitation et entretien
Objet	Bâtiments, installations de climatisation, génératrices de secours, matériel, logiciels, licences, etc.	Remplacement ordinaire, matériel (p. ex. routeurs), logiciels, etc.	Maintenance, mises à jours de logiciels pièces de rechange, frais de location, etc.
Fréquence	unique[6]	env. tous les 6 à 8 ans	annuelle
Financement	Composants centraux: Confédération	Composants centraux: Confédération	Composants centraux: utilisateurs
	Composants décentralisés: organes fédéraux, cantons et tiers	Composants décentralisés: organes fédéraux, cantons et tiers	(Conf. et tiers[7]/cantons: 70/30)
			Composants décentralisés: organes fédéraux, cantons et tiers

3 Conséquences

3.1 Conséquences pour la Confédération

3.1.1 Conséquences financières

Les dépenses d'investissement de la Confédération pour le développement et l'acquisition du système national d'échange de données sécurisé s'élèvent à 150 millions de francs. Les décisions que le Conseil fédéral prendra lors de l'établissement des budgets avec plan intégré des tâches et des finances sont réservées.

Le montant du crédit d'engagement se fonde sur l'indice suisse des prix à la consommation en décembre 2017 (100,8 points; décembre 2015: 100 points). Le taux de renchérissement à partir de 2020 est estimé à 1 %.

Le crédit d'engagement sera libéré en trois étapes: la première dans le cadre de l'arrêté fédéral qui fait l'objet du présent message et les suivantes sur décision du Conseil fédéral en fonction de l'avancement du projet.

Pour l'exploitation et l'entretien, il faut s'attendre à des dépenses supplémentaires d'un montant de 100 000 francs en 2020 et de 600 000 francs en 2021. Il faudra en effet déjà faire face à des frais d'exploitation dans la phase de planification, dans le cadre de la démonstration de validité du projet et pour la préparation des tests de fonctionnement des années suivantes. Ces dépenses connaîtront une hausse continue de 2022 à 2027. À partir de 2027, elles se monteront à 15 millions de francs par an

6 Cycles très longs (décennies), p. ex. pour la modernisation de bâtiments.
7 Confédération avec exploitants d'infrastructures critiques et tiers.

pour l'exploitation normale (sans les prestations propres). Les dépenses d'exploitation sont représentées dans le tableau 4.

Les prestations fournies par l'administration elle-même, qui se traduiront par des charges de personnel, se chiffreront à 4,3 millions de francs par an en moyenne à partir de 2020 et à 4,1 millions de francs pour l'exploitation normale à partir de 2028.

Par conséquent, les dépenses à la charge de la Confédération s'élèveront à un montant brut de 241,5 millions de francs de 2020 jusqu'à la fin du projet en 2027. Le DDPS (OFPP) ne pourra pas financer entièrement les investissements et l'exploitation avec les moyens à sa disposition.

La mise hors service du système de transmission de messages Vulpus permettra d'économiser chaque année 1,5 million de francs au titre des dépenses d'exploitation à partir de 2026. Un fonctionnement en parallèle sera assuré au moment du changement de système (2025).

Dès la mise en service complète du réseau de base en 2026, les cantons participeront aux coûts d'exploitation et d'entretien du système national d'échange de données sécurisé à raison d'une contribution annuelle de 4,5 millions de francs (36 raccordements). Ce montant équivaut à des frais annuels moyens d'environ 125 000 francs par utilisateur et englobe les charges résultant des prestations fournies par la Confédération ainsi que les dépenses pour l'exploitation et l'entretien. Il n'inclut pas les coûts de raccordement à la charge des utilisateurs eux-mêmes. Les contributions des exploitants d'infrastructures critiques et de tiers souhaitant utiliser le système reviendront également à la Confédération. À supposer qu'il y ait 120 raccordements au total (36 pour les cantons, 1 pour la Principauté de Liechtenstein, 40 pour les organes fédéraux et 43 pour les exploitants d'infrastructures critiques), la Confédération touchera des contributions annuelles de 10 millions de francs, sans tenir compte de la marge de risque.

Tableau 4

Dépenses totales pour le système national d'échange de données sécurisé entre 2020 et 2027

en millions de francs	2020	2021	2022	2023	2024	2025	2026	2027	Total
Dépenses totales	9,2	11,7	28,9	38,0	48,1	41,9	33,6	30,1	241,5
Investissements	6,8	7,9	23,8	26,9	32,9	24,7	15,8	11,2	150,0
Gestion de projet	3,1	3,4	4,8	4,8	4,5	3,7	3,4	1,8	29,5
Travaux de développement	1,5	1,0	4,4	3,0	4,0	2,8	0,5	0,5	17,7
Matériel, logiciels, licences	0,8	1,0	1,0	2,0	2,5	2,5	2,5	2,5	14,8
Infr, réseau: réseau dorsal	0,0	0,0	1,5	2,8	1,6	0,5	0,0	0,0	6,4
Infr, réseau: emplacements utilisateurs	0,0	0,0	4,0	6,8	8,0	8,0	5,5	3,4	35,7
Gestion du réseau	0,0	1,0	2,0	1,0	1,0	2,0	0,8	0,5	8,3
Emplacements utilisateurs Confédération	0,5	0,5	3,0	3,0	7,0	2,0	1,0	1,0	18,0
Marge de risque (15%)	0,9	1,0	3,1	3,5	4,3	3,2	2,1	1,5	19,6
Dépenses d'exploitation et d'entretien	0,1	0,6	1,5	7,0	10,0	12,0	13,9	15,0	60,1
Exploitation et maintenance	0,0	0,4	1,0	5,8	8,3	9,3	9,6	10,7	45,1
Coûts liés aux postes de travail	0,1	0,2	0,2	0,2	0,2	0,2	0,2	0,2	1,7
Emplacement utilisateurs Confédération	0,0	0,0	0,3	1,0	1,5	2,5	4,1	4,1	13,5
Prestations propres	2,3	3,2	3,6	4,1	5,2	5,2	5,4	5,4	34,4
Personnel (15 EPT existants)	0,9	0,9	0,9	1,4	2,5	2,5	2,7	2,7	14,5
Personnel (15 EPT supplémentaires)	1,4	2,3	2,7	2,7	2,7	2,7	2,7	2,7	19,9
Mise hors service de Vulpus	0,0	0,0	0,0	0,0	0,0	0,0	-1,5	-1,5	-3,0

3.1.2 Conséquences sur l'état du personnel

Pour que le projet puisse être réalisé dans les délais impartis en respectant les prescriptions financières et qualitatives et pour assurer à l'échelle nationale le fonctionnement en continu du système national d'échange de données sécurisé avec la collaboration des fournisseurs de prestations (BAC et prestataires externes), il faudra probablement 25 postes supplémentaires pour la dernière phase (à partir de 2028). Une partie de ces postes est nécessaire pour assurer l'exploitation du système en situation particulière ou extraordinaire. La mise en œuvre et l'exploitation du système national d'échange de données sécurisé, qui se chevaucheront en grande partie entre 2024 et 2027, occasionneront des charges de personnel correspondant à 30 emplois à plein temps pour le DDPS (OFPP, BAC) durant cette période. Le DDPS procédera à une compensation à l'interne pour 15 postes à durée indéterminée. Les 15 autres EPT supplémentaires nécessaires pendant la phase de projet, dont 10 à durée indéterminée pour l'exploitation normale à partir de 2028, requerront une augmentation de personnel, faute de quoi l'OFPP et la BAC ne pourront pas faire face à ce surcroît de travail.

Comme il s'agit d'un projet national particulièrement complexe touchant à la sécurité, il est nécessaire d'acquérir une indépendance maximale, de garantir le maintien du savoir-faire dans les compétences clés à l'interne et de suivre l'évolution technologique. À cet effet, il est certes prévu de confier à des prestataires externes certaines tâches et expertises spécifiques, d'une durée et d'une portée limitées. Les recommandations qui figurent dans le rapport du 24 juin 2015 des Commissions des finances et des Commissions de gestion des Chambres fédérales relatif à l'avis du Conseil fédéral du 25 février 2015 et à l'avis du Contrôle fédéral des finances du 24 février 2015 sur le projet informatique Insieme[8] prévoient cependant de conserver à l'interne de la Confédération les rôles clés et le savoir-faire correspondant. Le Conseil fédéral entend se conformer à ces recommandations dans la mesure où les ressources disponibles le permettent. L'augmentation des effectifs permettra de prendre en charge la responsabilité des applications à l'interne, d'assurer la gestion des acteurs et de mettre en place les compétences requises pour l'exploitation, le maintien de la valeur et le développement.

L'OFPP aura besoin au surplus de 10 équivalents plein temps pour la mise en place, l'optimisation et le maintien de la valeur du système (réseau de données, système d'accès aux données, réseau de suivi de la situation), la gestion des bénéficiaires de prestations (organes fédéraux, cantons, exploitants d'infrastructures critiques) et les prestations de la phase d'exploitation. Durant cette dernière phase, il en emploiera 6 pour le réseau de données sécurisé et le système d'accès et 4 pour le réseau de suivi de la situation. Ces postes seront transférés à partir de la réserve de personnel mise en place durant la phase de projet et affectés à l'exploitation normale à partir de 2028. Quant à la BAC, il lui faudra 5 équivalents plein temps supplémentaires pour assurer en toute situation et 24 heures sur 24 le fonctionnement du système d'échange de données sécurisé. Ces postes seront compensés à l'interne au DDPS en vue de l'exploitation normale à partir de 2028.

8 FF **2016** 4057

L'OFPP n'aura pas besoin de locaux supplémentaires. Les besoins pour les nouveaux postes de travail pourront être couverts par l'utilisation de postes dédiés à des projets et par des synergies dans le cadre de la réorganisation de l'OFPP et du déménagement de la CENAL de Zurich à Berne. La BAC n'a, elle non plus, pas besoin de locaux supplémentaires.

La coordination générale et la responsabilité du projet pour le système national d'échange de données sécurisé seront assumées par l'OFPP.

Le DDPS assumera des tâches complexes et des responsabilités supplémentaires dans différents domaines. La réalisation du système et son exploitation devront être coordonnés avec les fournisseurs de prestation, par exemple les propriétaires de lignes à fibres optiques et d'infrastructures, et les bénéficiaires de prestations. À cet effet, des contrats devront être négociés et conclus. Les produits fournis devront être testés et approuvés. Enfin, la gestion de l'exploitation et la maintenance ainsi que la gestion de la sécurité et de la qualité devront être garanties.

Un chef de projet sera désigné pour la direction générale du projet et la coordination des sous-projets.

La gestion de chacun des quatre sous-projets sera confiée à un chef de sous-projet. Les chefs de sous-projets aideront les utilisateurs de la Confédération et des cantons ainsi que les exploitants d'infrastructures critiques dans les travaux de planification de projet, de mise en œuvre sur place et d'exploitation. Ils seront aussi responsables de la gestion des interfaces entre le système national d'échange de données sécurisé et les réseaux des utilisateurs.

Les responsables de la gestion de mandats seront les interlocuteurs des utilisateurs. Ils réceptionneront les mandats et se chargeront de leur exécution.

Les responsables de produits surveilleront l'évolution du marché et émettront des pronostics pour la création et le développement du système national d'échange de données sécurisé. Durant toute la durée du projet, ils recenseront les besoins des organes fédéraux, des cantons et des exploitants d'infrastructures critiques.

Les responsables d'exploitation se chargeront, en accord avec les autorités, les organes fédéraux et cantonaux ainsi que les exploitants d'infrastructures critiques, de la coordination de l'exploitation, des tests et de la réception des produits et prestations. Ils seront responsables de la gestion des modifications, des nouvelles versions et de la configuration et introduiront les nouvelles versions de logiciels et le nouveau matériel. Ils coordonneront l'exploitation du réseau avec toutes les applications des utilisateurs de la Confédération, des cantons et des exploitants d'infrastructures critiques.

Les responsables de la gestion de services concluront des conventions de prestations avec les fournisseurs (BAC, industrie) et vérifieront leur exécution.

Les responsables de l'exploitation du réseau géreront et surveilleront le réseau de données sécurisé et le système d'accès aux données. Ils se chargeront de la gestion des erreurs, de la configuration, des prestations et de la sécurité.

Les responsables du service assurance garantiront la fourniture de prestations aux utilisatrices et utilisateurs. Ils assureront et coordonneront la gestion des événements

et des problèmes avec les fournisseurs de prestations et seront responsables de la communication avec les utilisatrices et utilisateurs.

Les responsables de la gestion de la sécurité et de la qualité élaboreront des directives en matière de sécurité. Ils appliqueront les prescriptions des stratégies nationales du 27 juin 2012 et du 18 avril 2018 de protection de la Suisse contre les cyberrisques[9] et garantiront la qualité. Durant toute l'exploitation, ils définiront des mesures d'amélioration et vérifieront leur mise en œuvre.

Les responsables de la gestion de contrats mèneront les négociations et concluront des contrats avec les fournisseurs de prestations (BAC, industrie) et tous les utilisateurs de la Confédération, des cantons et des exploitants d'infrastructures critiques. Ils seront en outre responsables des procédures contractuelles et du respect des contrats.

Le responsable du contrôle de gestion accompagnera le projet durant toute sa durée. Il sera responsable des rapports et accomplira des tâches transversales. Il veillera à coordonner les secteurs financiers, commerciaux et juridiques.

Le suivi des événements et des menaces dans le cyberespace sera assuré par le prestataire du DDPS, à savoir la BAC, pour toute l'infrastructure d'informatique et de télécommunication concernée.

Pendant la phase d'exploitation, la gestion des bénéficiaires de prestations (Confédération, cantons et exploitants d'infrastructures critiques) sera assurée par les titulaires de différentes fonctions qui sont nécessaires durant la phase de projet (cf. tableau 6).

9 Les stratégies peuvent être consultées à l'adresse suivante : www.upic.admin.ch > Thèmes > Cyberrisques SNPC > Stratégie SNPC 2012-2017 et Stratégie SNPC 2018-2022.

Tableau 6

Besoins en personnel et fonctions par année jusqu'à la fin du projet ainsi que pour l'exploitation normale

Postes pour les projets	Projet	2020	2021	2022	2023	2024	2025	2026	2027	2028
Chef de projet	SEDS & SAD (OFPP)	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
	SEDS & SAD (BAC) Réseau de suivi de la situation /Vulpus (OFPP)	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
Chef de sous-projet	SEDS & SAD (OFPP)	3,0	3,0	3,0	2,0	2,0	2,0	1,5	1,5	
	SEDS & SAD (BAC)	1,0	2,0	2,0	2,0	2,0	2,0	1,0	1,0	
	Réseau de suivi de la situation /Vulpus (OFPP)	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
Responsable de la gestion des mandats	SEDS & SAD (OFPP)	1,0	1,25	1,5	1,5	1,25				
	SEDS & SAD (BAC) Réseau de suivi de la situation /Vulpus (OFPP)	1,0	1,0	0,75	0,75					
Responsable de produit	SEDS & SAD (OFPP)	1,0	1,0	1,25	1,5	1,0	1,0	1,0	1,0	
	SEDS & SAD (BAC) Réseau de suivi de la situation /Vulpus (OFPP)	1,0	1,0	1,5	1,5					
Responsable d'exploitation	SEDS & SAD (OFPP)	0,5	0,5	0,5						
	SEDS & SAD (BAC) Réseau de suivi de la situation /Vulpus (OFPP)		0,5	0,5						
Responsable de la gestion des services	SEDS & SAD (OFPP)									
	SEDS & SAD (BAC)		0,5	0,5						
	Réseau de suivi de la situation /Vulpus (OFPP)			1,0	1,0					
Responsable de l'exploitation du réseau	SEDS & SAD (OFPP)									
	SEDS & SAD (BAC) Réseau de suivi de la situation /Vulpus (OFPP)		0,5							
Responsable de la sécurité et de la qualité	SEDS & SAD (OFPP)	1,0	1,0	1,0	0,75	0,75	0,75	0,75	0,75	
	SEDS & SAD (BAC)		1,0	1,0	1,0					
	Réseau de suivi de la situation /Vulpus (OFPP)		0,5	0,25						
Responsable de la gestion des contrats	Tous les projets	0,25	1,00	1,25	1,00	0,75	0,25	0,25	0,25	
Responsable du contrôle de gestion	Tous les projets	0,25	0,25	0,50	0,75	0,75	0,75	1,00	1,00	
Total des postes pour les projets		13	18	19,5	16,75	11,5	9,75	8,5	8,5	0,0

Suite du tableau 6

Postes pour l'exploitation	Exploitation	2020	2021	2022	2023	2024	2025	2026	2027	2028
	SEDS & SAD (OFPP)									1,0
Chef de sous-projet	SEDS & SAD (BAC)									1,0
	Réseau de suivi de la situation /Vulpus (OFPP)									
	SEDS & SAD (OFPP)						1,0	1,0	1,0	1,0
Responsable de la gestion des mandats	SEDS & SAD (BAC)									
	Réseau de suivi de la situation /Vulpus (OFPP)					0,5	0,5	0,5	0,5	
	SEDS & SAD (OFPP)					1,0	1,0	1,0	1,0	1,0
Responsable de produit	SEDS & SAD (BAC)									1,0
	Réseau de suivi de la situation /Vulpus (OFPP)					1,25	1,25	1,25	1,25	0,75
	SEDS & SAD (OFPP)				1,0	1,0	1,75	2,0	2,0	1,5
Responsable d'exploitation	SEDS & SAD (BAC)									
	Réseau de suivi de la situation /Vulpus (OFPP)				0,5	1,0	1,0	1,0	1,0	1,0
	SEDS & SAD (OFPP)									1,0
Responsable de la gestion des services	SEDS & SAD (BAC)				1,5	2,0	2,0	2,0	2,0	2,0
	Réseau de suivi de la situation /Vulpus (OFPP)					1,0	1,0	1,0	1,0	1,0
Responsable de l'assurance des services	SEDS & SAD (OFPP)									
	SEDS & SAD (BAC)					1,0	1,0	2,0	2,0	2,0
	Réseau de suivi de la situation /Vulpus (OFPP)									
Responsable de l'exploitation du réseau	SEDS & SAD (OFPP)									
	SEDS & SAD (BAC)			0.5	2,5	8,0	8,0	9,0	9,0	9,0
	Réseau de suivi de la situation /Vulpus (OFPP)									
Responsable de la sécurité et de la qualité	SEDS & SAD (OFPP)				0,5	0,5	0,5	0,5	0,5	0,5
	SEDS & SAD (BAC)									
	Réseau de suivi de la situation /Vulpus (OFPP)				0,25	0,25	0,25	0,25	0,25	0,25
Responsable de la gestion des contrats	Tous les systèmes									0,25
Responsable du contrôle de gestion	Tous les systèmes									0,75
Total des postes pour l'exploitation		0,0	0,0	0,5	6,25	17,5	19,25	21,5	21,5	25,0
Total des postes par année (projet + exploitation)		**13**	**18**	**20**	**23**	**29**	**29**	**30**	**30**	**25**

3.2 Conséquences pour les cantons

La Confédération prendra à sa charge les coûts d'investissement pour les composants centraux du futur système. Les coûts d'investissement relatifs aux composants décentralisés dans les cantons, par exemple pour consolider leurs emplacements utilisateurs, devront être assumés par les cantons eux-mêmes. Les cantons veilleront au raccordement de leurs autorités, communes, villes, etc. au système par l'intermédiaire de leurs propres réseaux. Les composants décentralisés des cantons seront reliés progressivement aux composants centraux. Les coûts d'investissement de même que les coûts d'exploitation et de maintenance annuels pour les composants décentralisés des cantons dépendront des infrastructures en place et des besoins individuels de ces derniers. Des informations détaillées sur les coûts figurent au ch. 3.1.1.

3.3 Conséquences économiques

La réalisation du système national d'échange de données sécurisé profitera également dans une mesure considérable à l'économie. Une absence des prestations d'informatique et de télécommunication à grande échelle menacerait en effet le fonctionnement de l'économie tout entière. Aujourd'hui, de nombreuses entreprises, notamment les exploitants d'infrastructures critiques, disposent d'une alimentation électrique de secours pour remédier à une éventuelle panne de courant. S'il garantit une exploitation autonome pendant une certaine durée, un tel dispositif n'assure toutefois pas la communication avec les organisations partenaires, autorités, etc. Fortement croissant ces dernières années, l'échange électronique de données entre les organisations et les entreprises gagnera encore en ampleur avec la numérisation en cours. Grâce au futur système national d'échange de données sécurisé, toutes les autorités et entreprises exploitant des infrastructures critiques qui veulent ou doivent assurer l'interopérabilité de leurs systèmes en cas de défaillance du réseau d'électricité bénéficieront d'une plate-forme commune. Le réseau pourra aussi être utilisé en situation normale et il est prévu qu'il le soit. La réalisation du système d'échange de données sécurisé permet en outre d'éviter la création de solutions isolées. Pour toutes ces raisons, une plus-value importante pourra être obtenue pour l'économie.

3.4 Conséquences sociales

La réalisation du système national d'échange de données sécurisé n'améliorera pas seulement la fiabilité des systèmes de télécommunication et l'échange de données entre les organes de conduite et d'intervention et les autorités: la population profitera elle aussi à terme d'un niveau de sécurité accru. L'ampleur des dommages aux personnes, aux animaux et aux biens pourrait être sensiblement réduite en cas de catastrophe ou de situation d'urgence. Il sera ainsi possible de combler une importante lacune en matière de sécurité au sein de la protection de la population.

3.5 Conséquences environnementales

Hormis l'impact de la logistique de transport, le projet n'aura aucune incidence notable sur l'environnement. Reposant sur un réseau de fibres optiques, il ne nécessite pas de nouveaux emplacements d'antennes et ne conduit donc pas à une augmentation des émissions de rayonnement non ionisant.

4 Relation avec le programme de la législature et les stratégies du Conseil fédéral

4.1 Relation avec le programme de la législature

Le projet s'inscrit dans le ch. 5.3.5 du message du 27 janvier 2016 sur le programme de la législature 2015 à 2019[10]. Selon la stratégie du Conseil fédéral, en effet, les instruments de la politique de sécurité doivent permettre de réagir en tout temps aux événements. Une telle capacité nécessite une coopération optimale entre tous les partenaires et une collaboration efficace entre tous les acteurs de la politique de sécurité. L'échange d'informations et le suivi de la situation sécurisés entre toutes les parties dans le cadre du futur système national d'échange de données sécurisé en sont les principaux instruments.

L'objectif 16 défini dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[11] est formulé comme suit: «La Suisse connaît les menaces intérieures et extérieures qui pèsent sur sa sécurité et dispose des instruments nécessaires pour y parer efficacement». L'adoption du message concernant la révision totale de la LPPCi y est mentionnée parmi les mesures permettant d'atteindre cet objectif (mesure nº 65). Ce message contient notamment les bases juridiques nécessaires à la réalisation du système national d'échange de données sécurisé et au réseau national de suivi de la situation.

4.2 Relation avec les objectifs 2018 du Conseil fédéral

Compte tenu du caractère urgent du projet, le Conseil fédéral a inscrit l'élaboration d'un message dans les objectifs du Conseil fédéral 2018 (parties I et II)[12]. Le 1er décembre 2017, il a chargé l'OFPP d'élaborer ce message en 2018.

10 FF **2016** 981
11 FF **2016** 4999
12 Les objectifs du Conseil fédéral peuvent être consultés à l'adresse suivante : www.chf.admin.ch > Documentation > Aide à la conduite stratégique > Les Objectifs.

4.3 Relation avec les stratégies du Conseil fédéral

En raison des changements climatiques, la fréquence et l'intensité des dangers naturels en particulier devraient augmenter[13], ce qui nécessitera des mesures d'adaptation[14]. La protection des infrastructures d'information et de communication contre les cyberrisques, dont l'ampleur aura tendance à augmenter, relève de l'intérêt national[15]. Disposer de systèmes de télécommunications sécurisés, c'est-à-dire résistant aux pannes, figure dès lors parmi les objectifs de la stratégie de la protection de la population et de la protection civile 2015+[16], approuvée par le Conseil fédéral le 9 mai 2012. Conformément à la stratégie «Suisse numérique» du 20 avril 2016[17], l'État doit être en mesure, à l'ère numérique, de protéger efficacement la société et l'économie. Le système national d'échange de données sécurisé apporte à cet égard une contribution importante au renforcement de la résilience des systèmes de télécommunication et des infrastructures critiques. Cette amélioration de la résilience est un objectif de la stratégie nationale pour la protection des infrastructures critiques 2018–2022[18] et de la stratégie nationale de protection de la Suisse contre les cyberrisques. Par conséquent, un réseau de transmission de données et de communication hautement sécurisé auquel les exploitants d'infrastructures critiques peuvent être raccordés figure parmi les objectifs et les mesures explicites tels qu'ils ont été définis dans la stratégie nationale pour la protection des infrastructures critiques 2018–2022, adoptée par le Conseil fédéral le 8 décembre 2017. Le système national d'échange de données sécurisé permettra aux exploitants d'infrastructures critiques, en cas de panne du réseau public de télécommunications, de maintenir les processus nécessaires au fonctionnement de leurs infrastructures et de garantir la communication avec les organisations de gestion des crises aux échelons fédéral et cantonal. Le rapport sur les dangers naturels en Suisse[19] et la stratégie sur les dangers naturels[20] proposent aussi de créer un réseau de données et de communication protégé contre les défaillances et les pannes ainsi qu'un réseau réunissant les différents systèmes de suivi pour améliorer la résilience face aux dangers naturels.

13 Köllner P., Gross C., Schäppi B., Füssler J., Lerch J., Nauser M. 2017: *Risques et opportunités liés au climat. Une synthèse à l'échelle de la Suisse*. Office fédéral de l'environnement, Berne. Connaissance de l'environnement n° 1706: 148 S.

14 Stratégie du Conseil fédéral de l'adaptation aux changements climatiques en Suisse 2014–2019. La stratégie peut être consultée à l'adresse suivante : www.ofev.admin.ch > Thèmes > Climat > Informations pour spécialistes > Adaptation aux changements climatiques > Stratégie du Conseil fédéral.

15 Voir note 9.

16 FF **2012** 5075

17 FF **2016** 3801

18 La stratégie peut être consultée à l'adresse suivante : www.ofpp.admin.ch > Autres domaines d'activités > Protection des infrastructures critiques > Stratégie nationale PIC.

19 Le rapport peut être consulté à l'adresse suivante : www.ofev.admin.ch > Thèmes > Dangers naturels > Dossiers > Dangers naturels en Suisse – que faire pour la sécurité ? > Rapport du Conseil fédéral « Gestion des dangers naturels en Suisse ».

20 La stratégie peut être consultée à l'adresse suivante : www.planat.ch > Stratégie 2018.

L'axe «S03 – Fourniture des prestations informatiques» de la stratégie informatique de la Confédération pour les années 2016 à 2019[21], adoptée le 4 décembre 2015, prévoit l'élaboration d'une stratégie sur les réseaux. Le Conseil fédéral l'a adoptée en même temps que le présent message. Cette stratégie montre les exigences auxquelles doivent répondre les réseaux de la Confédération et définit les réseaux nationaux qui permettront de respecter ces exigences. Le système national d'échange de données sécurisé fait partie de cette stratégie et est coordonné avec elle. Les détails seront réglés dans le cadre des travaux ultérieurs du projet. Les axes principaux de la stratégie sont présentés ci-après.

La Confédération encourage le doublement des infrastructures pour les réseaux de transport optique de données desservant des zones étendues. La première infrastructure est constituée par le réseau de conduite suisse, qui fournit des prestations robustes et sûres à l'armée. La deuxième infrastructure repose sur le réseau optique des autorités fédérales. Celui-ci vise à mettre des liaisons optiques de transport de données résilientes sur le plan de l'alimentation électrique et de haute sécurité à la disposition des services de la Confédération, des cantons, des exploitants d'infrastructures critiques et de tiers autorisés qui en ont besoin pour collaborer. Il sera mis en place lors d'une première phase dans le cadre de trois projets: le système national d'échange de données sécurisé, l'interconnexion des équipements d'exploitation et de sécurité des routes nationales et celle des centres de calcul civils.

Ces réseaux de transport de données utilisent dans la mesure du possible les infrastructures de fibre optique existantes du réseau de conduite suisse et des routes nationales. Cette solution permet de tirer profit de différentes synergies. D'une part, des infrastructures de la Confédération qui sont déjà disponibles en grande partie servent à plusieurs usages. D'autre part, l'exploitation de ces deux infrastructures est assurée par un prestataire unique, la BAC. Cette dernière dispose des ressources et des capacités nécessaires à l'exploitation de réseaux optiques de transport de données et peut garantir leur fonctionnement même dans des situations particulières ou extraordinaires.

Une plateforme intégrée devrait être mise en place dans la mesure du possible, à moyen voire à long terme, afin de permettre l'exploitation des liaisons entre la Confédération et les cantons et entre ces derniers via les réseaux IP. Cette solution devrait permettre d'éviter une trop grande complexité des passerelles et des interfaces avec les cantons tout en dégageant des synergies dans le domaine des infrastructures et de l'exploitation.

Plusieurs réseaux partiels ou liaisons IP isolés les uns des autres pourront être mis en place et exploités sur cette plateforme intégrée. Le rôle que celle-ci et les réseaux partiels qu'elle supporte doivent jouer dans l'exploitation reste à définir. À cette fin, la BAC et l'OFIT élaboreront d'ici à la fin de 2019, en collaboration avec l'OFPP, un modèle d'exploitation et de collaboration. Ce document fixera également les tâches et les interfaces en matière d'organisation et de processus, les compétences et les responsabilités. Il tiendra compte des exigences relatives à différentes applica-

21 La stratégie peut être consultée à l'adresse suivante : www.upic.admin.ch > Thèmes > Stratégie et planification TIC de la Confédération > SB000 – Stratégie informatique de la Confédération 2016-2019.

tions importantes pour la sécurité (exploitation possible également en cas de situation particulière ou extraordinaire), des contraintes imposées par la nouvelle LPPCi et par les services informatiques de la Confédération et des réglementations régissant les services standard.

5 Aspects juridiques

5.1 Constitutionnalité

L'Assemblée fédérale est habilitée à voter le présent arrêté financier en vertu de l'art. 167 de la Constitution[22] (Cst.).

La proposition portant sur la réglementation des compétences et la distribution des tâches entre la Confédération, les cantons et les tiers ainsi que sur la répartition des coûts des différents systèmes (cf. ch. 2.2.7) a été prise en considération dans le message concernant la révision totale de la LPPCi. Celui-ci est soumis séparément au Parlement en même temps que le présent message. Afin d'éviter que les cantons et les tiers ne réalisent chacun de leur côté des systèmes différents dont la réunion au sein d'un système national exigerait beaucoup de temps et de ressources, à l'instar de Polycom, il est également prévu de donner à la Confédération la compétence d'imposer des normes. Elle pourra également édicter des prescriptions techniques et fixer des délais.

5.2 Forme de l'acte à adopter

Conformément à l'art. 163, al. 2, Cst. et à l'art. 25, al. 2, de la loi du 13 décembre 2002 sur le Parlement[23], l'acte doit revêtir la forme d'un arrêté fédéral simple. Celui-ci n'est pas assujetti au référendum.

5.3 Frein aux dépenses

Conformément à l'art. 159, al. 3, let. b, Cst., l'art. 1 de l'arrêté fédéral concernant le crédit d'engagement doit être adopté à la majorité des membres de chaque conseil, étant donné qu'il prévoit des dépenses de plus de 20 millions de francs.

22 RS **101**
23 RS **171.10**

Liste des abréviations utilisées

AFD	Administration fédérale des douanes
BAC	Base d'aide au commandement de l'armée
CCDJP	Conférence des directeurs des départements cantonaux de justice et police
CENAL	Centrale nationale d'alarme
CG MPS	Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
Cgfr	Corps des gardes-frontière
DDPS	Département fédéral de la défense, de la protection de la population et des sports
ECS	Exercice de conduite stratégique
EMFP	État-major fédéral Protection de la population
EPT	Équivalent plein temps
ERNS	Exercice du réseau national de sécurité
fedpol	Office fédéral de la police
IP	Protocole internet
IPCC	Information de la population par la Confédération en situation de crise
KomBV-KTV	Réseau national des autorités de la Confédération et des cantons
LPPCi	Loi fédérale sur la protection de la population et sur la protection civile
MétéoSuisse	Office fédéral de météorologie et de climatologie
NCC	Centre de contrôle du réseau
OFPP	Office fédéral de la protection de la population
PES	Présentation électronique de la situation
PRZ	Centre d'essai et de référence
SOC	Centre d'opérations et de sécurité
SRC	Service de renseignement de la Confédération