

## Annexe 7

### Tableau des mesures publiques

Numéro de mesure (plan 2016)	Mesure sodé (permanente) ou mesure additionnelle (activée en tant que de besoin)	Mesures (plan décembre 2016)	Niveau de protection	POSTURE "SECURITE RENFORCEE-RISQUE ATTENTAT" POUR L'ENSEMBLE DU TERRITOIRE NATIONAL	ACTEURS CONCERNES	POSTURE TRANSITION 2017 - 2018 (activation le 02/11/2017)
						COMMENTAIRES
<p>Rappels sur le tableau des mesures : dans ce tableau apparaissent les mesures additionnelles activées dans le cadre de cette posture mais également quelques mesures sodés (qui doivent s'appliquer en permanence) pour lesquelles des précisions ou des commentaires ont été apportés.</p> <p>Les lignes qui apparaissent en jaune dans ce tableau correspondent aux mesures qui ont été créées afin de décliner, dans le plan Vigipirate, les nouvelles dispositions réglementaires de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme. Ces mesures ne seront applicables qu'à compter de la date de promulgation de la loi.</p> <p>Les mesures sont numérotées avec les critères suivants :</p> <ul style="list-style-type: none"> <li>- trigramme de domaine d'action (RSB, TER, etc.) ;</li> <li>- numéro d'objectif de sécurité du domaine ;</li> <li>- degré de contrainte de la mesure, sur une échelle de 0 (mesure du socle) à 3 (mesure très contraignante) ;</li> <li>- numéro d'ordre (dans le tableau du plan Vigipirate) de la mesure de 01 à 0x pour les mesures du socle et de 01 à 0x pour les mesures additionnelles.</li> </ul> <p>Exemple : la mesure AIR 10-01 :</p> <ul style="list-style-type: none"> <li>- est une mesure du secteur aérien (AIR),</li> <li>- s'inscrit dans le 1er objectif du secteur (protéger les aéronefs),</li> <li>- est une mesure du socle (le premier 0) et qui s'applique en permanence,</li> <li>- est la 1ère mesure du socle correspondant à cet objectif.</li> </ul>						
ALR 10-04	sodé	signaler toute transaction, vol ou disparition de matières et tout indice d'événement NRBC-E	publique		A/O	Une vigilance particulière sera apportée au signalement de toute transaction, vol ou disparition de matière NRBC-E (précurseurs d'explosifs, acide sulfurique, bouteilles de gaz, etc.). Une fiche de recommandations pratiques, dédiée aux précurseurs d'explosifs accompagne cette posture Vigipirate, et rappelle le point de contact national à appeler pour signaler tout vol, disparition ou transaction suspecte (PIXAF : 01.78.47.34.29).
ALR 11-02	additionnelle	diffuser l'alerte au grand public	publique	active	A/O	Les ministères veilleront à ce que les opérateurs publics et privés de leur périmètre mettent en place les logogrammes "Sécurité renforcée - Risque attentat" en lieu et place des anciens logogrammes qui peuvent être source de confusion pour la population. Une fiche rappelant les différents niveaux du plan Vigipirate est annexée à la note de posture. Les nouveaux logogrammes peuvent être téléchargés sur le site du SGEN : <a href="http://www.sgsn.gov.fr/vigipirate">http://www.sgsn.gov.fr/vigipirate</a> . <del>Les anciens logogrammes "Alerte attentat" doivent être enlevés et remplacés par les logogrammes "Sécurité renforcée - risque attentat" à l'entrée des établissements accueillant du public.</del>
ALR 11-04	additionnelle	rappeler les conduites à tenir en réponse à la menace d'actions terroristes (fusillade, colis abandonné, alerte à la bombe)	publique	active	A/O	Les fiches de sensibilisation annexées à la note de posture sont diffusées par les ministères qui ciblent le public à atteindre : - fiche "Recommandations pour la sécurisation des lieux de rassemblement ouverts au public" - fiche "Organiser un confinement face à une menace terroriste" - fiche "Produits chimiques : signalement de tout vol ou utilisation suspecte" - fiche "Sécurité du numérique : l'hameçonnage (ou phishing)" - fiche " <del>Journées européennes du patrimoine - comment sécuriser son établissement face à la menace terroriste</del> " - fiche " <del>Organiser un confinement face à une menace terroriste</del> " - fiche " <del>Sensibilisation aux risques de radicalisation en milieu scolaire</del> " - fiche " <del>Signalement de situations suspectes, recommandations à l'usage des agents publics et privés de sûreté et de sécurité</del> "
RSB 10-04	sodé	dans le cadre du droit commun, ordonner la fermeture administrative de lieux de culte qui, par les propos qui y sont tenus, les idées ou théories qui y sont diffusées, ou les activités qui s'y déroulent, provoquent à la commission d'actes de terrorisme en France ou à l'étranger, incitent à la violence, ou font l'apologie de tels actes	publique		A/O	Cette mesure s'applique sur le fondement des articles L.227-1 et L.227-2 du code de la sécurité intérieure. <b>Avertissement : l'application de cette mesure est subordonnée à la promulgation de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme.</b>
RSB 11-01 RSB 12-01 RSB 13-01	additionnelle	renforcer la surveillance et le contrôle	publique	active RSB 12-01	A/O	L'effort de vigilance porte sur les rassemblements liés aux manifestations religieuses, politiques, sportives et culturelles propres à la période couverte par la présente posture. Les marchés de Noël feront l'objet d'une attention particulière. <b>Les manifestations organisées dans le cadre des Journées européennes du patrimoine feront l'objet d'une attention particulière.</b> Une vigilance accrue, quant à la détention d'armes blanches ou autres objets suspects, sera portée lors des contrôles mis en place aux entrées de ces rassemblements. <b>Tout ouant sensibles.</b> Les fins de spectacles doivent également bénéficier d'un dispositif de sécurité jusqu'à la dispersion complète du public.
RSB 12-05	additionnelle	mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier)	publique	active	A/O	Au regard de la menace associée aux attaques par véhicules-béliers les préfets encourageront les collectivités territoriales et opérateurs privés à renforcer les dispositifs de protection passive (plots, barrières, blocs en béton, etc.) sur les lieux et artères les plus fréquentés.
RSB 23-02	additionnelle	en appui des FSI, faire appel aux armées pour la surveillance et la protection des populations dans les zones publiques identifiées	publique	active	A	A l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense et selon les nouvelles modalités du dispositif Sentinelle. Les patrouilles des armées pourront être réorientées pour prendre en compte les principaux événements propres à la période couverte par la posture "Transition 2017 - 2018".

## Annexe 7

### Tableau des mesures publiques

Numéro de mesure (plan 2016)	Mesure(s) permanente(s) ou mesure(s) additionnelle(s) (activée en tant que de besoin)	Mesures (plan décembre 2016)	Niveau de protection	POSTURE "SECURITE RENFORCEE-RISQUE ATTENTAT" POUR L'ENSEMBLE DU TERRITOIRE NATIONAL	ACTEURS CONCERNES	POSTURE TRANSITION 2017 - 2018 (activation le 02/11/2017)
						COMMENTAIRES
						<p>Mention nouvelle par rapport à la précédente posture            [ DR - mention classifiée "diffusion restreinte" - DR ]            [ CD - mention classifiée "confidentiel défense" - CD ]  <b>Mention supprimée de la précédente posture</b></p>
BAT 13-04	additionnelle	en appui des FSI, faire appel aux armées pour des missions de surveillance et de protection de la population aux abords des installations et bâtiments désignés	publique	active	A	La définition des sites concernés et les modalités de déploiement sont laissées à l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense et selon les nouvelles modalités du dispositif Sentinelle. L'application de cette mesure s'inscrit exclusivement dans une logique de protection des personnes et non des biens. Les modes d'action dynamiques sont généralisés.
BAT 12-05	additionnelle	mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier)	publique	active	A/O	Au regard de la menace associée aux attaques par véhicules-béliers les préfets encourageront les collectivités territoriales et opérateurs privés à renforcer les dispositifs de protection passive (plots, barrières, blocs en béton, etc.) sur les lieux et artères les plus fréquentés.
BAT 21-01 BAT 22-01 BAT 23-01	additionnelle	contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	publique	active BAT 21-01	A/O	Les contrôles de l'accès des personnes à l'entrée des établissements d'enseignement et des établissements de santé, médico-sociaux et sociaux est maintenu. Les dispositifs de sécurité des espaces de commerce privilégient la surveillance dynamique des espaces, la détection des comportements anormaux et le recours à la vidéosurveillance. L'effort de contrôle systématique aux accès des espaces touristiques, culturels et de loisirs est maintenu. <del>Les établissements de nuit de type discothèques sont sensibilisés à la menace terroriste et renforcent leurs contrôles aux accès.</del>
BAT 31-01	additionnelle	renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	publique	active	A/O	Renforcement de la surveillance interne dans les organes de presse, les sites touristiques culturels et de loisir, les écoles - en particulier les écoles confessionnelles - les bâtiments officiels. Les dispositifs de sécurité des espaces de commerce privilégient la surveillance dynamique des espaces, la détection des comportements anormaux et le recours à la vidéosurveillance.
IMD 10-01	socle	tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités	publique		O	Signaler tous vols, disparitions ou transactions suspectes de précurseurs d'explosifs (ou agents NRBC) au point de contact national : pôle judiciaire de la gendarmerie national – pixaf@gendarmerie.interieur.gouv.fr – Tph H/24 : 01.78.47.34.29. Références du code de la santé publique : article R5132-58 et article R5132-59.
IMD 10-02	socle	établir et mettre à jour les plans particuliers de protection (PPP), les plans d'opération internes (POI), les plans d'urgence internes (PUI), les plans particuliers d'interventions (PPI), les plans de protection externes (PPE) et les plans de sûreté relatifs aux transports de marchandises dangereuses à haut risque	publique		O	cf. instruction du Gouvernement du 30 juillet 2015 relative au renforcement de la sécurité des sites Seveso contre les actes de malveillance (NOR : DEVP1518240).
IMD 10-06	socle	signaler toute transaction suspecte, vol ou disparition de matières et tout indice d'événement NRBC-E	publique		A/O	Une vigilance particulière sera apportée au signalement de toute transaction, vol ou disparition de matière NRBC-E (précurseurs d'explosifs, acide sulfurique, bouteilles de gaz, etc.). Une fiche de recommandations pratiques, dédiée aux précurseurs d'explosifs accompagne cette posture Vigipirate, et rappelle le point de contact national à appeler en cas à appeler pour le signalement de vol, disparition ou transaction suspecte (PIXAF : 01.78.47.34.29).
CYB	socle	avoir les ressources humaines permettant la cybersécurité	publique		A/O	<p><b>Responsabiliser / Sensibiliser le personnel :</b></p> <ul style="list-style-type: none"> <li>- à la mise en place de mots de passe forts sur les comptes de messagerie et de réseaux sociaux ;</li> <li>- contre les attaques en déni de service et les défigurations et les approvisionner en éléments de langage et de communication sur ces attaques;</li> </ul> <p>Concernant les messages électroniques, inviter les utilisateurs à :</p> <ul style="list-style-type: none"> <li>- porter une attention toute particulière à l'ouverture des messages électroniques dont l'origine n'est pas certaine ;</li> <li>- ne pas suivre les liens figurant dans un message électronique. En cas de nécessité d'accès, ils privilégieront la navigation directe sur le site Internet référencé ;</li> <li>- r'ouvrir les pièces jointes aux messages qu'en cas de nécessité et avec précaution (vérification de l'origine, analyse antivirus ou ouverture dans un environnement dédié) ;</li> <li>- signaler toute suspicion d'attaque auprès du responsable de la sécurité des systèmes d'information.</li> </ul>
CYB		protéger logiquement ses systèmes d'information	publique			<p><b>Protéger logiquement ses systèmes d'information</b></p> <ul style="list-style-type: none"> <li>- Appliquer en priorité les mises à jour des postes utilisateur, en particulier les antivirus, le système d'exploitation et le navigateur Internet et les greffons (Flash, Java, etc.)</li> <li>- Appliquer un filtrage des pièces jointes aux messages électroniques en fonction de leur extension</li> <li>- Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires</li> </ul> <p>Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR</p> <ol style="list-style-type: none"> <li>1. Guide d'hygiène informatique : <a href="http://www.ssi.gouv.fr/hygiene-informatique">http://www.ssi.gouv.fr/hygiene-informatique</a></li> <li>2. Guide des bonnes pratiques : <a href="http://www.ssi.gouv.fr/guide-bonnes-pratiques">http://www.ssi.gouv.fr/guide-bonnes-pratiques</a></li> <li>3. Déris de service – Prévention et réaction : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001">www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001</a></li> <li>4. Sécuriser un site web : <a href="http://www.ssi.gouv.fr/securisation-sites-web/">http://www.ssi.gouv.fr/securisation-sites-web/</a></li> <li>5. Comprendre et anticiper les attaques DDoS : <a href="http://www.ssi.gouv.fr/guide-ddos/">http://www.ssi.gouv.fr/guide-ddos/</a></li> <li>6. Défigurations, déris de services : <a href="http://www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf">www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf</a></li> <li>7. Cyberattaques, prévention, réaction : <a href="http://www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf">www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf</a></li> <li>8. Les bons réflexes en cas d'intrusion sur un système d'information : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002">www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002</a></li> <li>9. Défiguration de sites : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002-004">www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002-004</a></li> <li>10. Mesures de prévention relatives à la messagerie : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002">www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002</a></li> <li>11. Politique de restrictions logicielles sous Windows : <a href="http://www.ssi.gouv.fr/entreprendre/guide/recommandations-pour-la-mise-en-oeuvre-d-une-politique-de-restrictions-logicielles-sous-windows">www.ssi.gouv.fr/entreprendre/guide/recommandations-pour-la-mise-en-oeuvre-d-une-politique-de-restrictions-logicielles-sous-windows</a></li> <li>12. Campagne de matériels prenant l'apparence d'un rançongiciel à multiples capacités de propagation : <a href="http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-012">www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-012</a></li> </ol> <p>Notification d'incidents : <a href="http://www.ssi.gouv.fr/en-cas-d-incident">www.ssi.gouv.fr/en-cas-d-incident</a></p>

## Annexe 7

### Tableau des mesures publiques

Numéro de mesure (plan 2016)	Mesure (sode permanente) ou mesure supplémentaire (activée en tant que de besoin)	Mesures (plan décembre 2016)	Niveau de protection	POSTURE "SECURITE RENFORCEE-RISQUE ATTENTAT" POUR L'ENSEMBLE DU TERRITOIRE NATIONAL	ACTEURS CONCERNES	POSTURE TRANSITION 2017 - 2018 (activation le 02/11/2017)
						COMMENTAIRES
						Mention nouvelle par rapport à la précédente posture [ DR - mention classifiée "diffusion restreinte" - DR ] [ CD - mention classifiée "confidentiel défense" - CD ] <b>Mention supprimée de la précédente posture</b>
AIR 22-01 AIR 23-01	additionnelle	renforcer l'inspection filtrage des personnes (passagers et non passagers) devant accéder en ZSAR sur certains aérodomes désignés	publique	active AIR 22-01	O	<del>Dans l'ensemble des aéroports de plus de 500 000 passagers, aux points d'inspection filtrage : Depuis le 1er septembre 2015, le contrôle aléatoire à l'aide d'EFD s'applique 5% minimum des passagers, en lieu et place de la palpation. De même, le contrôle des bagages de cabine et des objets transportés à l'aide d'équipements de détection d'explosifs s'applique à 5% minimum des bagages de cabine conformément à la nouvelle réglementation européenne depuis le 1er mars 2015.</del>
AIR 22-03	additionnelle	mettre en œuvre des patrouilles systématiques dans les aéroports et les aires de trafic	publique	active	A/O	Dans les ZSAR : modalités de mise en œuvre des patrouilles laissées à la discrétion des préfets compétents. Cette mesure s'applique pour toute la durée de la posture.
AIR 33-01	additionnelle	en appui des FSI, faire appel aux armées pour des opérations de surveillance des zones publiques des aéroports	publique	active	A	La définition des sites concernés et les modalités de déploiement sont laissées à l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense.
MAR 10-02	socle	renforcer la protection des navires à passagers sous pavillon français de type croisière ( <del>mesure non opérationnelle</del> )	publique		A/O	Mise en place de gardes privés sur décision de l'armateur. L'armement des agents privés de sécurité, fait l'objet d'une mesure transitoire (catégorie d'armes autorisées). L'accord des Etats des ports de destination du navire doit être préalablement recherché.
MAR 11-01	additionnelle	activer le contrôle naval volontaire dans les zones désignées	publique	active	A/O	Nord-ouest et est Océan Indien, Golfe persique, Golfe de Guinée, Sud-Est asiatique et en Méditerranée.
MAR 12-02	additionnelle	opérateurs ISPS : appliquer le niveau de sûreté ISPS 2 sur les navires battant pavillon français dans les zones désignées pour une durée spécifiée	publique	active	O	Niveau ISPS 2 applicable : - dans le Nord-ouest de l'Océan Indien (au nord du parallèle 12° Sud et à l'ouest du méridien 080° Est), - dans le Golfe arabo-persique, - dans le détroit de Malacca, - dans la zone du Golfe de Guinée (delta du Niger et eaux territoriales du Gabon à la Guinée-Bissau), - dans les ports de Libye. Les escales dans les ports libyens et les transits dans les eaux territoriales libyennes sont fortement déconseillés jusqu'à nouvelle information. En raison du conflit armé qui sévit au Yémen, les escales des navires battant pavillon français dans ce pays sont à différer jusqu'à nouvelle information. A quel dans un port de ces zones (sauf pour les ports de Libye), le capitaine du navire est autorisé à ramener le niveau ISPS au niveau 1 s'il estime que l'installation portuaire lui assure une sûreté suffisante.
MAR 13-05	additionnelle	escorter ou renforcer la protection des navires prioritaires désignés	publique	active	A/O	Le déploiement des équipes de protection (agents de l'Etat) à bord des navires à passagers sous pavillon français à destination de la Corse et du Royaume-Uni est maintenu. Il est élargi à l'Algérie, voire élargi à d'autres Etats côtiers en fonction des accords à venir avec ces derniers. Il pourra être renforcé en fonction de l'évolution de la menace dans ce secteur. <del>Lorsque le décret d'application sera publié, les gardes privés pourront embarquer à bord des navires à passagers sous pavillon français. Pour les voyages internationaux, cette disposition se fera en concertation avec l'Etat côtier de destination.</del>
MAR 22-06	additionnelle	adapter le dispositif de visite des conteneurs et des cargaisons	publique	active	A	Mesure additionnelle activée.
MAR 33-01	additionnelle	en appui des FSI, et hors dispositif des PSMP (peloton de sûreté maritime et portuaire), faire appel aux armées pour des opérations de surveillance et de protection de la population dans les zones publiques de ports	publique	active	A	La définition des sites concernés et les modalités de déploiement sont laissées à l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense.
MAR 31-02	additionnelle	diffuser des messages d'information et des consignes particulières aux usagers	publique	active	O	Mesure additionnelle activée.
MAR 52-01 MAR 53-01	additionnelle	assurer une surveillance côtière, maritime et aérienne renforcée, ciblée et adaptée aux menaces, en assurant le suivi des navires à risques détectés ou signalés	publique	active 52-01	A	Activation sur l'ensemble de la façade maritime en métropole en laissant aux préfets maritimes l'initiative des points d'application.
MAR 52-02	additionnelle	visiter ou inspecter, en mer, des navires à risque en vertu des habilitations des agents de chaque administration sur ordre du ministre chargé des transports ou du préfet maritime	publique	active	A	Activation sur l'ensemble de la façade maritime en métropole en laissant aux préfets maritimes l'initiative des points d'application.
TER 10-01	socle	organiser des rondes et patrouilles dans les gares, les stations, les rames des métros et des trains de banlieue ainsi que des contrôles d'identité, fouilles de véhicules et de bagages dans l'espace public	publique		A/O	Un effort particulier de coordination de l'ensemble des forces de sécurité présentes dans les gares multimodales est réalisé pour en renforcer la visibilité, le caractère dissuasif et l'efficacité. Les contrôles d'identité peuvent être étendus aux abords des gares ouvertes au trafic international. La durée de contrôle des obligations de détention, de port et de présentation des titres et document de voyage peut être portée de 6 heures à 12 heures. <b>Avertissement : l'application de cette dernière disposition est subordonnée à la promulgation de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme.</b>
TER 11-02	additionnelle	diffuser des messages d'information et des consignes particulières aux usagers	publique	active	O	Procéder à des appels à la vigilance du public, et inviter les usagers à signaler à l'opérateur tout incident de sûreté. Les appels à la vigilance du public, y compris en langues étrangères, pour rappeler de ne pas laisser de colis sans surveillance, sont effectués régulièrement, notamment pendant les plages horaires de grande affluence.
TER 13-04	additionnelle	en appui des FSI, faire appel aux armées pour des opérations de surveillance et de protection de la population dans les points d'accès aux transports urbains	publique	active	A	La définition des sites concernés et les modalités de déploiement sont laissées à l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense.
TER 20-03	socle	en appui des FSI, faire appel aux armées pour des opérations de surveillance dans les zones publiques des gares ferroviaires et routières	publique		A	La définition des sites concernés et les modalités de déploiement sont laissées à l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense.
TER 20-04	socle	organiser des rondes et patrouilles dans les gares, les stations, les rames des métros et des trains de banlieue ainsi que des contrôles d'identité, fouilles de véhicules et de bagages dans l'espace public	publique		A/O	Les contrôles d'identité peuvent être étendus aux abords des gares ouvertes au trafic international. La durée de contrôle des obligations de détention, de port et de présentation des titres et document de voyage peut être portée de 6 heures à 12 heures. <b>Avertissement : l'application de cette dernière disposition est subordonnée à la promulgation de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme.</b>
TER 21-01	additionnelle	diffuser des messages d'information et des consignes particulières aux usagers	publique	active	O	Procéder à des appels à la vigilance du public, et inviter les usagers à signaler à l'opérateur tout incident de sûreté. Les appels à la vigilance du public, y compris en langues étrangères, pour rappeler de ne pas laisser de colis sans surveillance sont effectués régulièrement, notamment pendant les plages horaires de grande affluence.
TER 31-02	additionnelle	diffuser des messages d'information et des consignes particulières aux usagers	publique	active	O	Procéder à des appels à la vigilance du public, en incitant les usagers à signaler à l'opérateur tout incident de sûreté. Les appels à la vigilance du public, y compris en langues étrangères, pour rappeler de ne pas laisser de colis sans surveillance sont effectués régulièrement, notamment pendant les plages horaires de grande affluence.
SAN 50-01	socle	protéger les établissements de santé	publique		A/O	Les directeurs des établissements de santé doivent poursuivre les efforts de sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurité d'établissement (PSE) et la mise en œuvre d'actions de formations à l'intention de l'ensemble de leurs personnels.
FRT 23-02	additionnelle	en appui des FSI et de la Douane, faire appel aux armées pour participer à la mission de contrôle aux frontières	publique	active	A	La définition des secteurs à contrôler est laissée à l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense. Les unités de la force Sentinelle doivent être associées à la conception et à la conduite des missions de contrôle aux côtés des FSI ou des douaniers.