Objectif de sécurité	Numéro de mesure (plan 2016)	Mesure socle (mesure permanente) ou additionnelle (mesure 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	POSTURE Printemps 2017 (activation le 21/03/2017) COMMENTAIRES
						Menant Concourant	*Mention nouvelle par rapport à la précédente posture* ***[DR - mention classifiée "diffusion restreinte" - DR]*** ***[CD - mention classifiée "confidentiel défense" - CD]*** ~~*Mention supprimée de la précédente posture*~~
							Rappels sur le tableau des mesures : dans ce tableau apparaissent les **mesures additionnelles activées dans le cadre de cette posture** mais également **quelques mesures socles** (qui doivent s'appliquer en permanence) **pour lesquelles des précisions ou des commentaires ont été apportés**. Les mesures sont numérotées avec les critères suivants : - trigramme de domaine (RSB, TER, etc.) ; - numéro d'objectif de sécurité du domaine ; - degré de contrainte de la mesure, sur une échelle de 0 (mesure du socle) à 3 (mesure très contraignante) ; - 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. Exemple : la mesure AIR 10-01 : - est une mesure du secteur aérien (AIR), - s'inscrit dans le 1er objectif du secteur (protéger les aéronefs), - est une mesure du socle (le premier 0) et qui s'applique en permanence, - est la 1ère mesure du socle correspondant à cet objectif. Exemple : la mesure BAT 13-04 : - est une mesure du secteur installations et bâtiments (BAT), - s'inscrit dans le 1er objectif du secteur (adapter la sûreté externe), - est une mesure additionnelle d'un niveau de contrainte 3 sur 3 (mesure très contraignante), - est la 4e mesure additionnelle correspondant à cet objectif.
1- Protéger les personnes et les flux	ALR 11-02	additionnelle	diffuser l'alerte au grand public	publique	**active**	A/O	**Les anciens logos "alerte-attentat" doivent être enlevés et remplacés par les logos "Sécurité renforcée - risque attentat" à l'entrée des établissements accueillant du public.**
	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.**
2-Surveiller, contrôler et protéger la zone ouverte au public désignée	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		A	**A l'appréciation des préfets de zone de défense et de sécurité en concertation avec les officiers généraux de zone de défense, les patrouilles des armées pourront être réorientées pour prendre en compte la répartition des bureaux de vote dans leur secteur lors des quatre jours de scrutin (élections présidentielles et législatives).**
1-adapter la sûreté externe	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. L'application de cette mesure s'inscrit exclusivement dans une logique de protection des personnes et non des biens ~~(les bâtiments non utilisés temporairement ne font pas l'objet d'une protection pendant leur fermeture~~). Les modes d'action dynamiques sont généralisés. **En cas de besoin de capacités spécifiques, les demandes des préfets sont centralisées par le ministère de l'intérieur qui adressera ses demandes au ministère de la défense.**
2-adapter la sûreté des accès	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. ~~Maintien des contrôles - non systématiques - à l'entrée des grands espaces commerciaux.~~ **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. **Les établissements de nuit de type discothèques sont sensibilisés à la menace terroriste et renforcent leurs contrôles aux accès.**
3-adapter la sûreté interne	BAT 31-01	additionnelle	renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	publique	**active**	A/O	~~De manière ciblée selon l'appréciation des ministères concernés pour les sites militaires, les sites touristiques symboliques, les services de l'Etat, les ambassades des pays occidentaux, les points d'importance vitale.~~ Reforcement de la surveillance interne dans les organes de presse, ~~les espaces de commerce~~, ~~les lieux de culte,~~ 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.**
1 - Protéger les lieux de production et de stockage des matières dangereuses et leurs transports	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 : DEVP1518240J).
1- Piloter la gouvernance de cybersécurité	CYB	socle	avoir les ressources humaines permettant la cybersécurité	publique		A/O	1.4.1. Responsabiliser le personnel Sensibiliser le personnel : - à la mise en place de mots de passe forts sur les comptes de messagerie et de réseaux sociaux ; - contre les attaques en déni de service et les défigurations et les approvisionner en éléments de langage et de communication sur ces attaques; Concernant les messages électroniques, inviter les utilisateurs à : - porter une attention toute particulière à l'ouverture des messages électroniques dont l'origine n'est pas certaine ; - 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 ; - n'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) ; - signaler toute suspicion d'attaque auprès du responsable de la sécurité des systèmes d'information.

	4-Protéger les systèmes	CYB		protéger logiquement ses systèmes d'information	publique			4.3. Protéger logiquement ses systèmes d'information - 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.) - Appliquer un filtrage des pièces jointes aux messages électroniques en fonction de leur extension - Configurer des restrictions logicielles sur les postes de travail pour empêcher l'exécution de codes à partir d'une liste noire de répertoires Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR 1. Guide d'hygiène informatique : http://www.ssi.gouv.fr/hygiene-informatique 2. Guide des bonnes pratiques : http://www.ssi.gouv.fr/guide-bonnes-pratiques 3. Dénis de service – Prévention et réaction : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001 4. Sécuriser un site web : http://www.ssi.gouv.fr/sécurisation-sites-web/ 5. Comprendre et anticiper les attaques DDoS : http://www.ssi.gouv.fr/guide-ddos/ 6. Défigurations, dénis de services : www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf, 7. Cyberattaques, prévention, réaction : www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf 8. Conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002 9. Défiguration de sites : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002 10. Mesures de prévention relatives à la messagerie : www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002 11. Politique de restrictions logicielles sous Windows : www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-mise-en-oeuvre-dune-politique-de-restrictions-logicielles-sous-windows Notification d'incidents : www.ssi.gouv.fr/en-cas-dincident
3-Exercer la vigilance dans la zone publique des aéroports	2-Protéger les zones de sûreté à accès réglementé (ZSAR) des plate-formes aéroportuaires	AIR 22-01 AIR 23-01	additionnelle	renforcer l'inspection filtrage des personnes (passagers et non passagers) devant accéder en ZSAR sur certains aérodromes désignés	publique		O	**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'ETD 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.**
		AIR 22-03	additionnelle	mettre en œuvre des patrouilles systématiques dans les aérogares et les aires de trafic	publique		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.**
3-Exercer la vigilance dans les zones publiques des ports	1-Protéger les navires	MAR 11-01	additionnelle	activer le contrôle naval volontaire dans les zones désignées	publique		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		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 quai 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 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.**
	5-Protéger les espaces maritimes	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		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		A	Activation sur l'ensemble de la façade maritime en métropole en laissant aux préfets maritimes l'initiative des points d'application.
3-Exercer la vigilance dans les trains grandes lignes	1-Exercer la vigilance dans les transports collectifs urbains	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.
		TER 11-02	additionnelle	diffuser des messages d'information et des consignes particulières aux usagers	publique		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.
	2-Protéger les gares, notamment multimodales	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 21-01	additionnelle	diffuser des messages d'information et des consignes particulières aux usagers	publique		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		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.
4- Protéger les établissements de santé		SAN 50-01	socle	protéger les établissements de santé	publique		A/O	**Les directeurs des établissements de santé doivent poursuivent 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.**