ANNEXE 1.

Tableau des mesures publiques (mesures du plan 2014)

Numéro de mesure (plan Vigipirate 2014)	Mesures (plan Vigipirate 2014)	Niveau de protection	POSTURE "SECURITE RENFORCEE-RISQUE ATTENTAT" POUR L'ENSEMBLE DU TERRITOIRE NATIONAL	ACTEURS	POSTURE Transition 2016-2017 (activation le 01/12/2016) COMMENTAIRES
			Légende	**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.
ALR 11-01	activer les cellules de veille et d'alerte et les cellules de crise	publique	active	**MININT** Tous ministères	Les cellules de crise des ministères sont activées en tant que de besoin.
ALR 11-02	diffuser l'alerte au grand public	publique	active	**SIG** **CIC** Tous ministères	L'application smartphone d'alerte aux populations – principalement conçue pour diffuser les alertes sur des attentats est entrée en service en juin 2016. Il est donc demandé aux préfets d'intégrer cette nouvelle fonctionnalité dans leurs plans de communication avec les citoyens, et le cas échéant, de l'utiliser pour relayer un message local d'alerte et les consignes comportementales adaptées.
RSB 11-01 RSB 12-01 RSB 13-01	renforcer la surveillance et le contrôle	publique	active RSB 13-01	**MININT** **Collectivités** **Opérateurs** **MEN** **MASS** **MAAF** **Collectivités**	L'effort de vigilance porte sur les rassemblements **liés aux fêtes de fin d'année, à la période des soldes d'hiver et lors des événements politiques précédant l'ouverture officielle de la campagne présidentielle. La sensibilisation à la détection et au signalement de comportements suspects doit être réalisée.** ~~**religieuses (musulmane le 13 septembre, chrétienne le 1er novembre, juives à l'automne)** liés aux grands événements estivaux (notamment le Tour de France, les festivals, Paris Plage) et sur les sites touristiques estivaux **(journées européennes du patrimoine les 17 et 18 septembre)**, culturels, sportifs et religieux), les maires des communes littorales de même que les polices municipales sous leur responsabilité sont sensibilisés par les préfets au contexte sécuritaire de la période.~~
BAT 21-01 BAT 22-01 BAT 23-01	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	publique	active BAT 23-01	**Tous ministères** **Collectivités** **Opérateurs**	Contrôles renforcés de l'accès des personnes à l'entrée des **établissements d'enseignement** ~~écoles, établissements scolaires, établissements de l'enseignement supérieur et de la recherche~~. ~~Effort de vigilance et de protection autour des principaux sites touristiques lors des journées européennes du patrimoine (17 et 18 septembre). Contrôles renforcés aux accès~~ et des établissements de santé, médico-sociaux et sociaux. Maintien des contrôles - non systématiques - à l'entrée des grands espaces commerciaux. Effort de contrôles systématiques aux accès des espaces de loisir.
BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	publique	active	**Tous ministères** **Collectivités** **Opérateurs**	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. Renforcement de la surveillance interne dans les organes de presse, les grands magasins et centres commerciaux, les lieux de culte, les sites touristiques, les écoles - en particulier les écoles confessionnelles - les bâtiments officiels ~~en Ile-de-France et dans les Alpes-Maritimes~~.
IMD 10-01	Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités	publique	socle		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	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	socle	**MININT** **Collectivités** MEDDE Tous ministères Opérateurs	cf. instruction du Gouvernement du 30 juillet 2015 relative au renforcement de la sécurité des sites Seveso contre les actes de malveillance (NOR : DEVP1518240J).
IMD 13-04	Restreindre, dérouter ou arrêter les trafics de matières dangereuses	publique	active		Des mesures d'interdiction de transport de matières dangereuses peuvent être prises par les préfets, au cas par cas.

CYB	Avoir les ressources humaines permettant la cybersécurité	publique	socle	**Tous ministères** **Collectivités** **Opérateurs**	1.4.1. : Responsabiliser 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.
CYB	Protéger logiquement ses systèmes d'information	publique	socle	**Tous ministères** **Collectivités** **Opérateurs**	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 : http://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique 2. Guide des bonnes pratiques : http://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/ 3. Déni de service – Prévention et réaction : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001 4. Sécurisation des sites web : http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-sécurisation-des-sites-web/ 5. Comprendre et anticiper les attaques en DDoS : http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-attaques-ddos/ 6. Défigurations, déni 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/agence/contacts/cossicert-fr
AIR 22-01 AIR 23-01	Appliquer un taux de palpation des passagers et de fouille des bagages de cabine supérieur à la réglementation en vigueur sur certains aérodromes désignés	publique		**MEDDE** **MININT** **Opérateurs**	Mesure prête à être activée sur très court préavis, sur des vols ciblés et de manière limitée dans le temps.
AIR 30-02	Faire appel aux armées pour des opérations de surveillance des zones publiques des aérogares	publique	socle	**MININT** MINDEF MEEM	Ensemble des points d'application à déterminer en ciblant en priorité les grands aéroports internationaux ; à adapter en concertation préfets de zone - officiers généraux de zone de défense.
AIR 31-02	Diffuser des messages d'information et des consignes particulières aux usagers	publique	active	**Opérateurs**	Procéder à des appels à la vigilance du public.
MAR 11-01	Activer le contrôle naval volontaire dans les zones désignées	publique	active	**MINDEF** **Opérateurs** MEDDE	Nord-ouest et est Océan Indien, Golfe persique, Golfe de Guinée, Sud-Est asiatique et en Méditerranée.
MAR 12-02	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	**Opérateurs**	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 21-01 MAR 22-01	Opérateurs ISPS : augmenter à un niveau spécifié les taux de contrôles aléatoires continus des passagers dans les installations désignées	publique	active MAR 22-01	**MEEM** MININT MEF	***[DR-100% des passagers et 20% des véhicules sont contrôlés à l'embarquement des navires à passagers. Les contrôles se font sur la base d'une analyse locale permettant de cibler les comportements particuliers avant l'embarquement (enregistrement tardif, véhicule de location, personne seule dans le véhicule, etc.) DR]***
MAR 52-01 MAR 53-01	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 MAR 52-01	**SGmer** MINDEF MININT MEEM MEF	Activation sur l'ensemble de la façade maritime en métropole en laissant aux préfets maritimes l'initiative des points d'application.
MAR 52-02	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	**SGmer** MINDEF MININT MEEM MEF	Activation sur l'ensemble de la façade maritime en métropole en laissant aux préfets maritimes l'initiative des points d'application.

TER 11-02	Diffuser des messages d'information et des consignes particulières aux usagers	publique	active	**Opérateurs**	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 20-03	Faire appel aux armées pour des opérations de surveillance dans les zones publiques des gares ferroviaires et routières	publique	socle	**MININT** MINDEF	Un effort particulier de coordination de l'ensemble des forces de sécurité présentes dans les gares multimodales sera réalisé pour en renforcer la visibilité et le caractère dissuasif. Ensemble des points d'application à déterminer en ciblant en priorité les principales gares à passagers ferroviaires et routières ; à adapter en concertation préfets de zone - officiers généraux de zone de défense.
TER 21-02	Diffuser des messages d'information et des consignes particulières aux usagers	publique	active	**Opérateurs**	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	Diffuser des messages d'information et des consignes particulières aux usagers	publique	active	**Opérateurs MININT**	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.
			Légende	**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*~~