Annexe 2 : tableau 1/2 des mesures publiques

Objectif de sécurité	Numéro de mesure	Mesures	Niveau de protection	POSTURE prorogée le 24 septembre 2014 STATUT	POSTURE prorogée le 24 septembre 2014 COMMENTAIRES
				Légende	*Mention nouvelle par rapport à la précédente posture* ***[DR - mention classifiée "diffusion restreinte" - DR]*** ~~*Mention supprimée de la précédente posture*~~
	RSB 11-01 RSB 12-01 RSB 13-01	renforcer la surveillance et le contrôle	publique	active RSB 11-01	A l'appréciation du niveau local pour le ciblage sur les manifestations ~~estivales~~ d'importance.
	BAT 10-04	Confier aux armées des missions de surveillance et d'observation aux abords des installations et bâtiments publics désignés	publique	socle	Ensemble des points d'application à déterminer en ciblant en priorité les points sensibles et de rassemblement de la population ; à adapter en concertation préfets de zone - officiers généraux de zone de défense.
	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 21-01	De manière ciblée selon l'appréciation des ministères concernés, pour les musées nationaux, les principaux sites touristique et lieux de culte sensibles. Extension aux grands magasins et centre commerciaux à forte affluence. Le niveau de contrôle appliqué doit démontrer un renforcement concret de la vigilance sans entraîner de contrainte excessive à l'activité normale de ces magasins. Il peut se traduire par des inspections visuelles des sacs de façon aléatoire. Le ciblage et l'intensité de ce contrôle sont à définir par les ministères économiques et financiers en liaison avec le ministère de l'intérieur et les représentants du secteur d'activité concerné. ~~Ciblage sur les principaux sites touristiques durant les périodes de forte affluence.~~
	BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	publique	active	Ciblage particulier pour les sites militaires, les sites touristiques symboliques, les services de l'Etat, les ambassades des pays occidentaux, les points d'importance vitale. ~~A l'appréciation du niveau local pour le ciblage sur les principaux sites touristiques durant les périodes de forte affluence.~~
	CYB	Avoir les ressources humaines permettant la cybersécurité	publique	socle	1.4.1. : Responsabiliser le personnel. 1) En rappelant aux utilisateurs les points suivants : - demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ; - minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ; - rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail. ~~2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci.~~

4-Protéger les systèmes	CYB	Protéger logiquement ses systèmes d'information	publique	socle	4.3. : Protéger logiquement ses systèmes d'information En conduisant dans les meilleurs délais les actions suivantes : - assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision ; - contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ; - vérifier ou mettre en place les mesures de prévention en matière de déni de service. L'arrêt du support de Windows XP, effectif depuis le 8 avril 2014, conduit l'ANSSI à rappeler les mesures prescrites lors de la dernière adaptation de mesures VIGIPIRATE du 20 février 2014 : - migration des postes et serveurs vers un système d'exploitation soutenu et, dans la mesure du possible, isolation de ceux qui ne peuvent être migrés (filtrage réseau, cloisonnement des comptes) ; - à défaut, supervision particulière desdits postes et serveurs. La vulnérabilité de Open SSL révélée par l'attaque Heartbleed impose de prendre des mesures particulières (ref d). En cas de vulnérabilité, le correctif doit être appliqué, les clefs des serveurs doivent être renouvelées et les utilisateurs doivent être appelés à changer leur mot de passe. Base documentaire : Notes d'information du site www.cert.ssi.gouv.fr, notamment : - [a] Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ; - [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ; - [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ; - [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL. Guide du site de l'ANSSI, notamment : - [e] www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB.

1-Protéger les aéronefs	AIR 10-03	Pour certaines destinations, mise en œuvre de contrôles supplémentaires des passagers et de leurs bagages de cabine dans les salles d'embarquement	publique	socle	Etats-Unis et Israël
1-Protéger les navires	MAR 11-01	Activer le contrôle naval volontaire dans les zones désignées	publique	active	Nord-ouest et est océan Indien, Golfe persique et Golfe de Guinée. Création d'une zone de CNV dans le sud-est asiatique, réduction de la zone de CNV attenante dans l'est de l'océan indien en conséquence à compter du 12/12/2013.
	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	Nord-ouest océan Indien (au nord du parallèle 12° Sud et à l'ouest du méridien 080° Est), Golfe arabo-persique, détroit de Malacca, zone du golfe de Guinée (Delta du Niger et eaux territoriales du Gabon à la Guinée-Bissau), (mesure reconduite jusqu'au 30/03/2015). A quai dans un port de ces zones, 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 30-05	Faire appel aux armées pour des opérations de surveillance des zones publiques des ports	publique	socle	Ciblé sur le grand port maritime de Marseille.
				Légende	*Mention nouvelle par rapport à la précédente posture* ***[DR - mention classifiée "diffusion restreinte" - DR]*** *Mention supprimée de la précédente posture*