

Numéro de mesure	Mesures	Niveau de protection	POSTURE ALERTE-ATTENTAT à compter du 1er septembre 2015 STATUT	ACTEURS	POSTURE à compter du 1er septembre 2015 COMMENTAIRES
ALR 11-01	activer les cellules de veille et d'alerte et les cellules de crise	publique	active	<u>MININT</u> Tous ministères	Activation des cellules de veille et de crise laissée à l'appréciation des ministères.
ALR 11-02	diffuser l'alerte au grand public	publique	active	<u>SIG</u> <u>CIC</u> Tous ministères	Diffusion de "l'alerte-attentat" en Île-de-France (affichage du logo Vigipirate aux endroits où des mesures de protection renforcées sont mises en œuvre).
RSB 11-01 RSB 12-01 RSB 13-01	renforcer la surveillance et le contrôle	publique	active RSB 12-01	<u>MININT</u> <u>Collectivités</u> <u>Opérateurs</u> <u>MEN</u> <u>MAAF</u> Collectivités	Renforcement de la sécurité des manifestations politiques, scientifiques, culturelles sociales ou festives jugées sensibles, à l'appréciation des préfets. <del>Une attention particulière sera accordée aux rassemblements festifs saisonniers durant les vacances scolaires de printemps et les différentes périodes de congé du mois de mai.</del> Un effort particulier de vigilance et de protection sera porté lors des rassemblements <del>et manifestations</del> d'envergure tels que les <b>manifestations culturelles (concerts à ciel ouvert etc.) festivals</b> , les fêtes religieuses, ou les rencontres sportives. <del>propres à la période estivale. Les voyages et sorties scolaires doivent faire l'objet d'une vigilance particulière s'agissant des lieux d'embarquement et de débarquement.</del>
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 22-01	<u>Tous ministères</u> <u>Collectivités</u> <u>Opérateurs</u>	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 supplémentaire du contrôle des accès dans les organes de presse, les grands magasins et centres commerciaux, les lieux de culte, les bâtiments officiels et les écoles, en particulier confessionnelles, en Île-de-France. <del>Un effort particulier de vigilance et de protection sera réalisé sur les principaux sites touristiques, culturels et historiques rencontrant une forte affluence durant la période estivale.</del> <b>Une attention particulière sera accordée à la période de la rentrée scolaire. Un effort sera réalisé lors des journées du patrimoine, fin septembre 2015, à l'appréciation des préfets.</b> Le ciblage, les modalités et l'intensité de ce contrôle sont à définir : - par le ministère de l'intérieur pour les lieux de culte, - par les ministères économiques et financiers en liaison avec le ministère de l'intérieur et les représentants du secteur d'activité concerné pour les grands magasins et centres commerciaux, - par le ministère de l'éducation nationale pour les établissements scolaires, - par chaque ministère pour les bâtiments officiels. Dans la mesure du possible, les contrôles doivent être au moins aléatoires sinon systématiques. Un effort sera porté sur leur visibilité et sur une fréquence accrue des appels à la vigilance du public. Les contrôles peuvent se traduire par des inspections visuelles des sacs, des filtrages des entrées, une présence renforcée des services de sécurité. Renforcement supplémentaire dans les lieux de culte, écoles confessionnelles, établissements culturels et symboliques sensibles des diverses confessions religieuses sur l'ensemble du territoire national.

BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	publique	active	<u>Tous ministères</u> <u>Collectivités</u> <u>Opérateurs</u>	<p>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.</p> <p>Renforcement de la surveillance interne dans les organes de presse, les grands magasins et centres commerciaux, les lieux de culte, les écoles - en particulier les écoles confessionnelles - les bâtiments officiels en Île-de-France.</p> <p>Un effort particulier de vigilance et de protection sera réalisé sur les principaux sites touristiques, culturels, <del>et</del> historiques <b>et religieux</b> rencontrant une forte affluence. <del>durant la période estivale.</del> Le ciblage, les modalités et l'intensité de ce contrôle sont à définir :</p> <ul style="list-style-type: none"> <li>- par le ministère de l'intérieur pour les lieux de culte,</li> <li>- par les ministères économiques et financiers en liaison avec le ministère de l'intérieur et les représentants du secteur d'activité concerné pour les grands magasins et centres commerciaux,</li> <li>- par le ministère de l'éducation nationale pour les établissements scolaires,</li> <li>- par chaque ministère pour les bâtiments officiels.</li> </ul> <p>Cette mesure peut se traduire par le recours à la vidéo surveillance, des rondes de sécurité plus fréquentes...</p> <p>Renforcement supplémentaire dans les lieux de culte, écoles confessionnelles, établissements culturels et symboliques sensibles des diverses confessions religieuses sur l'ensemble du territoire national.</p>
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	<u>MININT</u> <u>Collectivités</u> MEDDE Tous ministères Opérateurs	<p><a href="#">cf. instruction du Gouvernement du 30 juillet 2015 relative au renforcement de la sécurité des sites Seveso contre les actes de malveillance (NOR : DEVP1518240).</a></p>
CYB	Avoir les ressources humaines permettant la cybersécurité	publique	socle	<u>Tous ministères</u> <u>Collectivités</u> <u>Opérateurs</u>	<p>1.4.1. : Responsabiliser le personnel.</p> <p>1) En rappelant aux utilisateurs les points suivants :</p> <ul style="list-style-type: none"> <li>- demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ;</li> <li>- minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ;</li> <li>- rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail.</li> </ul> <p>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.</p>
CYB	Protéger logiquement ses systèmes d'information	publique	socle	<u>Tous ministères</u> <u>Collectivités</u> <u>Opérateurs</u>	<p>4.3. : Protéger logiquement ses systèmes d'information (partie 1)</p> <p>En conduisant dans les meilleurs délais les actions suivantes :</p> <ul style="list-style-type: none"> <li>- assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision ;</li> <li>- contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ;</li> <li>- vérifier ou mettre en place les mesures de prévention en matière de déni de service.</li> </ul>

CYB	Protéger logiquement ses systèmes d'information	publique	socle	<u>Tous ministères</u> <u>Collectivités</u> <u>Opérateurs</u>	<p>4.3. : Protéger logiquement ses systèmes d'information (partie 2) <span style="float: right;">Base documentaire :</span></p> <p>Notes d'information du site <a href="http://www.cert.ssi.gouv.fr">www.cert.ssi.gouv.fr</a>, notamment :</p> <ul style="list-style-type: none"> <li>- [a] Note CERTA-2012-INF-001 : Défis de service – prévention et réaction ;</li> <li>- [b] Note CERTA-2012-INF-002 : Les défigurations de type WEB ;</li> <li>- [c] Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ;</li> <li>- [d] Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL.</li> <li>- [d] Note CERTA-2004-INF-001-001 : Protection des sites Internet</li> <li>- [e] Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion</li> </ul> <p>Guide du site de l'ANSSI, notamment :</p> <ul style="list-style-type: none"> <li>- [f] <a href="http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf">www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf</a> : recommandation pour la sécurité des sites WEB.</li> <li>- [g] <a href="http://www.ssi.gouv.fr/actualite/protger-son-site-internet-des-cyberattaques">www.ssi.gouv.fr/actualite/protger-son-site-internet-des-cyberattaques</a>.</li> </ul> <p>[a] sécurisation des sites Internet : <a href="http://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web">www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web</a></p> <p>[b] attaques par défiguration : <a href="http://www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques-par-défiguration">www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques-par-défiguration</a></p> <p>[c] comprendre et anticiper les attaques en déni de service : <a href="http://www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos">www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos</a></p> <p>[d] conduite à tenir en cas d'intrusion : <a href="http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002">www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002</a></p> <p>Notification d'incidents :</p> <p>[e] <a href="http://www.ssi.gouv.fr/agence/contacts/cossicert-fr">www.ssi.gouv.fr/agence/contacts/cossicert-fr</a></p>
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 aéroports désignés	publique		<u>MEDDE</u> <u>MININT</u> <u>Opérateurs</u>	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 aéroports	publique	socle	<u>MININT</u> MINDEF MEDDE	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	<u>Opérateurs</u>	Procéder à des appels à la vigilance du public.
MAR 11-01	Activer le contrôle naval volontaire dans les zones désignées	publique	active	<u>MINDEF</u> <u>Opérateurs</u> MEDDE	Nord-ouest et est Océan Indien, Golfe persique, Golfe de Guinée et Sud-Est asiatique.

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	<u>Opérateurs</u>	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. 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. Mesure <b>reconduite applicable</b> jusqu'au 30/09/2015 <b>puis réétudiée à l'issue de cette date.</b>
TER 11-02	Diffuser des messages d'information et des consignes particulières aux usagers	publique	active	<u>Opérateurs</u>	Procéder à des appels à la vigilance du public, <b>et inviter les usagers à signaler à l'opérateur tout incident de sûreté.</b> <del>Effort durant les périodes de plus forte affluence à l'occasion des vacances scolaires de printemps et des différentes périodes de congé du mois de mai. des départs, et des chassés-croisés.</del>
TER 20-03	Faire appel aux armées pour des opérations de surveillance dans les zones publiques des gares ferroviaires et routières	publique	socle	<u>MININT</u> MINDEF	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	<u>Opérateurs</u>	Procéder à des appels à la vigilance du public, <b>et inviter les usagers à signaler à l'opérateur tout incident de sûreté.</b> <del>Effort durant les périodes de plus forte affluence à l'occasion des vacances scolaires de printemps et des différentes périodes de congé du mois de mai. de départ, de retours et de chassés-croisés des vacances estivales des départs, et des chassés-croisés</del>
TER 31-02	Diffuser des messages d'information et des consignes particulières aux usagers	publique	active	<u>Opérateurs</u>	Procéder à des appels à la vigilance du public, <b>en incitant les usagers à signaler à l'opérateur tout incident de sûreté.</b> <del>Effort durant les périodes de plus forte affluence à l'occasion des vacances scolaires de printemps et des différentes périodes de congé du mois de mai. de départ, et de chassés-croisés</del>