DOMAINE	NUMERO DE MESURE	TYPE DE MESURE SOCLE ou ADDITIONNELLE	INTITULE DE LA MESURE (plan Vigipirate - Edition mai 2019)	NIVEAU DE PROTECTION	ETAT DE LA MESURE ACTIVE : ACT INACTIVE : INA	POSTURE "*été - automne 2021*" (active à/c décembre 2021) **Légende associée aux commentaires :** **[DR - mention classifiée "diffusion restreinte" - DR]** Mention nouvelle par rapport à la précédente posture ~~Mention supprimée de la précédente posture~~
RASSEMBLEMENT ET ZONES OUVERTES AU PUBLIC (RSB)	RSB 10-01	socle	mettre en place un dispositif de surveillance et de contrôle	publique ciblage DR	ACT	
	RSB 10-02	socle	interdire les cortèges, défilés et rassemblements dans le cadre du droit commun	publique	ACT	
	RSB 10-03	socle	interdire certaines réunions publiques (organisées hors voie publique) ou fermer provisoirement certains lieux de réunion dans le cadre du droit commun	publique	ACT	
	RSB 10-04	socle	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	ACT	Cette mesure s'applique sur le fondement des articles L.227-1 et L.227-2 du code de la sécurité intérieure.
	RSB 11-01 RSB 12-01 RSB 13-01	additionnelle	renforcer la surveillance et le contrôle	publique	ACT	**RSB 12-01 : 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. Une vigilance accrue, quant à la détention d'armes blanches ou autre objets suspects, sera portée lors des contrôles mis en place aux différents accès de ces rassemblements.** **Une vigilance particulière sera portée aux évènements majeurs affectant cette période : rassemblements liés aux fêtes de fin d'année et aux célébrations religieueses associées, évènements PFUE et élections nationales.**
ES OUVERTES AU PUBLIC (RSB)	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	ACT	**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.** **Ils pourront s'appuyer sur le guide réalisé par le ministère de l'intérieur : "*Guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique*".** ***Ce guide est téléchargeable sur le site INTRANET du ministère de l'Intérieur et en accès libre sur la page d'accueil Internet du Ministère : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique.***

RASSEMBLEMENT ET ZON	RSB 20-01	socle	contrôler les circulations et les flux de personnes et de véhicules sur la voie publique (*hors cortèges, défilés et rassemblements*) dans le cadre du droit commun.	publique	ACT	
	RSB 20-02	socle	procéder à des contrôles d'identité, visite de véhicules, inspection et fouille de bagages dans les lieux identifiés (mesure de droit commun).	publique	ACT	
	RSB 20-03	socle	réglementer l'accès et la circulation des personnes dans le périmètre de protection fixé par un arrêté préfectoral.	publique ciblage DR	ACT	**Cette mesure s'applique sur le fondement de l'article L.226-1 du code de la sécurité intérieure.** **La communication ne doit pas faire connaître le détail, le ciblage, les moyens engagés dans la mise en œuvre de cette mesure.** **La décision du Conseil constitutionnel, du 29 mars 2018, précise :** **- qu'il appartient aux autorités publiques de s'assurer que soit continûment garantie l'effectivité du contrôle exercé par les officiers de police judiciaire sur les personnes privées qui sont associées à la surveillance générale de la voie publique ;** **- que la mise en oeuvre des opérations de contrôle de l'accès et de la circulation, des palpations de sécurité, d'inspection et de fouille de bagages ainsi que de visites de véhicules soit faite sans aucune discrimination entre les personnes ;** **- que le renouvellement d'un périmètre de protection ne peut être décidé par le préfet qu'à la condition que celui-ci établisse la persistance du risque.**
	RSB 23-02	additionnelle	en appui des FSI, faire appel aux armées pour la protection des populations dans les zones publiques identifiées	publique	ACT	**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 "Hiver Printemps 2022"**
INSTALLATIONS ET BATIMENTS (BAT)	BAT 10-01	socle	réglementer le stationnement et/ou la circulation aux abords des installations et bâtiments	publique	ACT	
	BAT 10-02	socle	surveiller les abords des installations et bâtiments	publique	ACT	
	BAT 10-03	socle	contrôler les abords des installations et bâtiments	publique	ACT	
	BAT 11-01 BAT 12-01 BAT 13-01	additionnelle	restreindre voire interdire les activités aux abords des installations et bâtiments désignés	publique ciblage DR	ACT	**BAT 12-01 [DR - BAT 12-01 [DR - A] : à l'appréciation des préfets pour le ciblage des organes de presse, des lieux de culte, des bâtiments officiels, des locaux relevant du ministère de la justice, des lieux culturels (salle de spectacle, rassemblement festif, locaux de presse), les commissariats de Police et les brigades de gendarmerie . Une vigilance particulière sera appliquée pour les rassemblements organisés dans le cadre de la PFUE ainsi que lors des élections nationales.**
	BAT 11-02 BAT 12-02 BAT 13-02	additionnelle	restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés	publique ciblage DR	ACT	**BAT 12-02 [DR - A l'appréciation des préfets pour le ciblage des organes de presse, des lieux de culte, des établissements de santé, médico-sociaux et sociaux, des établissements scolaires - en particulier des écoles confessionnelles - des établissements d'enseignement supérieurs et de recherche, des bâtiments officiels ainsi que les locaux relevant du ministère de la justice et les lieux culturels (salle de spectacle, rassemblement festif, locaux).**
	BAT 11-03 BAT 12-03	additionnelle	renforcer la surveillance aux abords des installations et bâtiments désignés	publique ciblage DR	ACT	**BAT 12-03 [DR - Attention particulière à l'étranger autour des ambassades, résidences officielles, bâtiments consulaires, instituts, lycées et écoles françaises dans les régions de l'arc de crise (Sahel, région du lac Tchad, Afrique du Nord, Turquie, Proche et Moyen-Orient et l'Afghanistan) DR] ainsi que les locaux relevant du ministère de la justice et les lieux culturels (salle de spectacle, rassemblement festif, locaux)..**
	BAT 13-04	additionnelle	en appui des FSI, faire appel aux armées pour des missions de protection des installations et bâtiments désignés **et de la population se trouvant aux abords immédiats**	publique	ACT	**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. Les modes d'action dynamiques sont généralisés.**

INSTALLATIONS ET BATIMENTS (BA	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	ACT	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. Ils pourront s'appuyer sur le guide réalisé par le ministère de l'Intérieur : "Guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique". Ce guide est téléchargeable sur le site INTRANET du ministère de l'Intérieur et en accès libre sur la page d'accueil Internet du Ministère : https://www.interieur.gouv.fr/Publications/Securite-Interieure/Securisation-des-evenements-de-voie-publique.
	BAT 20-01	socle	surveiller les accès des personnes, des véhicules et des objets entrants (dont le courrier)	publique	ACT	
	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	ACT	BAT 21-01 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 grands 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. La sécurité des palais de justice sera renforcée lors des procès des personnes mises en cause pour faits de terrorisme. un contrôle particulier sera appliqué pour les rassemblements organisés dans le cadre spécifique des fêtes de fin d'année, des célébrations religieuses associées, puis de la PFUE et élections nationales.
	BAT 30-01	socle	identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès	publique	ACT	
	BAT 30-02	socle	surveiller la circulation interne des bâtiments et installations	publique	ACT	
	BAT 30-03	socle	interdire certaines réunions publiques (organisées hors voie publique) ou fermer provisoirement certains lieux de réunion dans le cadre du droit commun	publique	ACT	
STALLATIONS ET BATIMENTS (BAT)	BAT 30-04	socle	réglementer l'accès et la circulation des personnes dans le périmètre de protection fixé par un arrêté préfectoral.	publique ciblage DR	ACT	Cette mesure s'applique sur le fondement de l'article L.226-1 du code de la sécurité intérieure. La communication ne doit pas faire connaître le détail, le ciblage, les moyens engagés dans la mise en œuvre de cette mesure. La décision du Conseil constitutionnel, du 29 mars 2018, précise : - qu'il appartient aux autorités publiques de s'assurer que soit continûment garantie l'effectivité du contrôle exercé par les officiers de police judiciaire sur les personnes privées qui sont associées à la surveillance générale de la voie publique ; - que la mise en oeuvre des opérations de contrôle de l'accès et de la circulation, des palpations de sécurité, d'inspection et de fouille de bagages ainsi que de visites de véhicules soit faite sans aucune discrimination entre les personnes ; - que le renouvellement d'un périmètre de protection ne peut être décidé par le préfet qu'à la condition que celui-ci établisse la persistance du risque.
	BAT 31-01	additionnelle	renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	publique	ACT	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.

IN						
SECURITE DU NUMERIQUE (NUM)	BAT 32-02	additionnelle	mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (fusillade, explosif, chimique, véhicule bélier)	publique	ACT	**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.** **Ils pourront s'appuyer sur le guide réalisé par le ministère de l'intérieur : "Guide des bonnes pratiques opérationnelles de sécurisation d'un événement de voie publique".** **Ce guide est téléchargeable sur le site INTRANET du ministère de l'Intérieur et en accès libre sur la page d'accueil Internet du Ministère : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique.**
	NUM 11-02	additionnelle	rechercher sur le SI des marqueurs particuliers correspondant à une attaque	publique ciblage DR	ACT	Compte tenu des campagnes d'attaque Solar Winds et Microsoft Exchange, il est recommandé de prendre connaissances des marqueurs de vulnérabilités via les rapports des éditeurs de sécurité et indiquer à l'ANSSI (via le COSSI - cert-fr.cossi [AT] ssi.gouv.fr) le résultat de la recherche et ses modalités (date la plus ancienne de l'historique des journaux, nombre), même si elle est négative. *Solar Winds* : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-026/ • Rapport Palo Alto : https://unit42.paloaltonetworks.com/solarstorm-supernova/ • Alerte US-CERT et liste des marqueurs : https://us-cert.cisa.gov/ncas/alerts/aa20-352a *Microsoft Exchange* : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004/ • Utilisation de l'outil Exchange On-premises Mitigation Tool (EOMT) fourni par Microsoft le 15 mars 2021, ayant notamment pour fonction de rechercher sur le système des traces connues d'exploitation grâce au Microsoft Safety Scanner : https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/). Pour plus de détails se référer aux Alertes CERT correspondantes. Dans la mesure du possible, il convient d'ajouter ces marqueurs aux systèmes de détection présents (NIDS, HIDS, etc.).
	NUM 31-03	**additionnelle**	**absorber le trafic illégitime au niveau du réseau**	**publique**	ACT	**Compte tenu des attaques menées par DDoS, il est important de s'assurer que les opérateurs de services numériques disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer.**
	NUM 31-09	additionnelle	rappeler l'importance d'une mesure d'hygiène ou sectorielle existante	publique	ACT	**Pour sécuriser les accès à distance des systèmes d'information en cas de télétravail, il est recommandé de recourir à une authentification multi facteurs (https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/), afin d'éviter une authentification depuis un poste attaqué, volé ou perdu et s'assurer du caractère sécurisé de la connexion réseau à travers Internet lorsqu'un utilisateur a besoin de se connecter au système d'information de l'entité à distance. Au regard des menaces d'attaque par hameçonnage, il importe de sensibiliser les utilisateurs à être particulièrement attentifs aux courriels qu'ils reçoivent, les inciter à ne pas activer les macros dans les pièces jointes et mettre en place des mesures pour limiter l'exécution des macros. La fiche « hameçonnage » du SGDSN est une ressource utile : http://www.sgdsn.gouv.fr/vigipirate/securite-du-numerique-lhameconnage-ou-phishing/.**
RITE DU NUMERIQUE (NUM)	NUM 41-01	additionnelle	valider et appliquer un correctif de sécurité	publique	ACT	Les correctifs de sécurité correspondant aux bulletins d'alerte du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques : • CERTFR-2021-ALE-006 (https://www.certa.ssi.gouv.fr/alerte/CERTFR-2021-ALE-006/) Vulnérabilité dans F5 BIG-IP (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure). • CERTFR-2021-ALE-005 (www.certa.ssi.gouv.fr/alerte/CERTFR-2021-ALE-005) Multiples vulnérabilités dans Microsoft DNS server (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure). • CERTFR-2021-ALE-004 (www.certa.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004) Multiples vulnérabilités dans Microsoft Exchange Server (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure). • CERTFR-2020-ALE-026 (www.certa.ssi.gouv.fr/alerte/CERTFR-2020-ALE-026) Présence de code malveillant dans SolarWinds Orion (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure). • CERTFR-2020-ALE-020 (www.certa.ssi.gouv.fr/alerte/CERTFR-2020-ALE-020) Vulnérabilité dans Microsoft Netlogon (se référer à ce bulletin pour obtenir les informations techniques nécessaires à la mise en œuvre de cette mesure).

SECURITE DU NUMERIQUE (NUM)	**NUM 41-02**	additionnelle	vérifier la correction effective d'une vulnérabilité	publique	ACT	Face aux récentes vulnérabilités affectant Microsoft Exchange, l'ANSSI souhaite contrôler le niveau de sécurité et notamment des annuaires Active Directory de chaque Opérateur d'Importance Vitale, Opérateur de Services Essentiels et de chaque ministère afin d'y déceler les défauts de configuration les plus habituels qui affaiblissent le niveau de sécurité et de vérifier, quand c'est possible, que les composants Microsoft Exchange sont bien à jour. A cette fin, l'ANSSI conseille d'utiliser l'outil de collecte en source ouverte ORADAD (Outil de récupération automatique de données de l'Active Directory). La procédure à suivre est la suivante : • Télécharger la dernière version de l'outil de collecte ORADAD disponible sur GitHub [https://github.com/ANSSI-FR/ORADAD/releases] • Extraire les fichiers (exécutable ORADAD.exe et fichier de configuration) • Ouvrir un terminal et exécuter l'outil avec un compte du domaine et depuis un poste membre du domaine. Le fichier de configuration doit être positionné dans le dossier contenant l'exécutable ORADAD.exe [commande à exécuter : ORADAD.exe <outputDirectory>] • Envoyer le fichier contenant les résultats de la collecte (et présent dans le répertoire <outputDirectory>) par email à l'adresse club@ssi.gouv.fr • Si la taille du fichier de collecte est supérieure à 10 Mo, l'ANSSI met à disposition du bénéficiaire un serveur d'upload sur lequel le bénéficiaire peut déposer le fichier contenant les résultats de la collecte. L'URL et les comptes permettant d'accéder au serveur seront fournis à la demande (adresser la demande par email à club@ssi.gouv.fr). L'ANSSI s'engage à fournir un rapport, sous forme électronique, sous quinze jours, avec quelques recommandations à mettre en place pour améliorer significativement le niveau de sécurité et faire face à cette tendance de prise de contrôle du SI par le contrôle de l'annuaire Active Directory. L'ANSSI indiquera également la présence de la vulnérabilité Exchange lorsqu'applicable.
	NUM 51-02 **NUM 52-02**	additionnelle	adapter les dispositifs de réponse à incidents aux caractéristiques de la menace	publique	ACT	Compte tenu des menaces cyber persistantes, il est essentiel de s'assurer que les outils et dispositifs de réponse à incident sont opérationnels et adaptés à la menace numérique et que le personnel chargé de le mettre en œuvre soit familiarisé avec celui-ci. Il est par ailleurs recommandé d'effectuer un exercice d'activation du PCA ou de gestion de crise cyber si le dernier exercice a été effectué il y a plus d'un an. Le guide de l'ANSSI sur les exercices de gestion de crise cyber aide les entités à organiser ces exercices : https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/.
	NUM 51-06	additionnelle	procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques	publique	ACT	Compte tenu de la menace persistante liée aux rançongiciels, il est nécessaire d'être en capacité de restaurer le bon fonctionnement des systèmes les plus critiques en cas de destruction ou d'altération des données par un programme automatisé en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration.