Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Paris, le 02 novembre 2017

Ministère Culture

LE HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE

N° 2017/13

Note
de posture VIGIPIRATE

Objet : Posture VIGIPIRATE « Transition 2017-2018 »

Réf. : Partie publique du Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes n°10200/SGDSN/PSE/PSN du 1er décembre 2016

La posture VIGIPIRATE « Transition 2017-2018 » **s'applique à partir du 2 novembre 2017** et prend en considération les vulnérabilités propres à la période de la fin d'année 2017 et du début 2018. Elle s'applique, sauf événement particulier, **jusqu'au 28 février 2018** afin de prendre en compte l'évaluation du nouveau dispositif SENTINELLE qui sera réalisée début 2018**.**

L'ensemble du territoire national est maintenu au niveau « sécurité renforcée - risque attentat ».

La posture met notamment l'accent sur :

- **la sécurité** des grands espaces de commerce lors des soldes d'hiver, celle **des lieux de rassemblement, marchés de Noël et lieux de culte** marqués par une forte affluence pendant les fêtes de fin d'année ;
- la sécurité dans le **domaine des transports publics de personnes,** en particulier lors des départs et retours des vacances scolaires et universitaires, ainsi que dans les **établissements d'enseignement ;**
- la **protection des systèmes d'information** face au risque d'attaques cybernétiques**.**

La période de la fin d'année 2017 et du début d'année 2018 est caractérisée par :

- **la sortie de l'état d'urgence et l'adoption du projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme ;**
- **le maintien des contrôles aux frontières intérieures ;**
- **l'évolution des modalités de déploiement des armées sur le territoire national à travers la révision du dispositif SENTINELLE.**

Les travaux et mesures destinés à rendre plus efficaces les interactions avec les forces de sécurité intérieures conservent toute leur pertinence.

La circulaire INTA1711331J du 20 avril 2017, relative au plan de relance du tourisme, instaure une convention de site qui permet à la préfecture d'attribuer un label « sécuri-site » à un lieu touristique concerné s'inscrit dans cette logique**.** Cette convention doit déterminer les mesures de sûreté les adaptées au site touristique.

De même, les procédures internes de confinement ou d'évacuation permettent une gestion rapide et efficace du public et des personnels situés dans l'enceinte d'un site ou d'un événement culturel face à une attaque directe, ou lors d'une attaque à proximité.
Enfin, les sorties de spectacle de confinement ou d'évacuation doivent bénéficier d'un dispositif de sécurité jusqu'à la dispersion du public.

A cet égard plusieurs documents ont été élaborés pour soutenir les responsables de sites ou d'événements dans ce domaine, notamment quatre guides qui sont toujours d'actualité :

- *Guide à destination des organisateurs de rassemblements et festivals culturels* ;
- *Guide à destination des dirigeants de salles de spectacle, de cinémas ou de cirques* ;
- *Guide à destination des dirigeants d'établissements culturels patrimoniaux (musées, monuments historiques, archives et bibliothèques)* ;
- *Gérer la sûreté et la sécurité des événements et sites culturels*, publié au mois d'avril 2017.

Ces guides peuvent être consultés sur le site Internet du ministère de la Culture à l'adresse http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels.

Ces guides sont également disponibles sur le site du gouvernement http://www.encasdattaque.gouv.fr, ainsi que le « guide à destination des présidents d'université, des directeurs d'établissements d'enseignement supérieur et des référents défense et sécurité ».

Les attaques par voitures-béliers demeurent un mode d'action fréquemment utilisé par les organisations terroristes.
La vigilance pour faire face à cette menace concerne l'ensemble des acteurs, publics et privés, qui gèrent des parcs de véhicules. Les gestionnaires de parcs de véhicules sont ainsi appelés à signaler, sans délai, aux autorités tout vol de véhicule ou comportement suspect.
Une fiche de recommandations sur ce sujet est disponible sur le site Internet du SGDSN :

- http://www.sgdsn.gouv.fr/uploads/2017/07/fiche-recommandations-vehicules-beliers.pdf

Les préfets encouragent les collectivités territoriales et opérateurs privés à renforcer les dispositifs de protection passive (plots, barrières, etc.) sur les lieux et les artères les plus fréquentés, en s'appuyant notamment sur l'expertise des référents sûreté des directions départementales de sécurité publique et des groupements de gendarmerie départementale.

Ces consignes doivent être retransmises aux acteurs du champ culturel conformément à la chaîne d'information et d'alerte du Ministère de la Culture, notamment, pour les DRAC **(via les DRAC adjoints et DAC, désignés référents sécurité-sûreté locaux du ministère de la Culture par la circulaire SAFIC/SDAIG/MPDOC 2017/002 en date du 24 avril 2017**), les acteurs considérés comme sensibles (cf. votre cartographie régionale), afin qu'ils organisent leur propre protection, et d'en rendre compte au préfet de chaque département.

Par ailleurs vous trouverez en téléchargement sur le site du SGDSN, http://www.sgdsn.gouv.fr/publications/, des fiches pratiques telles que :

- *Recommandations pour la sécurisation des lieux de rassemblement ouverts au public* ;
- *Signalement de situations suspectes – Recommandations à l'usage du grand public* ;
- *Organiser un confinement face à une menace terroriste*.

Enfin, il convient de rappeler à vos collaborateurs appelés à effectuer des missions à l'étranger de consulter préalablement le site du ministère des affaires étrangères http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/ afin de prendre connaissance des consignes de sécurité spécifiques au pays concerné **et à s'inscrire sur le site *Ariane*** du ministère de l'Europe et des Affaires étrangères.

Le Haut fonctionnaire de défense et de sécurité

Hervé Barbaret

Signé : Hervé Barbaret

TABLEAU DES MESURES DE VIGILANCE, DE SURVEILLANCE ET DE CONTROLE

Nota : les mesures nouvelles figurent en gras dans le tableau

N° mesure	Mesure	Commentaires
ALR 11-02	Diffuser l'alerte au grand public	- Les anciens logos « alerte-attentat » doivent être enlevés et remplacés par les logos « Sécurité renforcée – risque attentat » ci-dessous :  - diffusion de messages d'appel à la vigilance dans les établissements recevant du public (ERP), y compris en langues étrangères ; - information claire des visiteurs et spectateurs à l'entrée et sur les sites web de chaque établissement concernant les mesures de contrôle en vigueur : utiliser les pictogrammes en ligne sur le site http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels - utilisation de l'application smartphone SAIP d'alerte aux populations, principalement conçue pour diffuser les alertes sur des attentats.
ALR 11-04	Rappeler les conduites à tenir en réponse à la menace d'actions terroristes (fusillade, colis abandonné, alerte à la bombe)	**Trois fiches de posture sont diffusées en complément de ce tableau :** - **Fiche *Recommandations pour la sécurisation des lieux de rassemblement ouverts au public* ;** - **Fiche *Organiser un confinement face à la menace terroriste ;*** - **Fiche *Sécurité du numérique : l'hameçonnage (ou* phishing*).***
RSB 23-02	En appui des forces de sécurité intérieures, faire appel aux armées pour la surveillance et la protection des populations dans les zones publiques identifiées.	A l'appréciation des préfets de zone de défense et de sécurité **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 **« Transition 2017-2018 »**.

BAT 21-01 BAT 22-01 BAT 23-01	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	L'effort de contrôle systématique aux accès des espaces touristiques, culturels et de loisirs est maintenu. 1) CONTROLE DES VISITEURS / SPECTATEURS : - pour les établissements équipés de portiques : passage systématique sous portique ; - pour les établissements équipés de magnétomètres : utilisation systématique. - valises et sacs de grande contenance : interdits dans les ERP non équipés de scanner à rayons X. Pour les établissements concernés, il convient d'informer le public (site web et affichage) de cette mesure, et de modifier le règlement intérieur de l'établissement. Toute personne refusant l'un de ces contrôles doit se voir interdire l'entrée de l'établissement. Toutefois, pour les chefs d'établissement de l'enseignement supérieur du secteur de la culture qui reçoivent des étudiants, ces derniers peuvent, selon la situation de leur établissement, autoriser leurs professeurs et leurs étudiants à introduire des valises, des sacs et des étuis d'instruments de musique après contrôle visuel du contenu. 2) POUR LE PERSONNEL : Badge (ou pièce d'identité) obligatoire pour l'accès à l'établissement. A l'appréciation des chefs d'établissement et selon la situation de leur établissement, ceux-ci peuvent procéder au renforcement des contrôles (inspection visuelle des sacs) pour les personnels des manifestations extérieures, les prestataires extérieurs, les personnels intérimaires et temporaires, et en tant que de besoin selon la taille, la configuration, le site ou le caractère symbolique de l'établissement, pour les personnels permanents, après information/consultation du CHSCT spécial d'établissement consacré aux mesures de sûreté et de sécurité. 3) LIMITATION DES ACCES AUX SITES : - accès visiteurs : limitation du nombre d'accès à l'initiative des chefs d'établissement ; - autres accès : les accès réservés à du personnel spécifique (artistes, prestataires extérieurs, agents de l'établissement) doivent faire l'objet d'un renforcement des contrôles tel qu'indiqué ci-dessus. 4) VEHICULES ENTRANTS : contrôle systématique et vérification de la marchandise.
BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	Renforcement de la surveillance interne dans les sites touristiques culturels et de loisir. Limitation des flux de visiteurs si l'affluence est jugée trop importante.

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	Signaler tous vols, disparitions ou transactions suspects de précurseurs d'explosifs au point de contact national : pôle judiciaire de la gendarmerie nationale : pixaf@gendarmerie.interieur.gouv.fr Tel : 01.78.47.34.29 Références code de la santé publique : Articles R5132-58 et R5132-59
CYBER	Avoir les ressources humaines permettant la cybersécurité Protéger logiquement ses systèmes d'information	**1) RESPONSABILISER/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 que 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.** **2) 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 de noire de répertoires.** **Fiches de recommandations disponibles sur le site Internet de l'ANSSI et du CERT-FR** ***- Guide d'hygiène :* www.ssi.gouv.fr/hygiene-informatique** ***- Guide de bonnes pratiques :* www.ssi.gouv.fr/guide-bonnes-pratiques** ***- Dénis de service (prévention et réaction) :* www.cert.ssi.gouv.fr/site/CERTA-**

		2012-INF-001 ***- Sécuriser un site web :*** **www.ssi.gouv.fr/sécurisation-sites-web/** ***- Comprendre et anticiper les attaques en DdoS :*** **www.ssi.gouv.fr/guide-ddos/** ***- Défigurations de sites :*** **www.ssi.gouv.fr/uploads/2015/02/Fiches_d_information_Administrateurs.pdf** ***- cyberattaques (prévention, réaction) :*** **www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf** ***- Bons réflexes en cas d'intrusion sur un système d'information :*** **www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002** ***- Défiguration de site*** **www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002-004** ***- Mesures de prévention relatives à la messagerie :*** **www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002** ***- 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** **- Campagne de maliciels prenant apparence d'un rançongiciel à multiples capacités de propagation : www.cert.ssi.gouv.fr/site/CERTFR-201-ALE-012** **Notification d'incidents :** **www.ssi.gouv.fr/en-cas-dincident**