Programme des nouveaux gTLD
Mise à jour de la note explicative
Réduire les comportements malveillants

Contexte – Programme des nouveaux gTLD

Depuis sa création il y a 10 ans en tant qu'organisation multipartite à but non lucratif dédiée à la coordination du système d'adressage de noms sur Internet, l'ICANN compte, parmi ses principes fondamentaux, la promotion de la concurrence sur le marché des noms de domaines et le maintien de la sécurité et de la stabilité d'Internet - un principe reconnu notamment par les États-Unis et d'autres gouvernements. Le développement des domaines génériques de premier niveau (gTLD) permettra plus d'innovation, de choix et de changement concernant le système d'adressage d'Internet, à présent desservi par 21 gTLD.

La décision d'introduire des nouveaux gTLD a fait suite à une longue période de consultation approfondie, menée auprès de l'ensemble des regroupements de la communauté Internet mondiale, et a été prise par les représentants d'un grand nombre de parties prenantes (gouvernements, individus, sociétés civiles, regroupements commerciaux et de propriétés intellectuelles, communauté technologique). Ont également contribué le Comité consultatif gouvernemental (GAC), le Comité consultatif At-Large (ALAC), l'Organisation de soutien aux politiques de codes de pays (CCNSO) et le Comité consultatif pour la sécurité et la stabilité (SSAC). Le processus de consultation, achevé par l'Organisation de soutien aux politiques des noms génériques (GNSO) en 2007, a abouti à la politique d'introduction des nouveaux gTLD adoptée par le conseil de l'ICANN en juin 2008. Le lancement du programme est attendu au cours de l'année calendaire 2010.

Cette note explicative fait partie d'une série de documents publiés par l'ICANN, qui aident la communauté Internet mondiale à comprendre les exigences et processus présentés dans la version préliminaire du guide de candidature. Depuis la fin 2008, le personnel de l'ICANN a partagé la progression du processus d'élaboration du programme avec la communauté Internet à travers des forums de commentaires publics sur les versions préliminaires du guide de candidatures et les documents associés. À ce jour, plus de 250 jours de consultation sur les documents essentiels du programme ont été comptabilisés. Les commentaires reçus continuent d'être soigneusement étudiés et utilisés pour affiner davantage le programme et contribuer à l'élaboration de la version finale du guide de candidature.

Pour obtenir des informations, plannings et activités actuels, associés au programme des nouveaux gTLD, consultez la page

http://www.icann.org/en/tlds/select.htm.

Notez qu'il s'agit uniquement d'une discussion préliminaire. Les candidats potentiels ne doivent pas s'appuyer sur les détails présentés dans le programme des nouveaux gTLD, ce programme restant soumis à modification suite aux différents commentaires qui seront reçus.

Récapitulatif

Des progrès significatifs ont été faits sur la réduction de comportements malveillants potentiels liés au programme des nouveaux gTLD, afin de répondre aux inquiétudes de la communauté.

Les solutions décrites ici viseront à améliorer considérablement l'environnement DNS et fourniront une protection aux requérants, un environnement plus stable ainsi que des outils pour détecter et lutter contre les risques de comportements malveillants. Même si ce domaine exige un perfectionnement constant, ces améliorations contribueront au lancement stable du processus des nouveaux gTLD. La principale préoccupation de l'ICANN restera de résoudre les problèmes de sécurité, de stabilité et de résilience en constante évolution tandis que le programme des nouveaux gTLD progresse vers un lancement et une éventuelle mise en œuvre.

De nombreux travaux de qualité ont été accomplis, notamment par des volontaires de la communauté dans des forums de commentaires ou des groupes de travail. Nous saluons leur contribution à améliorer considérablement l'environnement DNS. L'ICANN vous en remercie.

Ce document est une mise à jour de la note d'origine « Réduire les comportements malveillants » (« note sur les comportements malveillants »), publiée le 3 octobre 2009. La note d'origine est disponible au lien suivant :

http://www.icann.org/fr/topics/new-gtlds/mitigating-malicious-conduct-04oct09-fr.pdf

Dans la note d'origine sur les comportements malveillants, l'ICANN a sollicité des commentaires sur la proposition d'ajouter des mesures spécifiques au contrat de registre des nouveaux gTLD pour tous les registres afin de réduire les risques de comportements malveillants au sein des nouveaux gTLD.

Afin de faciliter ce processus, l'ICANN a complété une étude sur les comportements malveillants, notamment au sein de l'espace TLD. Au cours de cette étude, le personnel de l'ICANN a sollicité et reçu des commentaires de plusieurs sources extérieures, notamment du Regroupement de la propriété intellectuelle (IPC, Intellectual Property Constituency), du Groupe de sécurité Internet du registre (RISG, Registry Internet Safety Group), du Comité consultatif pour la sécurité et la stabilité (SSAC, Security and Stability Advisory Committee), des Équipes de réponses aux urgences informatiques (CERT, Computer Emergency Response Teams) et de membres des communautés bancaire/financière et de la sécurité d'Internet. Ces parties ont décrit plusieurs problèmes de comportements malveillants potentiels et ont encouragé l'ICANN à envisager des méthodes pour les résoudre ou les réduire au sein des contrats de registre des nouveaux gTLD, ou en tant qu'éléments du processus de candidatures. Ces mesures recommandées visent à améliorer la stabilité et la sécurité générales pour les requérants, et à développer la confiance de tous les utilisateurs de ces zones de nouveaux gTLD.

Les résultats de cette étude, et la période de consultation publique correspondante, ont engendré neuf recommandations destinées à fournir des domaines d'intérêt à partir desquels pourraient être créés des contrôles afin de réduire le risque de comportements malveillants au sein des gTLD. Les neuf recommandations seront mises en application dans le programme :

1. ***Examen des opérateurs de registres*** : cette recommandation nécessite que les opérateurs de registres postulant pour de nouveaux gTLD soient examinés de manière appropriée afin de déterminer s'ils ont des antécédents d'activités malveillantes ou illégales.
2. ***Plan établi pour le déploiement DNSSEC*** : cette recommandation requiert qu'un candidat aux nouveaux gTLD établisse obligatoirement un plan pour le déploiement DNSSEC afin de réduire le risque d'enregistrements DNS usurpés.
3. ***Prohibition des caractères génériques*** : cette recommandation exige des contrôles appropriés autour des caractères génériques DNS afin de réduire le risque de redirection DNS vers un site malveillant.
4. ***Suppression des enregistrements orphelins de type glue*** : cette recommandation requiert que les gTLD suppriment les enregistrements de serveurs de noms lorsqu'un système est supprimé du gTLD afin de réduire le risque d'utilisation de ces enregistrements par un acteur malveillant.
5. ***Exigences d'enregistrements des WHOIS complets*** : cette recommandation nécessite que les nouveaux gTLD conservent des enregistrements des « WHOIS complets » afin d'améliorer l'exactitude et l'intégralité des données WHOIS. L'utilisation d'enregistrements de WHOIS complets procure un mécanisme clé de lutte contre l'utilisation malveillante des nouveaux gTLD en fournissant une chaîne plus complète de contrats au sein du TLD. Ceci devrait permettre une recherche de données et une résolution des problèmes de comportements malveillants plus rapides dès leur identification.
6. ***Centralisation de l'accès aux fichiers de zone*** : cette recommandation exige que les informations d'accès aux données des fichiers de zone soient disponibles via une source centralisée afin de permettre une identification plus rapide et précise des points de contact clés au sein de chaque TLD. Cela réduit le temps nécessaire pour prendre des mesures correctives dans les TLD rencontrant des problèmes de comportements malveillants.
7. ***Points de contacts et procédures documentées pour le signalement d'abus au niveau du registre*** : cette recommandation requiert que les gTLD établissent un point de contact unique chargé de traiter les plaintes relatives aux abus, et que les registres fournissent une description de leurs politiques de lutte contre les abus. Ces exigences sont considérées comme des étapes fondamentales dans la lutte contre les comportements malveillants au sein des nouveaux gTLD.
8. ***Participation à un processus de requête de sécurité de registre accélérée*** : cette recommandation nécessite que les nouveaux gTLD puissent prendre des mesures rapides et efficaces au vu de menaces généralisées contre le DNS en établissant un processus dédié visant à contrôler et à approuver des requêtes de sécurité accélérées.
9. ***Proposition de vérification des zones de haute sécurité*** : cette recommandation suggère la création d'un programme volontaire conçu pour désigner les TLD souhaitant établir et prouver un niveau de sécurité et de fiabilité amélioré. Cet objectif général du programme vise à fournir un mécanisme aux TLD qui souhaitent se distinguer en tant que TLD sécurisé et fiable, et aux modèles commerciaux de TLD qui bénéficieraient de cette distinction.

La fin de cette note traitera du statut de travail spécifique concernant chaque recommandation.

Statut des neuf recommandations relatives aux comportements malveillants

Cette section contient les mises à jour et/ou statuts actuels (le cas échéant) pour les neuf recommandations destinées à réduire le risque de comportements malveillants dans les nouveaux gTLD, tel que présenté dans le mémorandum d'origine sur les comportements malveillants (voir « Résumé des points clés de ce document » ci-dessus). Chaque recommandation se compose d'une section « Mises à jour et/ou statuts actuels » détaillant les mises à jour significatives et d'une section « Améliorations recommandées spécifiques pour le processus des nouveaux gTLD » en référence au mémorandum sur les comportements malveillants, publié le 3 octobre 2009.

1 Examen des opérateurs de registres

- ### Mises à jour et/ou statuts actuels

  La recommandation exigeant « l'évaluation » ou la vérification des antécédents des opérateurs de registres a été un principe directeur dans l'amélioration du traitement des candidatures aux nouveaux gTLD. Le traitement des candidatures aux nouveaux gTLD comporte désormais des critères spécifiques qui exigent qu'un candidat aux nouveaux gTLD soit soumis à divers contrôles des antécédents dans le cadre du traitement des candidatures. Par ailleurs, d'après le mémorandum d'origine sur les comportements malveillants, le Module 2 de la version préliminaire du guide de candidature contient des propositions spécifiques sur le droit de refuser des candidats qualifiés s'ils échouent à un processus d'évaluation spécifié. Les détails des critères et propositions du Module 2 de la version préliminaire du guide de candidature sont référencés ci-dessous ou au lien suivant :

  http://www.icann.org/fr/topics/new-gtlds/draft-evaluation-criteria-30may09-fr.pdf

2 Exiger le déploiement DNSSEC

- ### Mises à jour et/ou statuts actuels

  Un plan de déploiement DNSSEC établi demeure une composante obligatoire du traitement des candidatures aux nouveaux gTLD et un élément requis dans la procédure de test préalable à la délégation pour chaque nouveau gTLD. La documentation sur les exigences est référencée dans le Module 5 de la version préliminaire du guide de candidature. Tout comme dans le mémorandum d'origine sur les comportements malveillants, la Spécification 6 de la version 3 du contrat de registre contient des propositions relatives au DNSSEC (voir ci-dessous). La première phrase de la Section 6 de la version 3 a été remplacée par « L'opérateur de registres doit signer ses fichiers de zone TLD en implémentant les extensions de sécurité des systèmes de noms de domaines (Domain Name System Security Extensions, DNSSEC) ».

  REMARQUE : la RFC 4310 (telle que mentionnée ci-dessous) a été mise à jour à la RFC 5910.

3 Prohibition des caractères génériques

- **Mises à jour et/ou statuts actuels**

La proposition relative à la prohibition des caractères génériques DNS fait toujours partie de la Spécification 6 de la version 3 du contrat de registre (voir « Statut du mémorandum d'origine sur les comportements malveillants » ci-dessous). Par ailleurs, l'ICANN a publié une note explicative intitulée « Harms and Concerns Posed by NXDOMAIN Substitution (DNS Wildcard and Similar Technologies) at Registry Level » le 24 novembre 2009. Elle décrit les préjudices et préoccupations soulevés par la substitution NXDOMAIN (généralement implémentée par l'utilisation de caractères génériques DNS) au niveau du registre. Ce document est un ensemble de conclusions publiées par des experts sur le sujet. Le mémorandum actuel est référencé au lien suivant :

http://www.icann.org/en/announcements/announcement-2-24nov09-en.htm

À l'occasion de la réunion publique de Sydney en juin 2009, le conseil d'administration de l'ICANN est arrivé à la conclusion que les nouveaux domaines de premier niveau ne devraient pas utiliser la redirection DNS et la synthétisation de réponses DNS.

En réponse à la résolution du conseil d'administration, le personnel de l'ICANN a inclus l'interdiction de rediriger et de synthétiser les réponses DNS dans le contrat de registre préliminaire pour les nouveaux gTLD. L'ICANN a également intégré un engagement similaire dans le cadre de la requête pour les nouveaux IDN ccTLD dans les conditions générales proposées ainsi que dans les trois options de relation proposées entre l'ICANN et le responsable IDN ccTLD.

Enfin, le conseil d'administration a également demandé au personnel de l'ICANN d'établir des rapports sur les préjudices et préoccupations soulevés par l'utilisation de la redirection et de la synthétisation des réponses DNS, collectivement, la substitution NXDOMAIN.

4 Encourager la suppression des enregistrements orphelins de type glue

- **Mises à jour et/ou statuts actuels**

Le SSAC a constitué un groupe de travail pour étudier cette question. Le groupe de travail examine actuellement les fichiers de zone pour tous les gTLD actuels afin de recenser les serveurs de noms orphelins et, si possible, de déterminer si ces serveurs orphelins sont utilisés à des fins criminelles ou malveillantes. Les recommandations générées par le groupe de travail SSAC proposent aux registres des conseils supplémentaires sur la façon de gérer les enregistrements orphelins et elles seront évaluées pour une éventuelle inclusion dans les processus clés des gTLD.

Tel que stipulé dans le mémorandum d'origine sur les comportements malveillants, les registres doivent fournir une description de la façon dont ils suppriment les enregistrements orphelins de type glue au moment où un serveur de noms est supprimé de la zone (voir ci-dessous).

5 Exigences pour un WHOIS complet

- **Mises à jour et/ou statuts actuels**

La recommandation visant à faire du « service WHOIS complet » une exigence pour tous les nouveaux gTLD est désormais en place. Tous les nouveaux gTLD devront implémenter des exigences pour un WHOIS complet, conformément au nouveau contrat de registre.

Par ailleurs, une nouvelle clause concernant « l'aptitude de recherche » WHOIS a été provisoirement ajoutée dans le contrat de registre préliminaire afin de la soumettre aux commentaires. La clause comporte la proposition suivante :

« Selon l'UDRP, afin d'assister les plaignants à déterminer si un modèle de 'mauvaise foi' a été démontré par un requérant spécifique, les informations WHOIS seront disponibles dans une base de données accessible au public et soumise aux politiques de confidentialité applicables, et pourront être recherchées par nom de domaine, nom de requérant, adresse postale du requérant, noms de contacts, ID de contacts des registraires et adresse de protocole Internet, sans limitation arbitraire. Afin de proposer une base de données WHOIS efficace, la capacité de recherche booléenne sera disponible. »

La clause fournit un outil supplémentaire aux personnes impliquées dans l'identification et la lutte contre les comportements malveillants dans l'espace de noms, à condition que les méthodes et normes utilisés pour effectuer des recherches comportent une structure de contrôle destinée à réduire l'utilisation malveillante de la capacité de recherche. Cette clause existe dans certains contrats de registre actuels (.ASIA, .MOBI, .POST) et est incluse dans cette version préliminaire du contrat de registre des nouveaux gTLD à des fins de discussion. Pour référence, .NAME (http://www.icann.org/en/tlds/agreements/name/appendix-05-15aug07.htm) dispose d'une fonction de recherche « WHOIS approfondie » depuis sa création. La fonction de recherche repose sur un modèle d'accès différencié qui permet de réduire le risque d'utilisation malveillante de la fonction. Le public est invité à formuler des commentaires, notamment sur la façon dont cette condition permettrait de traiter certains types de comportements malveillants, ainsi que sur des solutions alternatives qui prévoient que l'utilisation des données WHOIS pour les noms enregistrés constitue un outil efficace pour réduire les comportements malveillants dans les nouveaux gTLD. Si la condition est approuvée, des suggestions sur le développement d'une spécification technique uniforme pour les fonctions de recherche existantes seront également sollicitées.

6 Centralisation de l'accès aux fichiers de zone

- **Mises à jour et/ou statuts actuels**

La recommandation de créer un mécanisme visant à prendre en charge la centralisation de l'accès aux enregistrements de fichiers de zone a été acceptée par l'ICANN, et un groupe consultatif appelé « Groupe consultatif sur l'accès aux fichiers de zone » (Zone File Access Advisory Group, ZFA AG) a été créé. Ce dernier a reçu le mandat de collaborer avec la communauté afin d'établir une proposition de mécanisme visant à prendre en charge la centralisation de l'accès aux fichiers de zone. Le ZFA AG a terminé son travail sur la proposition d'une stratégie, qui est référencée au lien suivant :

http://www.icann.org/fr/topics/new-gtlds/zfa-strategy-paper-12may10-fr.pdf

La prochaine étape de centralisation de l'accès aux fichiers de zone consiste à implémenter les recommandations décrites dans la proposition.

7 Points de contacts et procédures documentées pour le signalement d'abus au niveau du registre

- **Mises à jour et/ou statuts actuels**

La recommandation exigeant que les nouveaux gTLD communiquent un point de contact spécifique pour les abus de registre et fournissent une description de leurs politiques de lutte contre les abus est une exigence pour tous les nouveaux gTLD. Cela n'a pas changé depuis le mémorandum d'origine sur les comportements malveillants (voir ci-dessous).

8 Participation à un processus de requête de sécurité de registre accélérée

- **Mises à jour et/ou statuts actuels**

Comme indiqué dans le mémorandum d'origine sur les comportements malveillants, l'ICANN a publié une note explicative intitulée « Expedited Registry Security Request Process Posted » (voir ci-dessous). Cette note explicative définit un processus de requête de sécurité de registre accélérée appelé « Expedited Registry Security Request » (ERSR). Il est le résultat d'un effort de collaboration entre l'ICANN et les registres des gTLD visant à élaborer un processus pour prendre rapidement des mesures dans le cas où les registres des gTLD :

- informent l'ICANN d'un incident de sécurité actuel ou imminent pour leur TLD et/ou le DNS ; et
- demandent une renonciation contractuelle pour les mesures qu'ils pourraient prendre ou ont prises afin de réduire ou de résoudre l'incident.

Une renonciation contractuelle est une dispense de conformité à une clause spécifique du contrat de registre pour la période requise pour répondre à l'incident.

La procédure de requête ERSR basée sur le Web est désormais disponible et référencée dans l'annexe A, ou au lien suivant :

http://www.icann.org/en/registries/ersr/.

Ce nouveau processus doit uniquement être employé par les registres des gTLD pour des incidents nécessitant une action immédiate du registre afin d'éviter tout effet néfaste sur la sécurité ou la stabilité du DNS. Dans l'intérêt de la stabilité du DNS, ce processus a été immédiatement implémenté en ligne le 1er octobre 2009. Des informations complémentaires sur le processus ERSR sont disponibles au lien suivant :

http://www.icann.org/en/announcements/announcement-01oct09-en.htm

9 Proposition de vérification des zones de haute sécurité

- **Mises à jour et/ou statuts actuels**

La recommandation de créer une proposition de vérification des zones de haute sécurité a été faite par des groupes de parties prenantes financiers et bancaires tels que le BITS, et une initiative intitulée « Programme des domaines de premier niveau des zones de haute sécurité » (« programme HSTLD ») a été créée. L'initiative consiste à rédiger une proposition de contrôles potentiels pour la vérification de zones de haute sécurité. Afin d'analyser les approches possibles d'une telle proposition et de la soumettre aux commentaires de la communauté, l'ICANN a formé un groupe consultatif de domaines de premier niveau des zones de haute sécurité (« HSTLD AG »). Le HSTLD AG a pour mandat de collaborer avec la communauté, au travers d'un modèle d'élaboration ascendante, afin de proposer une ou des approches au programme volontaire composé d'incitations et de normes de contrôle pour accroître la sécurité et la fiabilité dans les TLD qui ont été sélectionnés pour participer à un tel programme.

Le HSTLD AG est actuellement constitué de membres de la communauté qui ont exprimé un intérêt à participer à l'élaboration du programme, et d'experts dans des disciplines liées au programme (par ex., sécurité, audit, programmes de certification, responsables de services financiers), soutenus par des membres du personnel de l'ICANN. Le HSTLD AG se rencontre régulièrement afin de tirer le meilleur des concepts introduits dans les documents d'origine d'octobre 2009 ainsi que des éléments de contrôle et des exigences du programme préliminaires, et prévoit de publier un programme recevable pour le soumettre à l'examen et à la considération de la communauté. Le HSTLD AG mène ses activités et l'élaboration du programme au travers d'un processus transparent et ouvert. Des informations complémentaires incluant les participants du groupe et les enregistrements des réunions hebdomadaires du HSTLD AG sont disponibles au lien suivant :

http://www.icann.org/en/topics/new-gtlds/hstld-program-en.htm

Le programme ne sera pas exploité par l'ICANN. Une entité indépendante établira les critères et certifiera les TLD selon ces critères. Elle sera chargée de contrôler, de renouveler et de publier les certifications.

Annexe A

Processus de requête de sécurité de registre accélérée

Le processus de requête de sécurité de registre accélérée (ERSR) a été élaboré pour les registres des gTLD qui informent l'ICANN d'un incident de sécurité actuel ou imminent (ci-après désigné par « Incident ») pour leur TLD et/ou le DNS et constitue un outil qui leur permet de demander une renonciation contractuelle pour des mesures qu'ils pourraient prendre ou ont prises afin de réduire ou de résoudre un Incident. Une renonciation contractuelle est une dispense de conformité à une clause spécifique du contrat de registre pour la période requise pour répondre à l'incident. Le processus ERSR permet qu'une sécurité opérationnelle soit maintenue autour de l'Incident tout en tenant informées les parties concernées de manière appropriée (par ex., l'ICANN, d'autres fournisseurs affectés, etc.).

Un Incident peut être :

- une activité malveillante impliquant le DNS d'échelle et un certain degré de gravité qui menace la sécurité, la stabilité et la résilience systématique d'un TLD ou le DNS ;
- la divulgation, l'altération, l'insertion ou la destruction non autorisées des données du registre, ou l'accès non autorisé à des informations ou à des ressources, ou leur divulgation non autorisée, sur Internet par des systèmes fonctionnant conformément à toutes les normes applicables ;
- une occurrence risquant de provoquer une défaillance temporaire ou à long terme d'une ou plusieurs fonctions essentielles d'un registre gTLD, tel que défini dans le plan de continuité des registres gTLD de l'ICANN [PDF, 96K].

Le processus ERSR est uniquement destiné aux Incidents et exige une action immédiate du registre ainsi qu'une réponse accélérée sous 3 jours ouvrés de l'ICANN. Ce processus doit remplacer les requêtes qui doivent être effectuées via la procédure d'évaluation des services de registre (RSEP).

Il est reconnu que dans certaines occasions, les registres se voient demander de prendre des mesures immédiates afin d'empêcher ou de résoudre un Incident. Dans le cas de tels Incidents, les registres sont tenus de soumettre une requête ERSR dès que possible afin que l'ICANN puisse répondre par une renonciation rétroactive, le cas échant.

Les registres peuvent soumettre une requête ERSR en complétant un formulaire de requête à l'adresse http://www.icann.org/cgi/registry-sec. La requête soumise est traitée comme suit :

- La requête ERSR sera automatiquement transférée à l'équipe de réponse aux problèmes de sécurité de l'ICANN et une copie sera fournie au demandeur. L'équipe de réponse aux problèmes de sécurité se compose de membres du personnel des services suivants : Sécurité, Relations registres des gTLD, Conseil général et Conformité.
- Au cas par cas, un membre désigné de l'équipe de réponse aux problèmes de sécurité sera chargé de contacter le registre sous 1 jour ouvré afin de confirmer l'Incident et de demander des informations complémentaires, le cas échéant.
- L'équipe de réponse aux problèmes de sécurité peut demander des informations complémentaires, le cas échéant, afin d'examiner et d'envisager la requête ERSR, et le demandeur devra fournir promptement de telles informations.
- L'équipe de réponse aux problèmes de sécurité se rassemblera dans les 2 jours ouvrés suivant la réception de la requête (et des informations complémentaires requises) afin d'examiner et de déterminer une réponse.
- L'ICANN répondra verbalement ou par écrit sous 3 jours ouvrés suivant la réception de la requête ERSR au demandeur ou à son représentant désigné.
- Un membre désigné de l'équipe de réponse aux problèmes de sécurité restera en contact avec le point de contact principal du registre pendant toute la durée de l'Incident.
- Si la requête est reçue après que le registre a répondu à un Incident, l'ICANN s'efforcera de répondre sous 10 jours ouvrés afin de fournir par écrit une renonciation rétroactive à la requête, le cas échéant.
- Après une réponse à une requête ERSR, l'équipe de réponse aux problèmes de sécurité en collaboration avec le registre affecté établira un compte-rendu après action (AAR) qui sera rendu disponible pour la communauté. Si un AAR doit être publié, l'ICANN et le registre affecté étudieront conjointement les sections de la requête ERSR et l'AAR devrait être rédigé afin de garantir la protection des informations exclusives et confidentielles. L'ICANN et le registre peuvent rédiger de telles informations qu'ils considèrent exclusives ou confidentielles dans la mesure du raisonnable.