المراجعة الثانية للأمن والاستقرار والمرونة (SSR2)

ملخص تنفيذي ونظرة عامة

الملخص التنفيذي

هذا التقرير عبارة عن مسودة مبكرة للنتائج والتوصيات المقدمة من فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات. وهناك العديد من العناصر التي يستمر فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات في التأكيد عليها، لكن فريق المراجعة يرى في المجمل أن التقرير وصل إلى مرحلة توفر فيها التعليقات العامة تعقيبات وآراء مفيدة وهامة تعود بالنفع على التقرير النهائي.

وعلى وجه الخصوص ، يثمّن فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات التعليقات والآراء المقدمة على:

- النتائج والتوصيات.
- ما هو ذلك القطاع في ICANN (أي مجلس الإدارة أو منظمة ICANN أو مجتمع ICANN) الذي يجب عليه التعامل مع كل توصية.
- ما المؤشرات الأنسب في جعل كل توصية قابلة للقياس، مع تجنب المبالغة في تعديل وهندسة الحل.
- ما الأولوية التي يجب إيلاؤها لكل توصية.
- ما التقارير الإضافية أو المواد الأخرى التي تشعر بأن على فريق المراجعة أخذها بالاعتبار قبل الانتهاء من توصياته (يرجى الاطلاع على صفحة ويكي لفريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات،[1] بما في ذلك "مواد الخلفية" و"مواد الإحاطة" و"الأسئلة والأجوبة" للمواد التي راجعها الفريق).

وفقًا للعملية المقررة لمراجعة المجتمع، ستتاح للمجتمع أيضًا فرص إضافية للمساهمة في التقرير النهائي لفريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات.

نظرة عامة

المقدمة

[تضاف في التقرير النهائي.]

نبذة خلفية

[تضاف في التقرير النهائي.]

الأهداف

بموجب اللائحة الداخلية لمنظمة ICANN[2] (القسم 4.6 (ج))، يوعز مجلس الإدارة بإجراء مراجعة دورية لتنفيذ ICANN التزامه بتعزيز الاستقرار التشغيلي والموثوقية والمرونة والأمن وقابلية التشغيل التوافقي على مستوى العالم لكل من الأنظمة والعمليات، سواء الداخلية أو الخارجية، والتي تؤثر و/أو تتأثر بشكل مباشر بنظام المعرّفات الفريدة للإنترنت التي تقوم ICANN بتنسيقها (والمشار إليها بلفظ "مراجعة الأمن والاستقرار والمرونة").

وعلى وجه التحديد:

ثانيًا. فيما يلي القضايا التي قدر ينظر فريق مراجعة الأمن والاستقرار والمرونة ("فريق مراجعة SSR") في تقييمها:

A. مسائل الأمن والاستقرار التشغيلي والمرونة، المادية والشبكة على حد السواء، والمتعلقة بتنسيق نظام الإنترنت للمعرفات الفريدة؛
B. التوافق مع إطار التخطيط لحالات الطوارئ الأمنية المناسبة لنظام الإنترنت والمعرفات الفريدة.

1 صفحة ويكي الخاصة بفريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات في ICANN على، https://community.icann.org/display/SSR/SSR2+Review.

2 "اللائحة الداخلية لهيئة الإنترنت للأرقام والأسماء المخصصة" ICANN، وتعديلاتها في 28 نوفمبر/تشرين الثاني 2019، https://www.icann.org/resources/pages/governance/bylaws-en.

C. الحفاظ على إجراءات أمنية واضحة وقابلة للتشغيل المتبادل عالميًا بالنسبة لتلك الأجزاء من نظام المعرّفات الفريدة للإنترنت والتي تقوم ICANN على تنسيقها.

ثالثًا. يجب أن يقيّم فريق مراجعة SSR مدى نجاح منظمة ICANN في تنفيذ جهود الأمان وفعالية جهود تحقيق الأمان في التعامل مع التهديدات والتحديات الفعلية والمحتملة على أمان واستقرار نظام أسماء النطاقات، ومدى كفاية وقوة جهود الأمان في مواجهة التحديات والتهديدات المستقبلية لأمان واستقرار ومرونة نظام أسماء النطاقات، وذلك بما يتفق مع مهمة ICANN.

رابعًا. سيقوم فريق مراجعة SSR أيضًا بإجراء تقييم لدرجة ومدى تنفيذ توصيات مراجعة SSR السابقة، ومدى ما آلت إليه عملية تنفيذ تلك التوصيات من تأثير مرغوب.

خامسًا. تُجرى مراجعة SSR مرة كل خمس سنوات على أقل تقدير، على أن تُحسب اعتبارًا من تاريخ تأسيس فريق مراجعة SSR السابق.

توصيات فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات - ملخص

قام فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات بمواءمة جميع توصيات فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات مع خطة ICANN الاستراتيجية للفترة من 2021-2025[3] وأهدافها وغاياتها. ويحدد التقرير الأهداف ذات الصلة التي تدعمها كل توصية على حدة؛ حيث أزال فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات أي توصيات من هذا التقرير لم تتماشى بوضوح مع الخطة الاستراتيجية.

تتوافق جميع توصيات فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات مع الخطة الإستراتيجية لمنظمة ICANN، وبالتالي تعتبر ذات أولوية عالية.

الرقم	التوصية	المالك	الأولوية
1	**إتمام تنفيذ جميع توصيات مراجعة الأمن والاستقرار والمرونة الأولى ذات الصلة**		عالية
2	**توصية فريق مراجعة الأمن والاستقرار والمرونة الأولى رقم 9 - أنظمة إدارة أمن المعلومات وشهادات الأمن** 2.1. يجب على منظمة ICANN وضع خريطة طريق لعمليات تدقيق الأمان وأنشطة التوثيق وفق معايير الصناعة التي يجري الاضطلاع بها، بما في ذلك تواريخ تنفيذ المراحل للحصول على كل توثيق وتسليط الضوء على مجالات التحسين المستمر. 2.2. يجب على منظمة ICANN وضع خطة لعمليات التوثيق ومتطلبات التدريب للأدوار في المنظمة، وتتبع معدلات الإكمال، وتوفير الأساس المنطقي لاختياراتهم، وتوثيق كيفية ملاءمة عمليات التوثيق مع استراتيجيات منظمة ICANN لإدارة الأمن والمخاطر. 2.3. يجب أن تقدم منظمة ICANN أيضًا أسبابًا لاختياراتهم، من خلال توضيح مدى ملاءمتها لاستراتيجيات الأمن وإدارة المخاطر 2.4. يجب على منظمة ICANN تطبيق نظام إدارة أمن المعلومات وإجراء مراجعة من جهة خارجية. 2.5. من أجل جني فوائد أي نظام للتوثيق والتدقيق، يجب إجراء تدقيق لمنظمة ICANN وتوثيقها من خلال جهة خارجية وفقًا لمعايير الأمان في هذا المجل ويجب تقييم خيارات التوثيق وفقًا للمعايير الدولية المقبولة قبولاً عامًا (مثل المعيار ITIL والمعيار ISO 27001 والمعيار SSAE - 18) لمسؤولياتها التشغيلية.		عالية

[3] "خطة ICANN الاستراتيجية للسنوات المالية 2021-2025" في ICANN، وآخر تحديث في 29 مارس/أذار 2019، https://www.icann.org/public-comments/strategic-plan-2018-12-20-en.

3	**توصيات فريق مراجعة الأمن والاستقرار والمرونة الأولى رقم 12 و15 و16 - استراتيجية وإطار ومؤشرات الأمن والاستقرار والمرونة، والكشف عن نقاط الضعف** 3.1. يجب على منظمة ICANN أن تعالج قضايا الأمن بشكل واضح وعلنا (مع مراعاة الأمن التشغيلي، على سبيل المثال، بعد وقف وتجهيل معتبرين لهوية المعلومات، إذا لزم الأمر)، وتعزيز أفضل الممارسات الأمنية عبر جميع الأطراف المتعاقدة. 3.2. يجب على منظمة ICANN أيضًا أن تستحوذ على أفضل الممارسات ذات الصلة بالأمن والاستقرار والمرونة في وثيقة إجماع، وأن تضع أهدافًا واضحة وقابلة للقياس ويمكن تتبعها، ثم تنفذ الممارسات في العقود والاتفاقيات ومذكرات التفاهم. 3.3. يجب على منظمة ICANN تنفيذ إعداد تقارير منسقة حول الكشف عن الثغرات الأمنية. يجب إيصال عمليات الإفصاح والمعلومات المتعلقة بالمسائل ذات الصلة بالأمن والاستقرار والمرونة على الفور إلى الأطراف المعنية محل الثقة (مثل المتضررين من مشكلة محددة أو من يتعين عليهم حلها)، كما في حالات الانتهاكات في أي طرف متعاقد وفي حالات الثغرات الرئيسية التي تم اكتشافها وإبلاغ منظمة ICANN بها. 3.4. يجب أن تضع منظمة ICANN خطة اتصال واضحة لإيصال التقارير إلى المجتمع وتقديم تقارير منتظمة (على الأقل سنويًا) وفي الوقت المناسب تحتوي على مقاييس مؤشرات مجهّلة المصدر لعملية الكشف عن الثغرات الأمنية. ويجب أن تحتوي هذه البيانات على إفصاح مسؤول على النحو المحدد في العملية المتفق عليها مع المجتمع وأن تشتمل على مؤشرات مجهّلة المصدر.		عالية
4	**توصية فريق مراجعة الأمن والاستقرار والمرونة الأولى رقم 20 و22 - شفافية الميزانية وتحديد ميزانية الأمن والاستقرار والمرونة في نطاقات gTLD الجديدة** 4.1. متى ما كان ذلك ممكنًا (من الناحية التعاقدية) ومعقولاً من حيث الجهد (أي أكثر من 10٪ من النشاط الموضح في بند الميزانية)، يجب أن تكون ICANN أكثر شفافية مع الميزانية المخصصة لقطاعات منظمة ICANN المتعلقة بتنفيذ إطار عمل أمن واستقرار ومرونة أنظمة المعرّفات (IS-SSR) وأداء الوظائف ذات الصلة بالأمن والاستقرار والمرونة، بما في ذلك الوظائف المرتبطة بطرح نطاقات gTLD الجيدة.		متوسطة
5	**توصية فريق مراجعة الأمن والاستقرار والمرونة الأولى رقم 27 - إدارة المخاطر** 5.1. يجب أن يكون إطار إدارة مخاطر ICANN مركزيًا ومنسقًا على المستوى الاستراتيجي. 5.2. يجب على منظمة ICANN توضيح إطار المخاطر بشكل واضح ومواءمة الإطار بشكل استراتيجي في مقابل متطلبات وأهداف المنظمة، ووصف مقاييس النجاح ذات الصلة وكيفية قيام منظمة ICANN بتقييم هذه المقاييس. 5.3. يجب على ICANN إتاحة المعلومات المتعلقة بإدارة المخاطر بشكل مركزي أمام المجتمع. يجب تحديث هذه المعلومات بانتظام لتعكس المشهد الحالي للتهديدات (سنويًا على الأقل).		عالية
6	**استحداث منصب مسؤول عن كل من الأمن الاستراتيجي والتكتيكي وإدارة المخاطر** 6.1. يجب على منظمة ICANN استحداث منصب مسؤول عن كل من الأمن الاستراتيجي والتكتيكي وإدارة المخاطر عبر مجال الأمن الداخلي للمنظمة، بالإضافة إلى نظام المعرّفات العالمي الخارجي. 6.2. ويجب على منظمة ICANN توظيف شخص مؤهل تأهيلاً مناسبًا لذلك المنصب وتخصيص ميزانية محددة تكون كافية لتنفيذ وظائف هذا الدور. 6.3. يجب أن يدير هذا المنصب وظيفة الأمان في منظمة ICANN وأن يشرف على تفاعلات الموظفين في جميع المجالات ذات الصلة التي تؤثر على الأمن. 6.4. يجب أن يقدم شاغل المنصب أيضًا تقارير منتظمة إلى مجلس إدارة ICANN وللمجتمع. 6.5. ومن المفترض أن يعمل هذا المنصب عمل مستكشف المسارات والقائم بحل المشكلات على أن يقوم بوضع استراتيجيات وتنفيذ برامج متعددة الأوجه لتحقيق تحسينات جوهرية. 6.6. بالإضافة إلى ذلك، يجب أن يشارك هذا الدور في جميع المفاوضات التعاقدية ذات الصلة بالأمان (على سبيل المثال، سلاسل التوريد لكل من الأجهزة والبرامج واتفاقات مستوى		عالية

	الخدمة المرتبطة بها) التي تقوم بها منظمة ICANN، من خلال التوقيع على جميع الشروط التعاقدية المتعلقة بالأمان.		
7	**إجراء مزيد من التطوير لإطار عمل إدارة مخاطر الأمن** 7.1. يجب على منظمة ICANN توضيح إطار إدارة المخاطر الأمنية بوضوح والتأكد من توافقه استراتيجيًا مع متطلبات وأهداف المنظمة. 7.2. يجب أن تصف منظمة ICANN مقاييس النجاح ذات الصلة وكيفية تقييم هذه المقاييس. وصفَ فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات أسس هذا الأمر بالتفصيل في تعقيبات إضافية بشأن توصية فريق مراجعة الأمن والاستقرار والمرونة الأولى رقم 9 (انظر "توصية فريق مراجعة الأمن والاستقرار والمرونة الأولى رقم 9 - أنظمة إدارة أمن المعلومات وتوثيقات الأمن" في بداية هذا التقرير). 7.3. يجب على منظمة ICANN: 7.3.1. اعتماد وتطبيق المعيار ISO 31000 "إدارة المخاطر" والتحقق من صحة وتوثيقات تنفيذها باستخدام عمليات التدقيق المستقلة والمناسبة.[4] يجب أن تعود جهود إدارة المخاطر بالنفع على خطط ومخصصات استمرارية الأعمال والتعافي من الكوارث. 7.3.2. التحديث المنتظم لسجل مخاطر الأمن واستخدام ذلك السجل في تحديد الأولويات وإرشاد الأنشطة التي تقوم بها منظمة ICANN. يجب على منظمة ICANN تقديم تقارير حول تحديثات منهجيتها والتحديثات التي تقوم بها على سجل المخاطر الأمنية. يجب أن تعود النتائج بالنفع على استمرارية الأعمال/التعافي من الكوارث ونظام إدارة أمن المعلومات (ISMS). 7.3.3. تعيين أو تخصيص شخص مسئول ومخصص يكون مسئولاً عن إدارة مخاطر الأمن تقوم التقارير إلى دور أمن حزمة-C وفقًا لما هو موضح في التوصية "منصب أمن حزمة-C".		عالية
8	**إقرار خطة لاستمرارية الأعمال استنادًا إلى المعيار ISO 22301.** 8.1. يجب على منظمة ICANN إقرار خطة لاستمرارية الأعمال لجميع الأنظمة المملوكة لمنظمة ICANN أو التي تقع تحت إشرافها، استنادًا إلى المعيار ISO 22301 "إدارة استمرارية الأعمال".[5] 8.2. يجب على ICANN تحديد أهمية الأطر الزمنية الوظيفية والمقبولة لكل من استمرارية الأعمال والتعافي من الكوارث استنادًا إلى مدى إلحاح وضرورة استعادة الوظائف بالكامل. 8.3. بالنسبة لعمليات هيئة المُعرّفات الفنية العامة (PTI) (وظائف IANA، والتي تشمل جميع الأنظمة ذات الصلة والتي تسهم في أمن واستقرار نظام أسماء النطاقات وأيضًا في إدارة خادم ملف الجذر)، يجب على منظمة ICANN وضع أسلوب ومنهم مشترك من أجل خدمة الاستمرارية بالتعاون الوثيق مع اللجنة الاستشارية لنظام خادم الجذر (RSSAC) ومشغلي خوادم الجذر. 8.4. يجب على منظمة ICANN نشر دليل (على سبيل المثال؛ موجز) لخطط ومخصصات استمرارية الأعمال الخاصة بها. ويجب الاستعانة بمدقق خارجي من أجل توثيق جوانب الامتثال في تنفيذ خطط استمرارية الأعمال المترتبة على ذلك.		عالية
9	**التأكد من أن خطة التعافي من الكوارث مناسبة وفعالة وأيضًا موثقة توثيقًا جيدًا** 9.1. يجب على منظمة ICANN ضمان أن خطة التعافي من الكوارث لعمليات هيئة المُعرّفات الفنية العامة (وظائف IANA) تشمل جميع الأنظمة ذات الصلة التي تسهم في أمن واستقرار نظام أسماء النطاقات وأيضًا تشتمل على إدارة ملفات خوادم الجذر كما أنها تتماشى مع المعيار المنظمة الدولية للتقييس 27031 إرشادات لجاهزية تكنولوجيا المعلومات والاتصالات لاستمرارية الأعمال. يجب على منظمة ICANN وضع هذه		عالية

[4] المنظمة الدولية للتقييس، "ISO 31000 إدارة المخاطر"، https://www.iso.org/iso-31000-risk-management.html.
[5] "ISO 22301:2019 الأمن والمرونة — أنظمة إدارة استمرارية الأعمال — المتطلبات"، https://www.iso.org/standard/75106.html.

	الخطة بالتعاون اللصيق مع اللجنة الاستشارية لنظام خادم الجذر ومع مشغلي خوادم الجذر. 9.2. يجب على منظمة ICANN إقرار خطة تعافي من الكوارث لجميع الأنظمة المملوكة لمنظمة ICANN أو التي تقع تحت إشرافها، أيضًا بالتوازي مع المعيار ISO 27031 إرشادات لجاهزية تكنولوجيا المعلومات والاتصالات لاستمرارية الأعمال. 9.3. كما يجب على منظمة ICANN وضع خطة للتعافي من الكوارث في غضون اثني عشر شهرًا من اعتماد مجلس إدارة ICANN لهذه التوصيات حول تأسيس موقع ثالث على الأقل من أجل التعافي من الكوارث (بالإضافة إلى لوس أنجلوس وكالبيبر)، وعلى وجه التحديد خارج الولايات المتحدة وأقاليمها ومنظمة أمريكا الشمالية، بما في ذلك خطة من أجل التنفيذ. 9.4. يجب على منظمة ICANN نشر ملخص بإجمالي خططها ومخصصاتها من أجل التعافي من الكوارث. ويجب على منظمة ICANN الاستعانة بمدقق خارجي من أجل توثيق جوانب الامتثال في تنفيذ خطط التعافي من الكوارث تلك.		
10	**تحسين إطار عمل تحديد وقياس امتثال أمين السجل والسجل** 10.1. وضع إطار عمل لمؤشرات الأداء من أجل الاسترشاد بمستوى الامتثال من جانب أمناء السجلات والسجلات فيما يخص التزامات WHOIS (بما في ذلك عدم الدقة)، إضافة إلى العناصر الأخرى التي تؤثر على إساءة الاستخدام والأمن والمرونة الموضحة في مراجعة خدمة دليل التسجيل/WHOIS2 ومراجعة المنافسة وثقة واختيار المستهلكين.[76] 10.2. تخصيص بند محدد في الميزانية من أجل فريق مسئولي الامتثال المنوط بهم التنفيذ النشط أو البدء النشط في أعمال اختبارات/تقييمات إدارة الأداء لمؤشرات اتفاقية مستوى الخدمة المتفق عليها. 10.3. تعديل فقرة تجديد اتفاقية مستوى الخدمة من "تجديد تلقائي" إلى تجديد دوري كل أربع سنوات ويشتمل على فقرة مراجعة مشمولة (ومن شأن فترة المراجعة هذه النظر في مستوى الامتثال بمؤشرات الأداء من جانب أمين السجل والسجل والتوصية بإرفاق متطلبات من أجل تقوية الأمن والمرونة متى ما ظهرت بوادر عدم الامتثال). 10.4. وعلاوة على ذلك، يجب على مجلس إدارة ICANN تولي المسئولية عن إنهاء عملية وضع السياسات العاجلة في منظمة دعم الأسماء العامة EPDP[8] وتمرير وتنفيذ سياسة WHOIS في العام التالي على نشر هذا التقرير.		عالية
11	**قيادة جهود من أجل تطوير تعاريف حول إساءة الاستخدام وتمكين إعداد وتقديم التقارير في مقابل تلك التقارير** 11.1. يجب مجلس إدارة ICANN قيادة جهود من شأنها الحد من الصياغة الغامضة والتوصل إلى اتفاق مقبول قبولاً عامًا فيما يخص إساءة الاستخدام والأمن والاستقرار والمرونة وتهديدات الأمن في عقودها المبرمة مع الأطراف المتعاقدة وخطط التنفيذ. 11.2. يجب على منظمة ICANN ومجلس الإدارة تنفيذ التزامات ذات صلة بالأمن والاستقرار والمرونة (بالإضافة إلى توصيات فريق مراجعة المنافسة وثقة واختيار المستهلكين وخدمة		عالية

6 فريق مراجعة خدمة دليل التسجيل-WHOIS، "مراجعة خدمة دليل التسجيل (RDS) أو WHOIS2: التقرير النهائي"، في 3 سبتمبر/أيلول 2019، https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf.

7 "المنافسة على ثقة العميل واختياره: التقرير النهائي"، ICANN في 8 سبتمبر/أيلول 2018، https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

8 توصيات سياسة منظمة دعم الأسماء العامة في ICANN "عملية وضع السياسات العاجلة في منظمة دعم الأسماء العامة EPDP فيما يخص المواصفة المؤقتة لبيانات تسجيل gTLD من أجل نظر مجلس إدارة ICANN فيها، 1 مايو/أيار 2019، https://www.icann.org/public-comments/epdp-recs-2019-03-04-en.

	دليل التسجيل/WHOIS2) استنادًا إلى تعاريف إساءة الاستخدام الموضوعة من جانب المجتمع دون تأخير9. 11.3. يجب على مجلس إدارة ICANN بالتوازي أن يشجع عزم المجتمع على وضع تعريف (وتطبيق) لانتهاك نظام أسماء النطاقات DNS، واعتماد مصطلح إضافي وتعريف خارجي متجدد لمصطلح "التهديد الأمني"—وهو المصطلح المستخدم في مشروع الإبلاغ عن نشاط انتهاك النطاق (DAAR)، وأيضًا اللجنة الاستشارية الحكومية GAC (في بيان بكين الختامي10 وللمواصفة 1111)، وتم تناوله في اتفاقيات دولية مثل اتفاقية الجرائم الإلكترونية و"الملاحظات التفسيرية" المرتبطة بها 12—للاستخدام بالترافق مع تعريف إساءة استخدام نظام اسم النطاق في منظمة ICANN.13 11.4. يجب على مجلس إدارة ICANN أن يعهد إلى اللجنة الاستشارية للأمن والاستقرار ومجموعة عمل الأمن العام بمهمة العمل مع خبراء الجريمة الإلكترونية وإساءة الاستخدام من أجل وضع تعريف لانتهاك نظام أسماء النطاقات DNS، مع الأخذ في الاعتبار العمليات والتعاريف الواردة في اتفاقية الجريمة الإلكترونية.		
12	**وضع آليات من أجل الوصول القانوني والمناسب إلى بيانات WHOIS** 12.1. يجب على مجلس إدارة ICANN وضع آليات قانونية ومناسبة من أجل الوصول إلى بيانات WHOIS عن طريق الأطراف المخولة بذلك مثل جهات إنفاذ القانون. 12.2. يجب على مجلس إدارة ICANN تولي المسئولة وأن يضمن أن تصل منظمة ICANN إلى إنهاء فوري وتنفيذ للمواصفة المؤقتة الخاصة ببيانات تسجيل gTLD.		عالية
13	**تحسين اكتمال واستغلال برنامج الإبلاغ عن أنشطة إساءة استخدام النطاقات** 13.1. يجب على مجلس إدارة ICANN ومنظمة ICANN العمل مع الجهات داخل وخارج مجتمع ICANN والتي تعمل على الحد من إساءة الاستخدام من أجل تحسين اكتمال واستغلال الإبلاغ عن نشاط انتهاك النطاق DAAR، وذلك من أجل تحسين كل من قياس إساءة استخدام النطاقات وتقديم التقارير حولها. 13.1.1. يجب على منظمة ICANN أن تنشر تقارير الإبلاغ عن نشاط انتهاك النطاق DAAR التي تحديد السجلات وأمناء السجلات التي تشارك نطاقاتهم أكثر في إساءة الاستخدام طبقًا لمنهجية الإبلاغ عن نشاط انتهاك النطاق DAAR. 13.1.2. يجب على منظمة ICANN إتاحة بيانات المصدر الخاص بالإبلاغ عن نشاط انتهاك النطاق DAAR من خلال مبادرة البيانات المفتوحة في ICANN وتحديد أولويات البنود ""daar وأيضًا "daar-summarized" لمستودع أصول بيانات مبادرة البيانات المفتوحة14 من أجل وصول المجتمع الفوري.		عالية

9 ويحدد تقرير فريق مراجعة المنافسة وثقة واختيار المستهلكين نفسه كل من إساءة استخدام نظام اسم النطاق وانتهاك أمن نظام أسماء النطاقات، مستشهدًا بالموافقة في الصفحة 8، الحاشية 11 من التعريفات التي احتوت على وثيقة فريق عمل ICANN المسماة "ضمانات ضد إساءة استخدام نظام اسم النطاق 18 يونيو/حزيران 2016". قامن مجموعة عمل المجتمع المعنية بسياسات إساءة استخدام التسجيل (RAP) في 2010 "بوضع تعريف بالإجماع لإساءة الاستخدام" نصه: إساءة الاستخدام هو إجراء: (أ) يتسبب في ضرر فعلي وموضوعي أو توقع مادي بالضرر، و(ب) إجراء غير قانوني أو غير شرعي أو يعتبر مخالفًا للهدف والتصميم ذي الغرض الشرعي المعلن عنه، إذا تم الإعلان عن هذا الهدف". (وقد جاء ذكر هذا التعريف بالموافقة في الصفحة 88، الحاشية 287 من التقرير النهائي لفريق مراجعة المنافسة وثقة واختيار المستهلكين)

10"مشورة اللجنة الاستشارية الحكومية GAC إلى ICANN: بيان بكين الختامي في اجتماع ICANN46، "آخر تعديل في 11 أبريل/نيسان 2013، https://gac.icann.org/contentMigrated/icann46-beijing-communique.

11 ICANN، "اتفاقية السجل"، https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm.

12المجلس الأوروبي، "اتفاقية حول الجرائم الإلكترونية"، ETS رقم 185 صفحة 7، في 23 نوفمبر/تشرين الثاني 2001، https://www.coe.int/en/web/cybercrime/the-budapest-convention.

13 انظر الملاحظة 50

14 راجع: https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv وفقًا لما هو منشور من جانب مكتب المسؤول الفني الرئيسي، والمتاح هنا: https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en.

	13.1.3. يجب على منظمة ICANN أن تنشر تقارير تشتمل على أنساق بيانات يمكن قراءتها آليًا، بالإضافة إلى بيانات رسومية في التقارير الحالية. 13.1.4. يجب على منظمة ICANN توفير المساعدة إلى مجلس الإدارة وجميع الدوائر ومجموعات أصحاب المصلحة واللجان الاستشارية في تفسير الإبلاغ عن نشاط انتهاك النطاق DAAR، بما في ذلك المساعدة في تحديد وتعريف السياسة والأنشطة الاستشارية التي تعزز من منع إساءة استخدام النطاقات والحد منها.		
14	**تمكين تحليل كمي صارم للعلاقة بين المدفوعات المقدمة لعمليات النطاق ودليل التهديدات الأمنية وإساءة الاستخدام.** 14.1. يجب على منظمة ICANN جمع وتحليل ونشر بيانات الأسعار من أجل تمكين المزيد دراسات أكثر استقلالية وتعقب العلاقة بين الأسعار وإساءة الاستخدام.		عالية
15	**تعزيز العقود المبرمة مع أمناء السجلات والسجلات من أجل الحث على الحد من انتهاك نظام أسماء النطاقات DNS** 15.1. يجب على منظمة ICANN جعل متطلبات الأمن والاستقرار والمرونة عند التعاقد أو تجديد الاتفاقيات الأساسية في الاتفاقيات المبرمة مع الأطراف المتعاقدة بما في ذلك اتفاقيات السجل (الأساسية أو الفردية) واتفاقيات اعتماد أمنا السجلات. ويجب أن تشتمل هذه المتطلبات التعاقدية على أحكام تحدد عتبات لإساءة الاستخدام (على سبيل المثال؛ 3% من جميع التسجيلات) التي قد تؤدي تلقائيًا إلى استعلامات تخص التوافق، مع عتبة أعلى (على سبيل المثال؛ 10% من جميع التسجيلات) عند تعتبر منظمة ICANN أن أمناء السجلات والسجلات قد أخلوا باتفاقاتهم. وقد أوصى فريق مراجعة المنافسة وثقة واختيار المستهلكين أيضًا بهذا النهج.[15] 15.2. يجب على منظمة ICANN طرح فقرة تعاقدية تؤيد فسخ التعاقد في حالة "نمط وممارسة" إساءة الاستخدام (كما في المادة 5.5.2.4 "المدة والإنهاء وفض النزاع" في اتفاقية اعتماد أمناء السجلات لسنة 2013)[16]. 15.3. ولدعم مراجعة هذه التغييرات التعاقدية، يجب على منظمة ICANN: 15.3.1. ضمان الوصول إلى بيانات التسجيل للأطراف ذوي الأغراض المشروعة من خلال الالتزامات التعاقدية وأصحاب آليات الامتثال القوية. 15.3.2. إقرار وإنفاذ متطلبات موحدة لخدمة بيانات المنطقة المركزية من أجل ضمان الوصول المستمر لأغراض أبحاث الأمن والاستقرار والمرونة. 15.3.3. جذب كل من نطاقات ccTLD ومنظمة ccNSO والتعاون معها من أجل تناول انتهاك نظام أسماء النطاقات DNS وتهديدات الأمان في نطاقات ccTLD. 15.3.4. يجب على مجلس إدارة ICANN والمجتمع والمنظمة العمل مع منظمة دعم أسماء رموز البلدان من أجل تطوير تعقب البيانات وإعداد التقارير بها، والوصول إلى انتهاك نظام أسماء النطاقات DNS وتهديدات الأمن في نطاقات ccTLD، ووضع خطة ccNSO من أجل دعم نطاقات ccTLD من أجل زيادة مستوى الحد من انتهاك نظام أسماء النطاقات DNS والتهديدات الأمنية. 15.3.5. الطرح الفوري لأمثلة المتطلبات الخاصة بخدمات بروتوكول الوصول إلى بيانات التسجيل الخاصة بالأطراف المتعاقدة من أجل إدراج مساحة عناوين منظمة ICANN في القائمة البيضاء ووضع عملية من أجل تدقيق الجهات الأخرى التي ستقوم خدمات بروتوكول الوصول إلى بيانات التسجيل الخاصة بالأطراف المتعاقدة بإدراجها في القائمة البيضاء لتحقيق الوصول بدون معدل محدد. 15.4. وعلى المدى الطويل، يجب على مجلس إدارة ICANN المطالبة بأن تبدأ منظمة دعم الأسماء العامة عملية من أجل اعتماد سياسات جديدة واتفاقيات مع الأطراف المتعاقدة من شأنها تحقيق تحسين مدروس للحد من انتهاك نظام أسماء النطاقات DNS والتهديدات		عالية

15 راجع التوصية 14 والتوصية 15 والتوصية 16 في "المنافسة وثقة المستهلك واختياره: التقرير النهائي،" https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

16 "اتفاقية اعتماد أمناء السجلات لسنة 2013"، ICANN، على https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

	الأمنية، بما في ذلك إجراء تغييرات على بروتوكول الوصول إلى بيانات التسجيل ومعلومات المسجل، وحوافز من أجل الأطراف المتعاقدة إزاء الحد من إساءة الاستخدام/التهديدات الأمنية، وإقرار إطار عمل من أجل مؤشرات الأداء، وتأسيس تدريب وعمليات توثيق للأطراف المتعاقدة وأصحاب المصلحة الأساسيين.		
16	**استحداث حوافز سعرية للأطراف المتعاقدة من أجل الحد من إساءة الاستخدام والتهديدات الأمنية** 16.1. يجب على منظمة ICANN تحفيز الحد من إساءة الاستخدام والتهديدات الأمنية من خلال إجراء التغييرات التالية على العقود: 16.1.1. الأطراف المتعاقدة ذات المهام الأقل من نسبة محددة (أي 1%) من أسماء النطاقات المخالفة (وفقًا لما يحدده موفرو الخدمات التجاريون أو الإبلاغ عن نشاط انتهاك النطاق DAAR) يجب أن يحصلوا على تخفيض مجاني (أي تخفيض من الرسوم الحالية، أو زيادة في الرسوم المعاملات الحالية على كل اسم نطاق وتوفير خصم لأمناء السجلات). 16.1.2. يجب أن يحصل أمناء السجلات على خصم مجاني على كل اسم نطاق يتم تسجيله لمسجل موثق حتى عتبة مناسبة. 16.1.3. التنازل عن رسوم سياسة تقييم خدمات السجل عندما تشير ملفات سياسة تقييم خدمات السجل المقدمة بوضوح إلى كيفية اعتزام الطرف المتعاقد الحد من انتهاك نظام أسماء النطاقات DNS، وأن تتلقى أي سياسة تقييم خدمات خاصة بالسجل موافقة مسبقة إذا ما كانت تسمح بحقل لبروتوكول التزويد المرن في مستوى السجل من أجل تعيين أسماء النطاقات تلك الواقعة قيد إدارة أي مسجل موثق. 16.1.4. إعادة ورد الرسوم المستحصل عليها من أمناء السجلات والسجلات على النطاقات التي تحديدها بأنها مسيئة للاستخدام وبها تهديدات أمنية مع تعطيلها في حدود الفترة الزمنية المناسبة بعد عملية التسجيل (على سبيل المثال؛ بعد 30 يومًا من تسجيل النطاق). 16.2. بالنظر إلى أن جميع الأطراف (منظمة ICANN والأطراف المتعاقدة وغيره من أصحاب المصلحة الأساسيين مثل السجلات وأمناء السجلات وموفري خدمات الخصوصية/البروكسي وموفري خدمة الإنترنت والأطراف المتعاقدة) يجب عليهم فهم كيفية قياس وتعقب واكتشاف وتحديد الإبلاغ عن نشاط انتهاك النطاق DAAR تحديدًا دقيقًا، يجب على منظمة ICANN وضع الأسس لعملية التدريب والتوثيق لجميع الأطراف في النواحي المحددة من خلال الإبلاغ عن نشاط انتهاك النطاق DAAR وغيرها من المصادر الخاصة بالطرق الشائعة لإساءة الاستخدام [يجب إضافة اقتباس] وكيفية تأسيس الجهود المناسبة للحد منها. يجب أن تشتمل عملية التدريب على نقطة بدء: التعقب التلقائي للأرقام المتوافقة ومعالجة الشكاوي؛ التقارير العامة السنوية/ربع السنوية حول الشكاوى والقضايا؛ والتحليل.		عالية
17	**تأسيس بوابة مركزية لتقارير إساءة الاستخدام** 17.1. يجب على منظمة ICANN تأسيس واستحداث بوابة مركزية لشكاوى انتهاك نظام أسماء النطاقات DNS توجه جميع تقارير إساءة الاستخدام تلقائيًا إلى الأطراف المعنية. على أن يعمل النظام بشكل مجرد عمل التدفق الداخلي، مع تدفق الملخصات والبيانات الكبيرة للخارج. يجب أن يكون استخدام النظام إلزاميًا لجميع نطاقات ccTLD، ويجب دعوة نطاقات gTLD للانضمام. يجب أن تكون الردود قابلة للبحث أمام الجمهور وتضمينها في التقارير السنوية (بصيغة كاملة، أو عن طريق الإشارة إليها). بالإضافة إلى ذلك، يجب إتاحة التقارير (على سبيل المثال؛ عن طريق البريد الإلكتروني) أمام نطاقات ccTLD غير المشاركة.		عالية
18	**ضمان أن أنشطة إدارة الامتثال في ICANN محايدة وفعالة** 18.1. يجب على منظمة ICANN إخضاع أنشطة الامتثال للتدقيق الخارجي وضبطها وفق أعلى المعايير. 18.2. ويجب على مجلس إدارة ICANN تمكين إدارة الامتثال من الاستجابة للشكاوى ومطالبة إدارة الامتثال بالبدء في تحريات وإنفاذ الالتزامات التعاقدية ضد من يقدمون الدعم والمغريات لإساءة الاستخدام المتكررة، وفقًا لما هو محدد في اتفاقية مستوى الخدمة. ويكن		عالية

	أن تشتمل هذه الصلاحية الإضافية على دعم لإجراءات تدريجية حول تصعيد تدابير الإنفاذ والإجراءات المناسبة القابلة للتنفيذ مما يمكن لمنظمة ICANN استخدامه من أجل الرد على أي تقاعس في تصحيح مخالفات الامتثال ضمن أطر زمنية محددة. 18.3. يجب على إدارة الامتثال في ICANN -كقاعدة عامة لهم- إشراك اتفاقيات مستوى الخدمة عند الإنفاذ وإعداد التقارير والعمليات الواضحة وذات الكفاءة، والمدعي المستنير بالكامل والإرضاء القابل للقياس والحد الأقصى من الإفصاح العام.		
19	**تحديث التعامل مع عمليات التسمية المخالفة** 19.1. يجب على منظمة ICANN بناء الأنشطة الحالية من أجل التحري عن عملية التسمية النموذجية المضللة، بالتعاون مع باحثين وأصحاب مصلحة، متى ما كان ذلك عمليًا. 19.2. وعند ظهور أعمال التسمية المضللة في مستوى التسمية المسيئة، يجب على منظمة ICANN تضمين هذا النوع من إساءة الاستخدام في عملية الإبلاغ عن نشاط انتهاك النطاق DAAR ووضع سياسات وأفضل ممارسات من أجل الحد منها. 19.3. يجب على منظمة ICANN نشر عدد شكاوى التسمية المسيئة التي تم تقديمها في البوابة بصيغة وطريقة تتيح لأطراف أخرى مستقلة القدرة على تحليل الضرر الحادث من استخدام أسماء النطاقات تلك والحد منها ومنعها. 19.4. يجب على منظمة ICANN تحديث "إرشادات تنفيذ أسماء النطاقات المدوّلة IDN" الحالية [يجب إضافة اقتباس] من أجل تضمين قسم يخص الأسماء التي تحتوي على علامات تجارية وسلاسل نطاق المستوى الأعلى واستخدام أخطاء إملائية (صعبة الاكتشاف). وعلاوة على ذلك، يجب على ICANN إنفاذ "إرشادات تنفيذ أسماء النطاقات المدوّلة IDN" إنفاذًا تعاقديًا لنطاقات gTLD والتوصية بأن تقوم نطاقات ccTLD نفس الشيء.		عالية
20	**إكمال وضع وتطوير اختبار لارتداد نظام أسماء النطاقات** 20.1. يجب على منظمة ICANN إكمال وضع وتطوير حزمة لاختبار لارتداد نظام أسماء النطاقات.[17] 20.2. يجب على منظمة ICANN ضمان تنفيذ أداء الاختبارات الوظيفية لمختلف التكوينات وإصدارات البرامج والحفاظ عليها.		عالية
21	**تنفيذ التوصيات من التقريرSAC063 والتقرير SAC073 ووضع إجراءات رسمية لوحدات حل التصديق الأساسية** 21.1. يجب على منظمة ICANN تنفيذ التوصيات المقدمة من SAC063 ومن SAC073 من أجل ضمان الأمن والاستقرار والمرونة لعملية وحدات حل التصديق لمفتاح توقيع شفرة الدخول الأساسية. 21.2. يجب على منظمة ICANN وضع إجراءات رسمية، تدعمها أداة ولغة نمذجة لعمليات رسمية[18] من أجل تحديد تفاصيل وحدات حل التصديق الأساسية المستقبلية، والتي تشمل نقاط اتخاذ القرارات، ودعامات الاستثناء، والتدفق بالتحكم الكامل، إلخ. ويجب أن يشتمل توثيق عملية وحدة حل تصديق المفتاح على نشر إجراءات برمجية (على سبيل المثال؛ برنامج أو FSM) للتعليق العام، ويجب ضم تعقيبات وآراء المجتمع في ذلك. يجب أن تحتوي العملية على معايير قبول موثقة تجريبيًا في كل مرحلة، ويجب إنجاز ذلك لكي تستمر العملية. ويجب إعادة تقييم هذه العملية بنفس معدل عملية التبديل نفسها على الأقل (أي بنفس المعدل الدوري) بحيث يمكن استخدام الدروس المستفادة من أجل تعديل العملية.		عالية

17 "مختبر وحدة حل التصديق"، مستودع GitHub في ICANN على https://github.com/icann/resolver-testbed.

18 التحليل التأكيدي لتحسين خصائص المفتاح للعمليات الحيوية المحفزة بشريًا: مثال على أمن الانتخابات، ليون جيه أوستروبل، مات بيشوب، هيذر كونبوي، هيونغ غان، بوريسلافا آي سيميدشيفا، جورج أفرونين، لوري أيه كلارك، شون بيزيرت، معاملات ACM حول الخصوصية والأمن (TOPS) مجلد 20، رقم 2، مايو/أيار 2017، الصفحات 1:5-31. (UM-CS-2016-012)

	21.3. يجب على منظمة ICANN إنشاء مجموعة من أصحاب المصلحة تضم الموظفين المعنيين (من منظمة ICANN أو من المجتمع) من أجل إجراء دوري لتدريبات عليا من شأنها متابعة عملية تبديل مفتاح توقيع شفرة الدخول الأساسية للجذر.		
22	**إقرار ممارسات أساسية للأمن من أجل مشغلي خادم ملف الجذر وعملياته** 22.1. يجب على منظمة ICANN -بالتعاون مع اللجنة الاستشارية لنظام خادم الجذر وغيرها من أصحاب المصلحة المعنيين- ضمان أن نموذج حوكمة نظام خادم الجذر وفقًا لمقترح التقرير RSSAC037 يشتمل على أفضل ممارسات الأمان الأساسية لمشغلي وعمليات خوادم الجذر من أجل الحد من مخاطر الأمن والاستقرار والمرونة المرتبطة بعمل وتشغيل خادم الجذر. ويجب أن تشتمل أفضل الممارسات على إدارة التغييرات وإجراءات التوثيق وإجراءات فحص السلامة. 22.2. يجب على منظمة ICANN أيضًا وضع مؤشرات الأداء الأساسية (KPI) ذات الصلة من أجل قياس مستوى تنفيذ هذه الممارسات والمتطلبات المثلى لضمان الإبلاغ العام سنويًا حول الكيفية التي يمكن لمشغلي خادم ملف الجذر (RSO) وغيرهم من الأطراف المعنية، بما في ذلك منظمة ICANN، من استيفاء وتحقيق مؤشرات الأداء الأساسية (KPI) هذه. 22.3. يجب على منظمة ICANN توثيق استراتيجيات التدريب الخاصة بخادم الجذر المدار بمعرفة ICANN (IMRS أو)، المعروفة عمومًا بلفظ جذر-L، ويجب تشجيع مشغلي خوادم الجذر الآخرين على القيام بنفس الشيء. 22.4. يجب على منظمة ICANN ضمان أن خادم الجذر المدار بمعرفة ICANN يستخدم عملية للإفصاح عن الثغرات الأمنية (وليس أمام الجمهور بالضرورة) وتقارير ومعلومات الأمن والتواصل مع الباحثين ونصائح أو توصيات اللجنة الاستشارية لنظام خادم الجذر، متى ما كان ذلك منطبقًا.		عالية
23	**الإسراع بتنفيذ نظم إدارة ملفات خوادم الجذر من الجيل الجديد** 23.1. يجب على عمليات ICANN وهيئة المُعرّفات الفنية العامة الإسراع بتنفيذ تدابير أمنية جديدة بنظام إدارة ملفات خوادم الجذر فيما يخص توثيق وترخيص التغييرات المطلوبة. 23.2. يجب على منظمة ICANN إطلاق تعليقات عامة بأسرع ما يمكن على التغييرات فيما يخص المراجعات التي تجرى على سياسات نظم إدارة ملفات خوادم الجذر.		عالية
24	**إنشاء قائمة بالإحصائيات والمؤشرات التي تدور حول الحالة التشغيلية لنظم المعرّفات الفريدة** 24.1. يجب على منظمة ICANN استحداث قائمة بالإحصائيات والمؤشرات التي تعكس الحالة التشغيلية (مثل التوافر والقدرة على الاستجابة) لكل نوع من معلومات المعرّفات الفردية، مثل الخدمة ذات الصلة بمنطقة الجذر، وسجلات هيئة الإنترنت للأرقام المخصصة وأي من خدمات gTLD التي تحظى منظمة ICANN بسلطة الإشراف عليها. 24.2. ويجب على منظمة ICANN نشر دليل بهذه الخدمات ومجموعات البيانات والمؤشرات على صفحة فردية بموقع منظمة ICANN على الويب، مثل ما يكون قيد منصة البيانات المفتوحة. 24.3. يجب على ICANN نشر ملخصات سنوية وطولية بهذه البيانات، وطلب الحصول على التعقيبات والآراء العامة على المخلصات، وضم التعليقات والآراء من أجل تحسين التقارير المستقبلية. 24.4. وبالنسبة لكل مجموعتي مؤشرات الأداء الأساسية (KPI)، يجب على منظمة ICANN تقديم ملخصات حول كل من العام السابق وطوليًا، وطلب ونشر ملخص بتعقيبات وآراء المجتمع حول كل تقرير وضم هذه التعقيبات من أجل تحسين تقارير المتابعة.		متوسطة
25	**ضمان أن الوصول المركزي إلى بيانات ملف المنطقة متاح بشكل متسق**		عالية

	25.1. يجب على مجتمع ICANN ومنظمة ICANN اتخاذ خطوات من أجل ضمان أن الوصول إلى خدمة بيانات المنطقة المركزية بالإضافة إلى البيانات الأخرى متاحًا، وفي الوقت المناسب ودون أي عراقيل غير ضرورية أمام الطالبين. 25.2. يجب على منظمة ICANN تنفيذ التوصيات الأربعة الواردة في التقرير SSAC 97:[19] "التوصية رقم 1: توصي اللجنة الاستشارية للأمن والاستقرار بأن يقترح مجلس إدارة ICANN على فريق عمل ICANN النظر في مراجعة نظام خدمة بيانات المنطقة المركزية من أجل تناول مشكلة الاشتراكات التي تنتهي من تلقاء نفسها افتراضيًا، على سبيل المثال، من خلال السماح لعمليات الاشتراك بالتجديد تلقائيًا بشكل افتراضي. ويمكن أن يشتمل ذلك على خيار يسمح لمشغل السجل الانتقال من الوضع الافتراضي وفقًا لكل مشترك، ومن ثم يجبر المشترك الذي يقع عليه الاختيار على إعادة التقدم في نهاية المدة الحالية. يجب أن تواصل خدمة بيانات المنطقة المركزية توفير القدرة لمشغلي السجلات على الإنهاء الواضح لوصول المشترك المسبب للمشكلات في أي وقت. التوصية رقم 2: توصي اللجنة الاستشارية للأمن والاستقرار بأن يقترح مجلس إدارة ICANN على فريق عمل ICANN ضمان والتأكد بأن تتوافق اتفاقية الاشتراك في خدمة بيانات المنطقة المركزية في الجولات التالية من نطاقات gTLD الجديدة التوافق مع ما يتم تنفيذه من تغييرات نتيجة تنفيذ التوصية 1. التوصية رقم 3: توصي اللجنة الاستشارية للأمن والاستقرار بأن يقترح مجلس إدارة ICANN على فريق العمل البحث عن طرق لتقليل عدد شكاوى الوصول إلى ملف المنطقة، والبحث عن طرق لحل الشكاوي في الوقت المناسب. التوصية رقم 4: توصي اللجنة الاستشارية للأمن والاستقرار بأن يقترح مجلس إدارة ICANN على فريق عمل ICANN ضمان أن الوصول إلى ملف المنطقة وإحصائيات استعلامات WHOIS القائمة على الويب يتم الإبلاغ عنها بدقة وبشكل عام، طبقًا للمعايير المحددة تحديدًا جيدًا والتي يمكن تجميعها بشكل موحد من خلال جميع مشغلي سجلات gTLD. يجب توضيح مؤشر الوصول إلى ملف الجذر (ZFA) بأسرع ما يمكن من الناحية العملية.		
26	**توثيق وتحسين واختبار عمليات مشغل سجل دعم الطوارئ EBERO** 26.1. يجب على منظمة ICANN أن تقوم بتوثيق عام لعمليات مشغل سجل دعم الطوارئ EBERO، بما في ذلك نقاط القرارات والإجراءات والتوقعات. ويجب أن تصف الوثيقة أوجه التداخل بالنسبة لكل قرار وإجراء وتوقع. 26.2. ومتى ما كان ذلك ممكنًا، يجب على منظمة ICANN أتمتة هذه العمليات واختبارها سنويًا. 26.3. يجب على منظمة ICANN إجراء اختبار تشغيلي عام لمشغل سجل دعم الطوارئ EBERO وفقًا لفترات بينية مقررة مسبقًا من خلال استخدام خطة اختبار منسقة مع الأطراف المتعاقدة مع ICANN مقدمًا وذلك لضمان أن جميع قوائم الاستثناءات تمت ممارستها ونشر النتائج. 26.4. يجب على منظمة ICANN تحسين العملية من خلال السماح لوكيل ضمان بيانات gTLD بإرسال مستودع ضمان البيانات مباشرة إلى موفر تشغيل سجل دعم الطوارئ EBERO.		عالية

[19] اللجنة الاستشارية للأمن والاستقرار التابعة لـ ICANN، التقرير "SAC097: نصيحة اللجنة الاستشارية للأمن والاستقرار فيما يخص خدمة بيانات المنطقة المركزية (CZDS) وتقارير النشط الشهري لمشغل السجل"، 12 يونيو/حزيران 2017، https://www.icann.org/en/system/files/files/sac-097-en.pdf.

27	**تحديث DPS وبناء الإجماع حول وحدات حل التصديق لخوارزمية DNSKEY** 27.1. يجب أن تقوم عمليات هيئة المُعرّفات الفنية العامة بتحديث DPS من أجل تسهيل الانتقال من خوارزمية توقيع رقمية واحدة إلى أخرى، بما في ذلك الانتقال المتوقع من خوارزمية توقيع رقمية بنظام RSA إلى ECDSA أو إلى خوارزميات مستقبلية ما بعد الكم، وهو ما سيستحدث نظام DNS أكثر مرونة مع توفير نفس المستوى العالي من الأمن في نفس الوقت. 27.2. وبما أن وحدة حل المصادقة لخوارزمية DNSKEY الخاصة بالجذر عبارة عن عملية معقدة وحساسة للغاية، يجب أن تركز عمليات هيئة المُعرّفات الفنية العامة على شركاء آخرين في منطقة الجذر وعلى المجتمع العالمي في وضع خطة بالإجماع من أجل وحدات حل مصادقة خوارزمية DNSKEY المستقبلية للجذر، مع الأخذ في الاعتبار الدروس المستفادة من وحدة حل مصادقة مفتاح توقيع شفرة الدخول الأساسية للجذر الأولى في 2018.		متوسطة
28	**وضع تقرير حول وتيرة قياس تضارب الأسماء واقتراح حل** 28.1. يجب أن تقدم منظمة ICANN نتائج تصف طبيعة ووتيرة تضارب الأسماء والمخاوف المرتبة عليها. ويجب على مجتمع ICANN تنفيذ حل قبل الجولة التالية من نطاقات gTLD. 28.2. ويجب على منظمة ICANN تسهيل هذه العملية من خلال البدء في دراسة مستقلة حول حالات تضارب الأسماء وصولاً إلى الإكمال النهائي واعتماد أو احتساب التنفيذ أو عدم الاعتماد لأي من التوصيات الناجمة عن ذلك. ويقصد فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات بكلمة "مستقلة" أنه يجب على منظمة ICANN ضمان عمل مجموعة العمل المعنية بمشروع تحليل تضارب الأسماء (NCAP) في اللجنة الاستشارية للأمن والاستقرار ببحث وتقديم تقارير حول تقييم نتائج الفريق التي يجب تفويضها من خلال الأطراف التي ليس لها أي مصلحة مالية في توسيع نطاق المستوى الأعلى. 28.3. يجب على منظمة ICANN تمكين المجتمع من الإبلاغ عن حالات تضارب الأسماء. ويجب أن تتيح هذه التقارير القدرة على التعامل المناسب مع البيانات الحساسة والتهديدات الأمنية ويجب نشرها واستخدامها في مؤشرات تقارير المجتمع.		متوسطة
29	**التركيز على مقاييس الخصوصية والأمن والاستقرار والمرونة وتحسين السياسات استنادًا إلى تلك المقاييس** 29.1. يجب على منظمة ICANN مراقبة تأثير الخصوصية على تقنيات مثل DoT (أي نظام أسماء النطاقات عبر أمان طبقة النقل) وDoH (أي نظام أسماء النطاقات عبر HTTPS) وتقديم تقارير دورية بشأنها. 29.2. يجب أن تحتوي سياسات الإجماع والاتفاقيات المبرمة مع مشغلي السجلات وأمناء السجلات -لهذا السبب- على مواد تعكس الامتثال لهذه مع ضمان عدم تقسيم نظام أسماء النطاقات بسبب الحاجة إلى الحفاظ على/تنفيذ الحد الأدنى من المتطلبات التي تحكم جمع وحفظ وتخزين ونقل وعرض بيانات التسجيل، والتي تشتمل على معلومات الاتصال الخاصة بالمسجل وبيانات الاتصال الإدارية والفنية بالإضافة إلى المعلومات الفنية المرتبطة بأي اسم نطاق. 29.3. يجب على منظمة ICANN: 29.3.1. استحداث وحدات متخصصة داخل إدارة الامتثال التعاقدي تركز علمها على متطلبات ومبادئ الخصوصية (مثل حدود التحصيل، ومؤهلات البيانات، وتحديد الأغراض، والضمانات الأمنية المقدمة للإفصاح) والتي يمكن أن تسهل احتياجات جهات إنفاذ القانون بموجب إطار عمل بروتوكول الوصول إلى بيانات التسجيل المتطور. 29.3.2. مراقبة تشريعات الخصوصية ذات الصلة والمتطورة (على سبيل المثال؛ CCPA والتشريعات التي تحمي المعلومات المحددة لهوية أصحابها (PII)) وضمان أن سياسات		عالية

	وإجراءات منظمة ICANN متوافقة وممتثلة لمتطلبات الخصوصية وحماية البيانات المحددة لهوية أصحابها وفقًا لاشتراطات التشريعات والقوانين ذات الصلة.[20] 29.3.3. وضع وتحديث سياسة من أجل حماية المعلومات المحددة لهوية أصحابها. يجب إيصال ونشر السياسة إلى جميع الأشخاص المشاركة في معالجة البيانات المحددة لهوية أصحابها. يجب تنفيذ تدابير فنية وتنظيمية من أجل توفير الحماية المناسبة للمعلومات المحددة لهوية أصحابها. 29.3.4. إجراء عمليات تدقيق دورية لمدى الالتزام بسياسات الخصوصية التي ينفذها أمناء السجلات لضمان أن لديهم -على أقل تقدير- الإجراءات المفعلة من أجل التعامل مع خروقات الخصوصية. 29.4. كما يجب أن يكون مسئول حماية البيانات في منظمة ICANN مسئولاً عن المعلومات المحددة لهوية أصحابها الخارجية في نظام أسماء النطاقات. ويجب على مسئول حماية البيانات توفير الإرشادات إلى المديرين وأصحاب المصلحة فيما يخص المسئوليات والإجراءات ومراقبة التطورات الفنية ذات الصلة وتقديم تقرير حولها.		
30	**الاطلاع دائمًا على آخر مستجدات الأبحاث الأكاديمية لمشكلات الأمن والاستقرار والمرونة واستخدام تلك المعلومات من أجل الاستفادة بها في مداولات السياسات** 30.1. يجب على منظمة ICANN تعقب التطورات التي تحدث في مجتمع الأبحاث في ذات المجال، مع التركيز على المؤتمرات المعنية بأعمال الشبكات وأبحاث الأمن، بما في ذلك على أقل تقدير ACM CCS، ومؤتمر قياس الإنترنت ACM، وأمن Usenix، وCCR وSIGCOMM وIEEE S&P، بالإضافة إلى APWG لمؤتمرات الأمن التشغيلي، ومجموعة العمل المختصة بالرسائل والبرمجيات الخبيثة وإساءة استخدام الهواتف النقّالة وFIRST، مع نشر تقرير لمجتمع ICANN يتم فيه تلخيص تأثيرات المنشورات ذات الصلة بمنظمة ICANN أو سلوك الأطراف المتعاقدة. 30.1.1. ويجب أن تشتمل هذه التقارير على توصيات من أجل الإجراءات، والتي تشمل إجراء تغييرات على العقود المبرمة مع السجلات وأمناء السجلات، والتي يمكن أن تحد أو تمنع أو تصحح أضرار الأمن والاستقرار والمرونة للمستهلكين والبنية التحتية المحددة في المنشورات التي يراجعها الأقران. 30.1.2. ويجب أن تشتمل هذه التقارير كذلك على توصيات من أجل إجراء دراسة إضافية لتأكيد النتائج التي يقوم الأقران على مراجعتها، ووصف لطبيعة البيانات التي قد تكون مكتوبة من أجل تنفيذ الدراسات الإضافية الموصى بها، والطريقة التي يمكن لـ ICANN بها مساعدة السمسار في الوصول إلى تلك البيانات، على سبيل المثال؛ خدمة بيانات المنطقة المركزية.		متوسطة
31	**توضيح تأثيرات الأمن والاستقرار والمرونة لنظام DNS-عبر-HTTP** 31.1. يجب على منظمة ICANN إطلاق تحري (تحريات) مستقلة حول التأثيرات ذات الصلة بالأمن والاستقرار والمرونة لاتجاهات نشر DoH، بالإضافة إلى تأثيرات الدور المستقبلي لهيئة الإنترنت للأرقام المخصصة في منظومة الإنترنت. وتتمثل النتيجة المرجوة من ذلك في ضمان حصول جميع أصحاب المصلحة على فرصة فهم التأثيرات ذات الصلة بالأمن والاستقرار والمرونة على هذه التطورات، ونطاق البدائل (أو نقصها) التي يحظى بها مختلف أصحاب المصلحة من أجل التأثير على المستقبل.		عالية

[20] إن فريق المراجعة على دراية بميثاق منظمة ICANN الذي يحدد أسلوبًا للمشاركة الحكومية https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf and التقرير التشريعي (وحدة التعقب) .https://www.icann.org/legislative-report-2019 وعلى الرغم من ذلك فإننا نود إجراء المزيد من التركيز المحدد على الخصوصية وعلى حماية البيانات.

إرشادات من أجل فرق مراجعة الأمن والاستقرار والمرونة المستقبلية - الدروس المستفادة

لكي يتم السماح بعمليات تقييم أكثر استقامة من جانب فرق مراجعة الأمن والاستقرار والمرونة في المستقبل، سوف يسعي فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات جاهدًا لصياغة التوصيات الخاصة به بما يتفق مع معايير SMART: ومتى ما كان ذلك ممكنًا، سوف تكون التوصيات محددة وقابلة للقياس وقابلة للتخصيص وذات صلة وقابلة للتعقب. ويرى فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات أن التوصيات الأكثر وضوحًا والموجهة بالإجراءات من شأنها تبسيط التنفيذ والتعقب وعملية التقييم التي يتم تنفيذها من خلال مراجعة الأمن والاستقرار والمرونة التالية. وقد قام فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات بتضمين معلومات إضافية حول العملية والمنهجية التي استخدمها فريق المراجعة الثانية لأمن واستقرار ومرونة نظام أسماء النطاقات في تنفيذ مهمته في "الملحق "ج":العملية والمنهجية."
