18.03.2020

# Nominet Response 2019 .UK Policy Consultation

## Overview

Since 1996 Nominet has operated at the heart of the UK's internet community as the .UK domain name registry.

As the environment in which we operate evolves, we actively engage with a wide variety of UK stakeholders to ensure that the policies we maintain reflect emerging threats, changes in stakeholder expectations and new industry practices. This ensures that .UK provides a platform for innovation and remains a competitive and trusted space for businesses and consumers.

Our 2019 .UK consultation ran from 9 October – 16 December 2019, covering three issues:

I. Reducing the use of .UK domain names for phishing attacks

II. Implementing law enforcement landing pages following suspensions for criminal activity

III. Implementing a .UK drop list to provide a transparent and orderly process for the re-registration of expired domains

Ensuring .UK policies reflect current expectations of the UK internet community is an ongoing process of continuous improvement. We therefore also included a forward-looking roadmap and invited stakeholders to submit issues of interest for consideration in future .UK policy discussions.

We held an open stakeholder roundtable on 4 December in London which was attended by 14 people. The slides are available to view on our website.

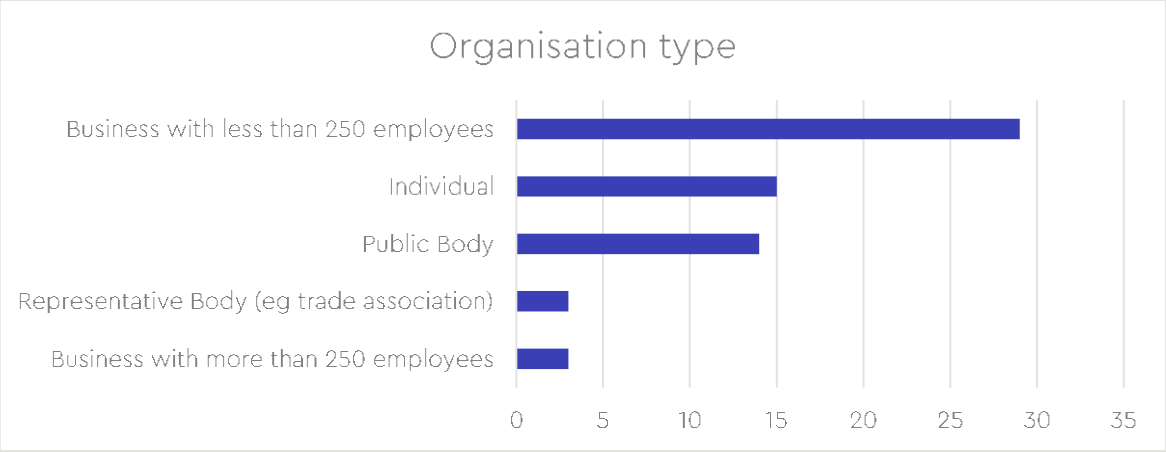
This document sets out a summary of the responses, our comments and next steps.

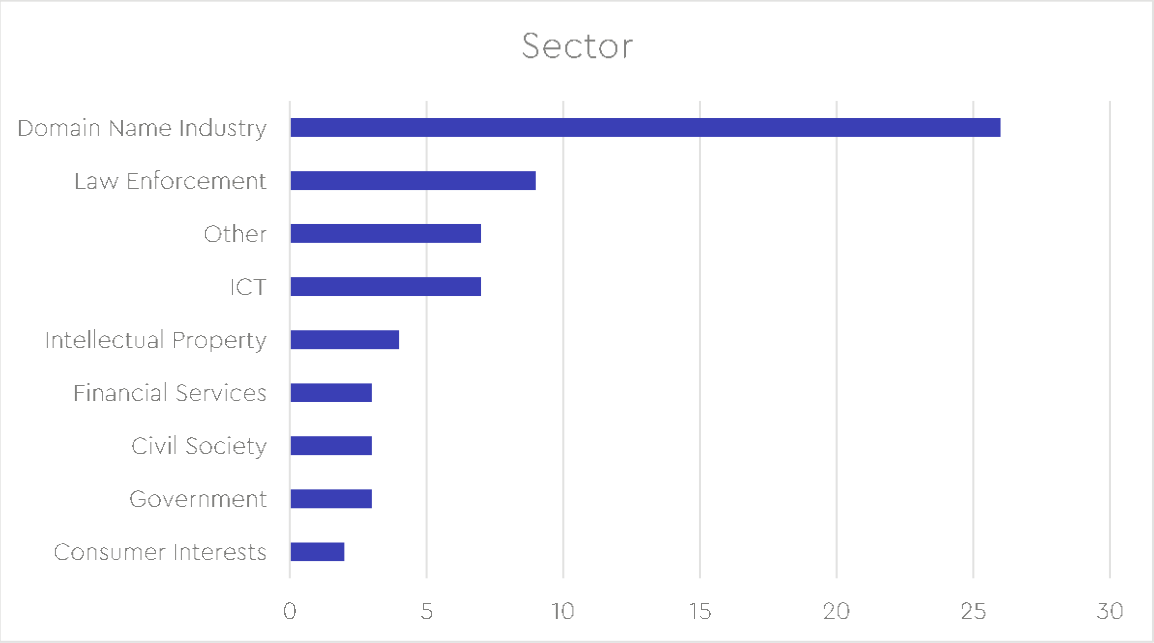
## Responses

We received 64 responses from a variety of individuals and organisations. The questions were optional, not all respondents answered every question. We heard from a wide range of organisations and sectors.

Most responses came from the domain industry. We also received input from the UK government Department for Digital, Culture, Media and Sport (DCMS), and related organisations such as the Intellectual Property Office and the National Cyber Security Centre (NCSC), law enforcement agencies, the intellectual property sector, consumer interest organisations, the financial sector and civil society.

We believe open consultation creates better policies and would like to thank those who provided responses and attended our roundtable.



## Phishing

### Background

We want to ensure our policies enable us to effectively address phishing in .UK, in response to the evolving threats landscape. We summarised our current Domain Watch initiative and asked respondents to consider the following questions:

1. Do you agree that we should update our policies to specifically allow us to prevent resolution in the DNS where we have identified a high risk of phishing use? [y/n] If no, why not? [freetext]

2. Do you have any other suggestions or thoughts as to how phishing may be prevented and/or mitigated in .UK? [freetext]

3. What other security threats should Nominet prioritise as part of our commitment to a secure and trusted .UK namespace, and reduce cybercrime in the UK? [freetext]

### Responses

In response to the first consultation question, almost all respondents (97%, 36/37) agreed with our proposal to update our policies to specifically allow us to prevent resolution in the DNS where we have identified a high risk of phishing. Some respondents emphasised the importance of being able to respond quickly and pre-emptively where phishing is concerned, for example:

- *"If there is a high risk that a domain is being used for phishing and scamming consumers, then a quick response to prevent people accessing the site will be the most effective way to protect consumers."* **Consumer Interests Body**

Another respondent emphasised that the scale of the challenge requires action to reduce the burden on end users:

- *"Phishing remains the most common attack vector used by cyber criminals. Given the scale of phishing attacks in the UK it is not sufficient to solely rely on the user to identify and manage all phishing attacks. It is only through the interventions of organisations such as Nominet that the impact of phishing on the UK can be meaningfully tackled. DCMS therefore fully supports Nominet's intention to change its policy to allow for greater discretion in identifying and disrupting .UK domains suspected to be at risk from phishing activities."* **Central Government Department**

In relation to the second question, almost all respondents indicated that phishing is a live issue which needs a robust response from the registry. Domain Watch was positively received by almost all stakeholders, and respondents generally encouraged Nominet to be more proactive, to develop and expand Domain Watch in order to increase the number of phishing domains pre-emptively

blocked at the point of registration, and to collaborate across the industry to raise standards globally.

Example responses included:

- *"Collaboration between worldwide ccTLD's which view enforcement in a similar way would be very useful. This would allow a joint approach to terminate domains with similar modus operandi behaviours that are targeting other domains trees but will also work in tandem with the .UK strategy. This will effectively assist information sharing and strengthen approaches throughout the internet in combatting illicit activities."* **Law Enforcement Agency**
- *"We work a little differently compared to most registrars and we've seen a decrease in fraudulent registrations over the last 2 years. We actually delete domains identified for phishing in AGP [Add Grace Period], so that we can refund the fraudulent payment method to avoid chargebacks and to ensure the victim is refunded. It's great to tackle abuse as a registry too and I think Nominet do a wonderful job."* **Domain Name Industry**
- *"To really protect consumers from phishing, collaboration between Nominet and other domain name registries will be important. While Nominet may be able to take actions to clean up phishing in the .UK space, scammers can simply use domain names in other registries to continue scamming consumers. Ideally, a longer term solution would involve similar measures being taken across all (or at least many) domain name registries to have a broader impact on stamping out phishing scams."* **Consumer Interests Body**
- "DCMS would encourage Nominet to consider how they might continue to evolve such interventions, such as exploring potential mechanisms to identify phishing activity on .uk domains that are already registered. It is also important that Nominet continues to engage with law enforcement agencies, including the National Crime Agency." **Central Government Department**

Some respondents also suggested training and compliance measures for registrars, in order to spread awareness of the issue and promote best practices to the wider industry:

- *"Better training for registrars and hosting providers to deal with issues around abuse to prevent/mitigate abuse in .UK."* **Domain Name Industry**
- *"Make it tougher on Registrars who register the sites to ensure they carry out the correct Due Diligence."* **Manufacturing Business**

Several registrars requested access to information to help them investigate:

- *"As a registrar it would be very helpful for us to see more of the data that Nominet has. Perhaps 'near-miss' registrations where it scores highly but not high enough to be blocked could be highlighted to the registrar via EPP."* **Domain Name Industry**
- *"Highlight or warn where a domain is set to nameservers that do not resolve or where the nameservers are set to a domain that doesn't exist or is expired."* **Domain Name Industry**

- *"Sending reports to the registrar immediately after receiving information that phishing may be occurring, in case they have not found out via other means. Not all registrars may be able to do anything other than contact the customer, but as some may also be the website host, they may be able to take more immediate action to stop the phishing."* **ICT Business**

One respondent suggested Domain Watch could include the option for brands to purchase "phishing protection". The issue was discussed further at our roundtable, and there appeared to be some concerns with this in terms of the criteria that would be used, and how this would work in practice, and whether human rights and free speech would be impacted.

## Nominet comments

This consultation demonstrated very broad support across the UK internet community for Nominet to take a more proactive role in addressing and preventing phishing. It was clear from our interactions with stakeholders that addressing phishing is a high priority but there are no easy or straightforward solutions.

We will now build on our Domain Watch initiative and explore what further action we can take to prevent and address phishing. To allow us to act quickly at the point of registration we will update our Terms and Conditions to specifically give us the powers to pre-emptively block domains which appear to indicate a high risk of phishing.

We agree that preventing and addressing phishing requires collaboration with registrars, the law enforcement community and the global domain industry. We will therefore undertake research and test ideas in collaboration with UK law enforcement and other Top Level Domain registries to determine the most effective ways to prevent and address phishing in .UK without disrupting the vast majority of legitimate registrants, some of whom may have their domain names compromised by malicious third parties.

We were impressed with the proactive approach some registrars are taking to prevent and address phishing. We would like to ensure that all registrars are equipped and motivated to address abuse and security threats in domains under their management.

To meet these ambitions we have outlined the next steps below.

## Next steps

1. **Update T&Cs**

We will update our Terms and Conditions to specifically allow us to prevent resolution in the DNS where we have identified a high risk of phishing. These updates will be as follows:

***"10. Cancelling or altering the domain name***

*10.1 We may cancel or put a **domain name** into a **special status** by notifying you if:*

*...*

*10.1.2 in our sole discretion we believe the domain name is being used, or has a high risk of being used, in a way that is likely to endanger any part of the domain name system, other internet users (including but not limited to the distribution of viruses and malware, phishing activity or facilitating distributed denial of service attacks), or our systems and internet connections; or"*

To view our Terms and Conditions in full visit: nominet.uk/policies

2. **Education and support for registrars**

To ensure all registrars have the information and support they need to address abuse in domains under their management we will run a Members' webinar to outline best practice and available Nominet tools for tackling abuse.

The date will be announced through our Membership Engagement Programme, for more information visit: www.nominet.uk/corporate-governance/members

To facilitate this we would like to highlight the availability of existing tools for registrars. These are located under 'Security Tools and Protection' at registrars.nominet.uk/uk-namespace/

This includes:

- **Domain Health**: a free service to help all .UK registrars to combat cybercrime on domains managed by them. Domain Health alerts .UK registrars when domains they administer are implicated in spam, phishing, malware and botnet activity, and provides practical advice as to what they can do to address these problems.

- **Investigation Lock**: Registrars can lock domains while they investigate if a domain name is being used for illegal activity, and keep domain names suspended when that investigation has been concluded if appropriate. The lock removes the domain from the zone file so it will no longer resolve. All information relating to the domain name is locked preventing registrant transfers and account modifications.

- **Domain Lock**: a chargeable service for Nominet registrars, it is a preventative measure to mitigate the risk of abuse on high profile names. It allows domain names in the UK namespace to be locked at the Registry level. This means that once a domain name is locked, no changes can be made to it or its Domain Name System (DNS) configuration until the lock is removed.

3. **Proactive collaborative approach to reduce phishing**

We will continue to develop Domain Watch and work collaboratively across the industry and UK internet community to prevent and address phishing.

We will continue to work with our data science team to measure, track and eliminate phishing domains in .UK, and report on progress in our annual Criminality Report, published in November.

## Landing pages

### Background

Since 2014 we have been formally collaborating with UK law enforcement agencies to disrupt the impact of criminal behaviour by quickly suspending domain names used for crime. Whilst this is a limited intervention – the content will continue to exist on the server or cloud provider regardless – any email functionality associated with the domain name will be blocked, and we recognise that the disruption to criminals using .UK domain names is nonetheless beneficial in protecting internet users, and making .UK domains an unattractive target for criminals.

Because domain suspension technically removes that domain from the DNS, any visitor using the domain to navigate to the site will be unable to access the site and will instead see in their browser an error message. We have received occasional requests in the past from UK law enforcement agencies for any traffic associated with a domain after suspension to be redirected to an informational page e.g. assistance for fraud victims or some other public resource more helpful than a standard error message.

This consultation sought views on what happens following the suspension of a domain. The landing pages questions were as follows:

4. What do you think about the principle that a domain which has been suspended for criminal use should be directed by Nominet to an informational landing page? [freetext]

5. We currently suspend domains for the remainder of the term of registration, or 12 months if that is longer than the remaining unexpired term. But this practice is not currently formalised in policy. Do you agree that this period is sufficient, and that we should formalise the suspension period in our policies? [y/n] & [freetext]

### Responses

Almost all stakeholders supported the concept of landing pages, but there were some clear differences on the purpose and audience for such pages.

The suggestions we received are summarised in the table below:

| Audience | Purpose |
|---|---|
| Registrant | Reverse incorrect suspension |
| General public | Harm prevention / education / information on online safety |
| | Information gathering - encourage reporting |
| | Prevent future offending |

Examples of the comments we received include:

- *"It is long overdue but the information should be meaningful, accurate and up-to-date - including on those who will help victims of fraud take action to obtain redress and/or reduce future risks."* **Financial Services business**
- *"This is a very good idea and lets consumers know that the website they have been directed to either by word of mouth, following a link on social media etc., has been suspended for criminal activity. It makes a consumer more aware and shows that LEA [law enforcement agencies] and Nominet are working together to keep internet users safe."* **Manufacturing business**
- *"We believe the principle as outlined would be of benefit, particularly as an aid to enhancing consumer protection."* **Law Enforcement Agency**
- *"Remove the ambiguity. If a domain is suspended due to criminal use or something else it is very helpful for us and our clients to know that is why the domain is suspended. Also knowing when the suspension will be lifted helps."* **Domain Name Industry**
- *"We are in favour for suspended domains to be directed to an informational landing page. Without this landing page visitors to the site could be misled into thinking there was a technical error rather than removal for illegal activity."* **Law Enforcement Agency**
- *"I think it's a fantastic idea and the MHRA wholeheartedly supports this move."* **Law Enforcement Agency**
- *"This appears to be a good idea. Potential victims may try to access the website without the knowledge it was a criminal entity. Landing pages will assist potential victims to avoid the company behind the site. If they have already become victims without knowing it, this may encourage them to file a report."* **Law Enforcement Agency**
- *"We support this principle, noting that domains suspended in URS proceedings are directed to a page informing the user about URS."* **Domain Name Industry**
- *"We are supportive of the proposal to direct visitors of suspended sites to an information landing page, as a clear way of explaining to a consumer/business why they are no longer able to access a website."* **Central Government Department**

Stakeholders at our roundtable agreed the text should be simple and concise, use official government agency logos and avoid links; there was some concern that links could be hijacked, spoofed, or undermine trust and wider messaging regarding how to stay safe online. One respondent noted that Nominet should not provide advice outside our scope of expertise and should instead collaborate with relevant organisations.

Several stakeholders raised concerns that applying a landing page to a compromised domain or a domain identified in error could have implication for legitimate registrants and would need to be resolved quickly. For example:

- *"IPO supports the view of law enforcement that this is a good thing to do, providing due diligence is conducted as to the source of the abuse and that a legitimate entity connected to the site is not implicated."* **Government Agency**

- *"The effects on a legitimate business by an erroneous accusation could be devastating. Even the effect on a personal domain (such as my own) could be "very inconvenient' since it would mean that my email would stop working."* **Individual, Civil Society**

Several stakeholders suggested a pilot would help resolve any potential problems, for example – a pilot could test process solutions to avoid impacting legitimate registrants who have had their domain compromised, and ensure they receive the information they need to secure their domain.

We also received suggestions to monitor traffic to the landing page in order to assess whether the page is worthwhile. Stakeholders encouraged Nominet to adopt a flexible and iterative approach. For example,

- *"Nominet should not wed itself to a single solution for the landing pages. In our experience, messaging needs to evolve over time as does the tactics used and therefore testing different messaging and different styles of landing pages will help inform what the most effective approach to take is. We also believe that Nominet should pilot any new system it implements to ensure its technical approach is sound."* **Intellectual Property Trade Body**

In relation to the duration of the suspension period, essentially all stakeholders supported Nominet formalising the suspension period. Most stakeholders suggested 12-24 months. Some suggested we should suspend domain names indefinitely. Others suggested time periods should be based on traffic per domain.

- *"In our experience, 12 months is unlikely to accommodate timescales of an investigation. It might be suggested that this be extended to two years or have an annual review from the date of suspension."* **Law Enforcement Agency**
- *"I would like to see a 24 month term of suspension. This will allow a longer timeframe for any 'brand' of the domain name to diminish prior to any re-use. Helpful to maintain the reason for suspension and to 'cleanse' the domain for any new legitimate registrant."* **Law Enforcement Agency**
- *"In terms of how long a landing page should remain live we believe it should last for a year and then the number of visitors to the landing page should be monitored and when this falls below an agreed number, the page can then end, although inappropriate resurrection/purchase of the relevant domain will remain a concern."* **Intellectual Property Trade Body**

## Nominet comments

Our consultation showed considerable support for the principle of a landing page from a wide variety of stakeholders.

We believe that providing a landing page has the potential to prevent harm and educate the general public to interact safely online. We heard valuable points on potential implementation challenges and agree that a pilot project is sensible to test the concept, check whether the pages receive any visitors, and establish a technical and operational approach.

We agree that it is important to ensure a registrant has knowledge of how to reverse an incorrect suspension. However, we do not believe that a landing page is the best place to provide this information. Registrants receive 48 hours notification from Nominet prior to a suspension, this provides them with details on how to prevent the suspension if they believe it is being applied incorrectly.

We agree that our suspension period should be formalised and publicly communicated. While there may be value in an individualised approach to each domain depending on traffic we think this may result in an overly complex implementation process. Based on feedback, we feel it is appropriate to extend the suspension period from 12 months to 24 months to allow for the conclusion of investigations and for traffic to the domain to diminish.

Since 2014, we have suspended ~92K domains for criminal activity. Of those that have been cancelled and then re-registered, ~3,500 are live with no indication they are being used for criminal activity, ~260 were cancelled, re-registered and then suspended again on notification from a law enforcement agency. This indicates 3.8% have been re-registered and are being used for a legitimate purpose, while only 0.3% have been re-registered and used for criminal activity.

## Next steps

1. **Update our T&Cs**

We will update our Terms and Conditions to expand the definition of 'special status' to clarify that it includes redirection. These updates will be as follows:

> ***"1. Definitions and interpretation***
>
> *In these conditions, the following words have the following meanings:*
>
> ***'special status'** – Various special states your **domain name** may be in, such as suspended due to breach of these conditions, blocked from transfer or deletion due to the operation of the **DRS Policy** or legal dispute, and redirected to an information/help page following suspension. This will normally mean that you will remain listed as the person who has registered the **domain name** but the **domain name** itself may not work."*

To view our Terms and Conditions in full visit: nominet.uk/policies

2. **Pilot**

We will run a pilot in collaboration with UK law enforcement agencies to trial a landing page to provide education and harm prevention messaging to internet users.

The pilot will aim to draw on varied expertise and experience to a) test the operational and technical process, b) refine the messaging, and c) monitor traffic to the domain over time.

We will report publicly on the progress of this pilot in 12 months.

If you are interested in providing input to the pilot, please contact policy@nominet.uk

### 3. Formal Criminal Practices Policy

To minimise the risk of re-registration we will extend our suspension period for domains suspended due to criminal activity to 24 months and clarify this publicly on our website in a policy document which also sets out the steps taken to ensure the registrant receives notification and information on how to prevent or reverse the suspension.

We will share a draft policy for comment in Spring 2020.

## Drops lists

### Background

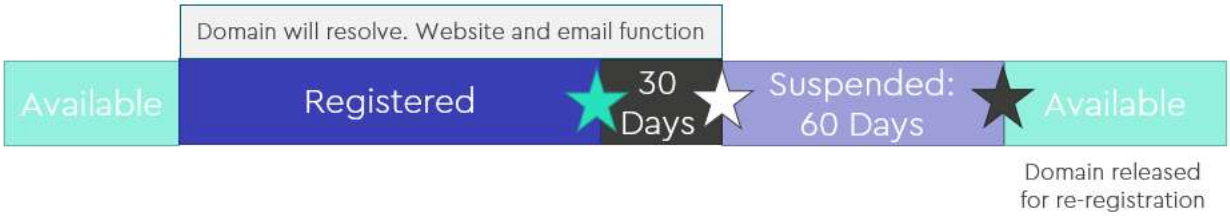
A domain name is registered with us for a specific term of between one and ten years. At the end of the term the registrant has the option to renew the domain, or to let it expire.

Our current process is that if a renewal request is not received within 30 days of the expiry date, the domain name is automatically suspended. When a domain has been suspended for further 60 days without being renewed, we'll schedule it for random cancellation over a 24 hour period. Once cancelled, the domain name will become available for re-registration.

**Expiry**. When a domain name comes to the end of its contracted registration period.

**Suspension**. Domain is removed from the zone file. The domain will not work as part of a website or email while suspended.

**Cancellation**. Deleted from the register (will therefore not work as part of a website or email, and will be released for re-registration on a first come, first served basis).




The current system of releasing expired domains for general registration is unique to Nominet. Whilst the process is well-understood by our registrars, it is not consistent with practices in other TLDs (for example, how we operate with our more recent Welsh gTLDs), and there are some disadvantages to it:

- Particularly when an attractive generic domain is in the process of being made available for re-registration, many thousands of requests are made over a 24 hour period to determine whether or not a domain is available to be registered. This reduces system capacity for other services (EPP).
- We receive a small number of complaints that Nominet members/registrars pool resources and game the Acceptable Use Policies (AUP)s to maximise their chances of success.

We sought views on competition in the secondary market and whether Nominet should publish official information on expiring domains.

The drop lists questions were as follows:

6. In principle, do you think Nominet should publish official information for registrars to clarify when expired domains will become available for general registration? [y/n] a) If no, why not? [freetext]

7. Do you think that Nominet should encourage competition in the .UK secondary domains market? [y/n] a) If yes, why do you think this is important? [freetext] b) If no, why not? [freetext]

8. In principle, do you think Nominet should publish official information for the general public to clarify when expired domains will become available for general registration? [y/n] a) If no, why not? [freetext]

9. Any other comments [freetext]

## Responses

Generally stakeholders agreed the current system could be improved. Most supported the principle of a drop list for registrars (89%), and for the general public (68%).

There was support for clarity, transparency and standardisation with the wider industry and gTLDs. For example:

- *"Other ccTLDs offer drop/deleting lists including varying levels of information."* **Domain Name Industry**
- *"A closer harmonisation of rules towards standard behaviour in GTLDs would also be helpful."* **Domain Name Industry**
- *"ICANN already publicises this information. EURID uses whois to display drop dates. This would bring .UK domains in line with the wider industry."* **Domain Name Industry**

Most responses in this area were from the domain industry. Law enforcement agencies commented that domains suspended for criminal activity should be excluded from any public drop list, in order to discourage abuse.

Several respondents raised concerns that a drop list alone would not resolve the real problem – that desirable domain names tend to be re-registered within seconds by specialist registrars, and that this reduces genuine domain usage.

For example:

- *"...Ideally access to dropping domains should be extended to the general public at the point of dropping: that is true competition, and could be done by a Nominet auction process open to everybody."* **Individual**

- *"We would encourage Nominet to re-think the drop process completely and whether it would not be sensible to find a different way to register these, other than "drop catching" which is about technical advantages and industry knowledge. Having a market based system with funds remitted to good causes would help to de-specialise the key domains from the dropcatch market."* **Domain Name Industry**

To address this issue we received suggestions to consider:

- **Registry auction**: Expiring domains are open to bids for a specified time period, the highest bid wins and can be registered with the winner's registrar of choice. Domains that do not receive any bids will then be released through the normal process.

- **Wait lists:** Implement a system to allow the general public to register interest in a domain before it is due to expire. Once it expires they could have first preference on registration through their preferred registrar.

- **Landing pages:** Redirect expired domains to a landing page which includes: a) the time and day a domain will become available for general registration if it is not renewed, and b) a Nominet spinner of registrars who offer drop catching services (similar to theukdomain.uk/buy-a-domain).

- **Expression of interest ballot:** Expired domains are given a specified "expression of interest period". Expressions of interest are all treated equally, at the end of the expression of interest period a technical algorithm picks a winner at random.

Respondents to the questions on competition highlighted that the existing system favours a small number of individuals, creates barriers to entry for new players and effectively perpetuates a closed market. Some respondents emphasised quality of service should drive competition between registrars. For example:

- *"At the moment, there are a small number of drop catching companies with proprietary knowledge that makes it difficult for anyone else wanting to participate in this market. I don't think Nominet should be running an auction for secondary domains, but I do think that drops should occur at a specific time for each domain."* **Domain Name Industry**
- *"The key issue is fairness: fair competition. Policy should be driven by creating the widest possible access to domain names for the general public. Competition between registrars should be driven by quality of services offered to the public, but access to domains, at the point they are dropping, should not be restricted to 'big Registrars' with better 'EPP create limits' than other players."* **Individual**
- *"At the moment a smallish number of companies are competing to catch names on the drop, by making more information public there could be more competition."* **Domain Name Industry**

## Nominet comments

We agree that the current system is quite complex for the general public to understand. The consultation itself demonstrated the challenge of clearly explaining the current system to anyone outside the domain industry.

This consultation has also raised several suggestions on how to allocate domains that are perceived to be of high value - for example, generic words or short domain names. These ideas seek to address a small proportion of expiring domain names targeted in a technical "arms race". These domain names account for approximately 0.7% of cancelled domain names.

In 2018, 1,769,802 .UK domain names were cancelled, of these:

- ~13% (229,352) were re-registered within a year
- ~5% (87,410) were re-registered within a day
- ~0.7% (12,109) were re-registered in the same timestamp they were cancelled

This small proportion of highly desirable domains drives the incentive to pool resources and game our Acceptable Use Policies (AUPs). As this is a complex area of behaviour with related operational and technical implications we believe that change should be approached cautiously. We received thorough and insightful consultation responses on this issue and believe further consideration is required before we make a decision on whether to implement .UK drop lists. We are also minded to run a further consultation on the suggested alternative release mechanism for highly desirable domains.

As a result, we are not making any changes to the current system of releasing expired .UK domains at this point.

## Next steps

1. **Provide an update on progress**

Nominet will further consider the implications of implementing a drop list in the context of our existing approach to preventing system abuse and provide an update to all stakeholders in due course.

This will include a decision on whether we will consult on the alternative release mechanisms for highly desirable domains: registry auctions, waitlists, landing pages and ballots for future .UK policy consultations.