Consultation title: Global Titles and Mobile Network Security - Proposals to address misuse of Global Titles

To (Ofcom contact): globaltitles@ofcom.org.uk

Name of respondent: [redacted]

Representing (self or organisation/s): P1 Security

Address (if not received by email): [redacted]

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

> Nothing ☒

> Name/contact details/job title ☐

> Whole response ☐

> Organisation ☐

> Part of the response ☐

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes ☐ No ☐

Declaration

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments. Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

P1 Security's response to Ofcom's consultation (22nd July 2024): Global Titles and Mobile Network Security - Proposals to address misuse of Global Titles

P1 Security is pleased to respond to Ofcom's consultation. We welcome Ofcom's efforts to promote network security and build protection against malicious signalling. We endorse Ofcom's approach and hope that it encourages other regulators around the world to take similar action. We particularly endorse two aspects of Ofcom's thinking:

- Application of a zero-trust regime and thinking, and
- GT Lessor having full responsibility and accountability for all signalling traffic transmitted by their GTs.

We believe these two factors are critical to the success of any approach to tackle the issues GT Leasing causes.

About P1 Security

P1 Security is a world leader in mobile network security. We help operators, governments, regulators and enterprises to defend against all network cybersecurity threats and attacks. Founded in 2009, P1 Security is one of the most trusted companies in network security with proven experience on all major technologies and network protocols.

Our products and services are dedicated to enhancing the level of safety on all major telecom protocols standards. We provide software to automate the identification and detection of potential threats in signalling protocols and help our customers remediate their consequences to provide increase security to their subscribers.

We boast a distinguished track record in providing specialized telecom security services. Our team of seasoned experts possesses deep-rooted knowledge of regulatory frameworks, compliance requirements, and industry-specific challenges. Our experts have been advising the most critical infrastructure for almost 15 years on topics going from security audits to full security architecture review through vendor management. We are a leading provider of security audit and have a deep interest in any market changes that impact penetration tests.

We understand that regulatory bodies have unique responsibilities, compliance mandates, and oversight requirements. We work closely with regulators to meet their specific needs. This ensures that our security measures align seamlessly with regulatory frameworks, providing enhanced oversight without compromising operational efficiency.

Response to Ofcom's Questions

Consultation question 1: Do you agree with our proposal to ban GT leasing to third parties? If not, please explain your reasons including how you would prevent malicious signalling by lessees.

P1 Security Response: We fully endorse this proposal. We do not believe that there are any cases that justify this practice other than those referenced by Ofcom in question 2 below.

Consultation question 2: Do you agree with our proposal to only include exemptions to our ban on GT leasing relating to intra-group and supplier use? If you consider that any other exemptions are

necessary, please explain how these exemptions could be limited to prevent malicious signalling by lessees.

P1 Security Response: We fully endorse this proposal and believe it offers a sensible approach to the real-world pragmatic needs of operators in an extremely low risk manner. Although the risk generated by Ofcom's proposed exemptions should be very low, Ofcom should give consideration to requiring operators to publish details of GTs used in this manner.

In the case of penetration testing, we do not believe any exemptions are required. We are a leading provider of SS7 (and other protocols) penetration testing and we have never used leased GTs. We fundamentally reject that approach as insecure and high risk. We believe that there is a material risk bad actors could attempt to include bad packets into traffic originating from leased GTs, which may or may not have previously used for penetration testing, or from GTs that have a similar identity to those GTs that have been leased to penetration testers. The Consultation notes at 3.16 that some lessors have up to 22 customers. It is entirely feasible to imagine that, with such a large number, some of those customers could be penetration testers and others could be responsible for the origination of bad packets.

The biggest concern to industry should be a GT that was previously used by penetration testers that since returned to the GT lessor. This GT could subsequently be leased to a bad actor. The GT might have a trusted reputation and could possibly be whitelisted in signalling firewalls due to its past usage. The consequences of this could be very serious.

A concern for penetration testers is that they might lease a GT that was previously used by a lessor to send bad packets. This GT could have a "bad reputation" and this would now be inherited by the company conducting penetration testing.

Additionally, there is the risk of number proximity. To illustrate this risk, we use the following example of range "7839 0" (note: Ofcom designates this range as "protected"), for the fictitious, assumed to be well-known network, *"Acme Telecom"*:

NMS Number Block: Number Block	Sub-range	CP Name	Planned Usage
7838 9	0-9	Hutchison 3G UK Ltd	Assigned to real subscribers*
7839 0	1	Acme Telecom	Assigned to real subscribers
7839 0	2	Acme Telecom	Assigned to real subscribers
7839 0	3	Acme Telecom	Assigned to real subscribers
7839 0	4	Acme Telecom	Assigned to real subscribers
7839 0	5	Acme Telecom	Leased for Roaming VAS Hosting
7839 0	6	Acme Telecom	Leased for Pen Testing Solutions
7839 0	7	Acme Telecom	Leased for SMS Enablement
7839 0	8	Acme Telecom	Assigned to real subscribers
7839 0	9	Acme Telecom	Assigned to real subscribers
7839 1	0-9	Guernsey Airtel Limited	Assigned to real subscribers*

* assumed for illustrative purposes – actual real-world usage is not known

Matters to highlight for this range are:

1. The range is sandwiched between two well-known mobile operators.
2. Acme Telecom uses the majority of the range for its own subscribers.

3. It has chosen to lease 3 sub-ranges to three different GT lessees.
4. Each of those lessees has a different use case, one of which is penetration testing.
5. It is also assumed no bad actor will declare their nefarious intent so the lease for the range 7839 07 is listed as SMS Enablement but it will also be used to originate bad packets.

In this example, the penetration testing range of "7839 06" will occasionally send bad packets – that is the point of penetration testing. The neighbouring ranges should not send bad packets but, "7839 07" is being used by a bad actor so will occasionally send bad packets. The risk is that victim networks of attacks from "7839 07" may incorrectly assume that it is related to the penetration testing from "7839 06" and ignore the attack as a false alarm.

The P1 Security approach has always been to register as an official telecom operator with dedicated GTs and MNC+MCC allocated by the French regulator, ARCEP. As such, we are able to establish direct roaming agreements with our customers for each penetration test. Our testing is totally separated from other leased GTs and there is no risk of such confusion. Having our own numbering resources provides us with legitimate interconnect access, enabling us to perform our assessments without relying on external leasing arrangements.

We believe that it is important that penetration testing consists of several approaches, including testing the target operator's test network (as Ofcom proposes in Table 4.1) as well as testing over the standard SS7 network, in the same manner that bad actors would launch their attacks. The latter approach is important since, in our experience, live networks are often not as well protected as test networks.

We are grateful that ARCEP has supported our approach and would encourage Ofcom to consider a similar approach too – our understanding is that Ofcom is not currently able to offer GTs to penetration testers. Although we are registered in France as an operator, we would appreciate the opportunity to potentially register as an operator in the UK. This is because, when testing French networks, we need to use our domestic GT and we would prefer to have the option of an international GT. Additionally, it also useful to have the ability to conduct testing using different GTs, both domestic and international, since there may be different treatment and routing of such traffic which is relevant to security researchers. We would request that Ofcom consider this matter.

Finally, we would add that there may be an argument for leased GTs to enable rapid scanning across multiple networks. It is true to note that the disadvantage of being assigned your own GT and MCC+MNC is that these are only useful if a roaming agreement is established. This is not an issue for penetration testing, but it is a major impediment to conducting research such as worldwide network scanning. However, we believe the appropriate approach to this is to sign a security research agreement with an established mobile operator and to benefit from their roaming footprint. This is different to GT leasing, since the research partner operator would have full visibility and control of all traffic leaving their network. In other words, there is no need for a leased GT.

Consultation question 3: Do you agree with our proposal to ban the creation of GTs from sub-allocated numbers by third parties?

P1 Security Response: We fully endorse this proposal. We cannot think of any justification for this behaviour.

Consultation question 4: Do you agree with our proposals to strengthen our rules to prohibit the misuse of GTs by operators that hold UK mobile numbers and to provide supplementary guidance on the types of steps range holders are expected to take when providing a service to a customer (using a GT as an input) that has the potential to generate malicious signalling?

P1 Security Response: We fully endorse this proposal.

Consultation question 5: Do you agree with our proposal to strengthen our rules to prohibit the creation of GTs from numbers not allocated for use?

P1 Security Response: We fully endorse this proposal. We cannot think of any justification for this behaviour. We also think that Ofcom should review aspects of this issue to ensure that a) the process to withdraw number ranges that were allocated for use becomes more transparent; and b) that all providers are obligated to remove routing to number ranges that are no longer allocated for use.

Consultation question 6: Do you agree with the proposed implementation period?

P1 Security Response: We fully agree with the time period. Whilst we would prefer it to be shorter, we think this is a sensible compromise given the potential impact of the proposals.

Consultation question 7: Do you agree with our provisional impact assessment?

P1 Security Response: Overall we do agree with Ofcom's provisional impact assessment. However, given our real-world experience in relation to penetration testing, we also suggest the use of a GT assigned to a penetration testing company is an additional alternative to leased GTs that Ofcom has not detailed in table 4.1. Whilst this is not currently possible for Ofcom to assign such a GT, P1 Security has been using the GT assigned to us by ARCEP for many years.

Given the above, we do not feel there is any need for penetration testers to avoid using GTs – we believe a comprehensive testing approach will combine the use of remote access to an operator's test network together with access to the live network, via its own GT.

Consultation question 8: Do you agree with our proposed changes to the General Conditions of Entitlement, National Telephone Numbering Plan and Numbering Condition Binding Non-Providers?

P1 Security Response: We have no view on this matter since it is beyond our typical area of focus.