U.S. Telecommunications Insecurity 2022

REPORT PREPARED FOR THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) UNDER A CONTRACT THROUGH DHS SCIENCE AND TECHNOLOGY BY:

ADAPTIVEMOBILE SECURITY LTD – DALLAS TEXAS

IN CONJUNCTION WITH

TELECOM DEFENSE, LAS VEGAS NEVADA SECURITY

JUNE 2022

ENEA
AdaptiveMobile Security

TELECOM DEFENSE

WARNING: Some information in this report is UNCLASSIFIED//FOUO. TLP:AMBER+STRICT = Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Recipients may only share this information within their own government organization, and only as necessary to act on that information, consistent with both the DHS policy relating to safeguarding FOUO information and with the Traffic Light Protocol (TLP). Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Information in this section may be exempt from public release under the Freedom of Information Act (FOIA) (5 U.S.C. 552). Further, this section may contain or be based upon on business confidential information subject to the Trade Secrets Act. DHS personnel are reminded of their obligations under DHS Form 1000-6, Non-Disclosure Agreement. Requests to disseminate information in this report should be coordinated with CISA/IOD/ERO. For U.S. Government use only.

NOTIFICATION: The information provided in this report is provided "as is" for informational purposes only. The Cybersecurity and Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages including, but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with, this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

Table of Contents

List of Figures 4
List of Tables 4
Introduction 5
Executive Summary 6
Closing the Security Gap: the Need for Dynamic Zero-Trust. 8
Example 1 – Surveillance of Inbound Roamer on U.S. Network. 9
Example 2 – Targeting of U.S. Subscribers / Reconnaissance of U.S. Operator Network 9
Example 3 – Indication of Potential Vulnerability to Obfuscated Attacks against U.S. Network 10
The Vulnerability in Context 11
The Need for Dynamic Zero-Trust Protection 12
Recommendations 14
Recommendation 1: (b) (5) 14
Specific Measures for Consideration: 14
Recommendation 2: (b) (5) 16
Specific Measures for Consideration: 16
Failed Trust Report: U.S. Interconnect Security 17
Domestic Threats 17
Signaling Services Provided to U.S. Operators Using Non-U.S. Based Facilities 18
Ownership Issues in Today's U.S. Telecommunication Industry 19
Operators Using Blacklisted Vendors 20
Operators Using Suspicious Mobile Node Vendors 20
Non-U.S. Mobile Number Ranges Used 21
Mobile Operators not Broadcasting a Mobile Network or Operating with Expired Licenses 21
Mobile Operators Not in the Traditional Mobile Operator Business 22
Future Threats 22
An Introduction to the US Interconnect Network 23
Specific Challenges for the United States 26
National Roaming. 26
American National Standards Institute (ANSI) Variant of SS7 26
Exchanging Messages on the Signaling Network 27
Global Titles (GTs) 27
Example Scenario 27

National Security Implications 28
Why Spectrum Licenses Matter for Signaling 29
Safeguards from Foreign Bad Actors 30
Signaling Carriers/Aggregators Operating in the United States 32
The Signaling Carriers Identified as Using Information Listed in IR.21 Documents 33
Threat Canvas from Aggregators 44
United States Global Title Owners 47
ANSI SCCP 49
List of Entities Controlling U.S. Global Title Resources: 53
Nationwide Operators 53
Large Regional Operators 56
Small Operators 57
Map of Mobile Operators with Spectrum License 93
Mobile Node Vendors 94
Other Major Telecom Security Gaps Which are Used to Undermine U.S. National Security 96
Recorded Attacks Originating from U.S. Global Title Holders 97
Conclusion 102
Dynamic Zero Trust Defense 103
Defending Forward 103
Glossary 104

List of Figures

Figure 1: SS7 Network Architecture 24
Figure 2: Hubs for SS7 Signaling Note: Image above is Unclassified 25
Figure 3: ANSI SCCP - ITU SCCP Signaling Path 50
Figure 4: Map of Mobile Operators with Spectrum License 93
Figure 5: Remote Access and Control to U.S. Global Title Resources 99
Figure 6: Additional Telecom Security Gaps ..... **Error! Bookmark not defined.**

List of Tables

Table 1: IPX Providers and Customers 45
Table 2: SS7, Diameter (IPX) and GRX Vendors for US MNOs 46
Table 3: Mobile Node Vendors 95

Introduction

(U) This report has been prepared by AdaptiveMobile Security in conjunction with the Telecom Defense Limited Company on the U.S. interconnect threat landscape for the exclusive use of CISA, the Cybersecurity and Infrastructure Security Agency, within the U.S. Department of Homeland Security. This report will:

1. (U) Outline interconnect vulnerabilities which can be exploited by the adversaries of the U.S.

2. (U) Provide details of three recent examples of potential threat activity directed against a U.S. operator network which are illustrative of the ways state-level threat actors seek to identify and exploit potential weak points in the U.S domestic telecoms landscape (i.e. gaps in defenses).

3. (U) Provide insight into different ownership structures within some of the telecom entities licensed and operating within the USA, who could present a threat to the security of the U.S., and which could require ongoing supervision, regulatory change and enforcement capability.

(U) The report has been compiled using a combination of public information from national numbering databases, Global System for Mobiles (GSM) radio license records from the Federal Communications Commission (FCC), foreign ownership FCC filing records, Office of Foreign Asset Control (OFAC) lists, secretaries of state entity registration records, information provided by contacts at industry suppliers, non-public records from the GSM Association, first-hand analyst experience and industry knowledge as well as sensitive threat information across all telecom signaling protocols, i.e. SS7, Diameter, GTP-C, GTP-U, and intelligence acquired from global deployments of AdaptiveMobile Security's real-time threat intelligence platform (also known as "SIGIL" for Signaling Intelligence Layer) over the past 30 months.

(U) All the data contained in this report and the views expressed are those of the authors and are based on sector expertise of over 30 years' experience in the U.S. telecommunications market, analyst reports, live events, and publicly available information within a variety of U.S. agencies, such as the Federal Communications Commission. Confidential threat data gleaned from real life attacks is also presented.

(U) A full glossary of abbreviated technical terms is available at the back of this report.

Executive Summary

1. (U) Telecommunication networks are critical to the safety and security of our society and are the foundation of all primary communications in countries today. However, these networks face an increased threat of cyber exploitation and attack by a growing number of international threat actors, as highlighted in a recent alert[1] issued by the U.S. Government on the exposure of American organizations to aggressive activity by cybercriminal groups who have declared their intent to attack the West for its support of Ukraine against the latest Russian invasion. This threat is compounded by the apparent resurgence of previously identified state-level threat groups[2] [3], expanded activity by others[4], and the appearance of new threat actors such as UAC-0056, aka: 'SaintBear'[5]. The fact that U.S. national networks can be readily compromised from anywhere in the world is not yet widely understood. These telecommunications vulnerabilities largely reside within the complex and arcane signaling/interconnect networks that were built on trust. According to the GSMA, this very trust which underpins the increasingly advanced and complex services enhancing peoples' ability to communicate, trade, and share ideas, also introduces a greater number of potential threats and greater scope for harm[6]. In short, the traditional "trust" paradigm is a failed trust. We must evolve our telecommunications security paradigms to verifiable, "zero trust" models if we hope to thrive and survive, and only work with those whose commitment to defeating the scourge of cyber warfare matches that of the United States

2. (U) Recent disclosures and reporting pertaining to data breaches at (b) (7)(E) and (b) (7)(E) (b) (7)(E) present significant concerns for the potential subsequent targeting of U.S. subscribers, and heightened risk to U.S. telecom network security as a knock-on effect of such breaches. This arises from the potential exposure of the personally identifiable information - including electronic identifiers of millions of U.S. citizens - to cyber threat actors who could be motivated to exploit such data to the detriment of American interests.

3. (U) Unlawfully acquired data, coupled with the malicious access to U.S. networks, combine to create the largest threat vector to those tasked with protecting U.S. subscribers' communications and their security. Information exposed to acquisition by state-level cyber threat actors as a result of such breaches can be exploited by sophisticated, targeted communications "Surveillance as a Service" (SaaS) platforms, such as NSO Group's Pegasus, Cytrox's Predator[7], QuaDream's REIGN[8], and CY4Gate's Epeius[9] [10] as well as providing private

[1] Specifically Alert AA22-11OA published on April 20 2022, source: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[2] Such as the 6 Russia-aligned state-level threat actors named in Microsoft's 'Special Report: Ukraine' published on Apr 27 2022 (source: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/)
[3] by Ukraine's Head of Information Security and Cybersecurity Agency in this article – source: https://therecord.media/from-the-front-lines-of-the-first-real-cyberwar/
[4] Such as Chinese cyber threat group APT10, AKA: 'Cicada', reported to have broadened its espionage activity to include countries such as the US (source: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks)
[5] Reportedly active since early 2021 (source: https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/)
[6] See GSMA report: Safety, privacy and security across the mobile ecosystem (2017) (source: https://aiforimpacttoolkit.gsma.com/resources/GSMA-report_Safety-Privacy-and-Security-across-the-mobile-ecosystem.pdf)
[7] https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
[8] https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/
[9] https://irpimedia.irpi.eu/en-surveillances-cy4gate-united-arab-emirates/
[10] https://www.cybersecurity-help.cz/blog/1910.html

information for blackmail, extortion, and other purposes. While the impact of these massive data breaches is not easily quantifiable, it can be better understood when you consider that our nation's nervous system i.e., our telecommunication networks, are subject to data dumps, alterations, deletions, and influence operations, as well as real-time monitoring (text, voice, data extraction, etc.) by people, organizations, and countries with self-serving and/or malicious intent.

4. (U) Telecommunications signaling is the complex expression of protocols and systems used to connect, relate, and share information with communications networks (international or domestic) throughout the world. Based on our analysis of up to 50 billion telecom events on a daily basis, the United States remains the most targeted country in the world in terms of global signaling/interconnect cyber exploits across the key protocols of Signaling System Seven (SS7), Diameter, General Packet Radio Service (GPRS) Tunnelling Protocol (GTP) – Control (GTP-C), and other legacy and emerging protocols. As the most economically powerful nation on earth with many adversaries, this should not be a surprise

5. (U) The interconnect structure (where carriers exchange traffic both domestically and internationally) is traditionally the target for nation-state attackers who abuse their access using protocols based on "trust", and present themselves as different countries/entities, especially in the case of China. Other international cyber actors abuse their access to communications networks and equipment serving the USA (but not necessarily housed in the USA), which then provides them with an almost endless suite of attack vectors. (b) (7)(E)

6. (U) International interconnects provide malicious cyber actors with relatively "trusted" front-door access into U.S. telecommunications networks. Compromised domestic carriers (especially the rural carriers), maintenance (and other) backdoors also exist that elevate the level of trust and can provide unfiltered, trusted network access. In a sense, U.S. telecommunications is like a mansion (and armory, etc.) with unlocked doors and trusting, welcoming tenants.

7. (U) The fact that the U.S. has a complicated and open domestic interconnect landscape with multiple players (for example, rural wireless carriers) and outdated regulation, coupled with technical vulnerabilities inherent in SS7/Diameter/GTP-C all combine to contribute to this perilous and untenable situation for the U.S. and those responsible for its protection. Additionally, the absence of an effective enforcement capability further compromises the safety and security of U.S. telecom subscribers. It should also be remembered that the US shares the +1 prefix with multiple other countries (Canada , Caribbean, etc.) under the North American numbering plan. (b) (7)(E)

.

(U) As this report explains, the prevalence of domestic interconnectivity supporting national roaming between U.S. networks presents an especially large attack surface which represents one of the major structural vulnerabilities unique to the U.S, and compounds the international interconnect-related threat. This report provides insights from both market and technical standpoints on these interconnects, carrier threats/vulnerabilities and related issues together with recent attack data. The report also outlines possible options for mitigation of the overall threat and reduction of the available attack

surface in order to bolster the security of telecoms as a National Critical Function and provide crucial protection for the United States, its networks, and its citizens.

Closing the Security Gap: the Need for Dynamic Zero-Trust.

(U) History informs us that any mass communication system will inevitably be open to security gaps and their exploitation, and cellular networks are no different. Whereas strenuous efforts have been made through the promotion of different generations of mobile service (3G, 4G, 5G), security has always been an afterthought with competing views from telecom equipment vendors as to what security is required. Most attention to date has been focused on the rather leaky SS7 protocol, which was developed in the US in the 1970s to assist different area code translation and which was "hijacked" by the GSMA to enable cellular roaming, a purpose for which it was never designed. (b) (7)(E)

(U) While there is no simple answer to the cyber warfare threats to telecom networks today, the adoption of a zero-trust policy for the telecom market would be a promising first step to curbing some threats from international threat actors. We define "zero trust" by adopting the NIST Zero Trust Architecture (ZTA) tenet:

> "*Trust nothing, verify everything. When a request to access a resource appears, the asset is evaluated. The evaluation of assets is continuous, so as to have an accurate assessment of the threat landscape and risks.*[11]"

(U) The need for **proactive zero trust protection** across the full U.S. telecommunications ecosystem is highlighted by recent threat activity detected by AdaptiveMobile Security in respect of a major U.S. operator. This report details three notable examples that occurred over a nine-week period from March to May 2022. The threat activity reflects the macro level trends identified by AdaptiveMobile Security as characterising the current cellular threat landscape. Note that certain identifiers of operators and telecoms resources have been redacted from the intelligence for the purposes of this report, however these can be provided separately in order to enable independent verification and investigation of the activity involved as appropriate with due regard to confidentialities involved.

[11] https://csrc.nist.gov/publications/detail/sp/800-207/final

Example 1 – Surveillance of Inbound Roamer on U.S. Network.

(U//FOUO TLP: Amber) On 5 March 2022, our Threat Intelligence Unit detected the likely targeting of an inbound roaming device which appears to have been located in Indianapolis at the time of the attack. The subscriber in question was associated with a Cypriot IMSI which was the identifier targeted using a PSI (Provide Subscriber Information) packet. The PSI originated from a Global Title (GT) associated with an operator in the South Pacific region. AdaptiveMobile Security have determined that this GT is leased by a broker based in central Europe, probably on behalf of a nation state security agency which our intelligence has previously associated with the remote targeting of subscribers in many regions globally, including Europe, APAC and MENA, as well as North America.

(U//FOUO TLP: Amber) This broker has emerged over the past 24 months to become one of the most prolific entities we observe exploiting vulnerable telecoms infrastructure globally on an ongoing basis for the likely purpose of surveillance. On the basis of substantial intelligence identifying a wide range of potential targeting activity around the world by GTs controlled by this broker, our assessment suggests that the company may act as a proxy for several nation state threat actors in the execution of espionage operations. Remarkably, this broker's GTs conduct scanning/probing attacks that check vulnerabilities and penetration paths on up to 250 cellular networks every month. We are confident that this prolific broker of telecom connectivity knows exactly what the GTs and domain are being used for.

Example 2 – Targeting of U.S. Subscribers / Reconnaissance of U.S. Operator Network

(U//FOUO TLP: Amber) In April 2022, a larger scale attack against multiple subscribers was detected on a U.S. network. Specifically, on 27 and 30 April, three subscribers were targeted by SRI (Send Routing Information) packets originating from GTs previously associated in our intelligence with a number of entities linked with targeting activity in multiple regions globally. Notably, the subscribers' identifiers, which were targeted from South East Asia, were their MSISDNs i.e., their mobile phone numbers, the possession of which by the attackers indicates an earlier attack.

(U//FOUO TLP: Amber) The originator of the potential threat activity in this instance is another malicious broker of telecom connectivity [12] – a southern European company that has been identified by AdaptiveMobile Security as controlling GTs used in likely espionage-related targeting activity in multiple regions globally similar to the earlier-mentioned broker. Data exists that links this company to a renowned entity engaged in Surveillance as a Service globally.

(U//FOUO TLP: Amber) Such attacks represent attempts to covertly acquire the locations of the devices involved, and therefore of the subscribers targeted, in real-time. They can also serve for the conduct of network reconnaissance by threat actors however (this use is detailed separately below). The

[12] See LinkedIn profile: (b) (7)(E)

use of SRI/SRI-SM PDUs is one of many ways in which threat actors are able to weaponise cellular network functionality to acquire and track the locations of targeted individuals in real-time (with the most advanced actors able to entirely obfuscate the attack). Such attack utility offers Hostile State Actors a capability of unique value in the context of espionage operations (not least for the stand-off it affords as an effective Over-The-Horizon targeting capability, along with the plausible deniability achievable by exploiting 3rd country infrastructure as the attack platform(s)).

(U//FOUO TLP: Amber) This attack also appears consistent with network reconnaissance (or probing) of cellular network environments which we observe to be executed with some regularity by the more significant (advanced and persistent) threat actors. We assess the purpose of such activity to vary based on its utility to attackers. Similar to activity sometimes reported in respect of attacks on ICS (Industrial Control Systems) environments by Advanced Persistent Threats (APTs), such activity could reflect the 'live fire' testing of capabilities by the threat actors involved, as well as serving as initial or confirmatory reconnaissance to identify the level of defenses (or lack thereof) in networks of strategic targeting interest.

(U//FOUO TLP: Amber) It also merits noting that one of the ways in which state-level threat actors can come into possession of MSISDN identifiers (among others) for U.S. citizens, and be able to associate specific identifiers with individuals of targeting interest, is by acquiring both together from information placed on the dark web by hackers breaching the data environments of large data holding companies. This means that even when a data breach may be caused by a lone actor, for example, bearing no affiliation or relationship otherwise with any nation state threat actor, the latter can gain targeting information by exploiting the former's activity, and potentially also the activity of cybercriminals more widely, as a source of potential targeting information. This under reported feature of the ecosystem of telecoms-enabled threats globally represents a key driver of systemic risk internationally as well as in respect of the U.S. domestic security landscape. Of course large databases of US cellular users are available on the internet for purchase also.

Example 3 – Indication of Potential Vulnerability to Obfuscated Attacks against U.S. Network

(U//FOUO TLP: Amber) The most recent of the three examples of note refers to the seven-day period between 4 May and 11 May 2022, during which over 9,000 Global Opcode violations were detected. Over 2,000 of these violations occurred within a single 24 hour period. The activity was attributed to entities including (but not limited to) several malicious entities. Such violations were identified by AdaptiveMobile Security as potentially masking a range of attacks designed to evade detection, including, for example, the exfiltration of the targeted device's IMSI from the network. The activity in question in this instance was detected immediately after an update by the operator to the newest release of our protective platform which provided visibility of such potential threat activity for the first time.

(U//FOUO TLP: Amber) AdaptiveMobile Security had flagged the potential for Global Opcode-based attacks to the operator in question in 2019. Based on the immediate discovery of such a high incidence of violations, we are satisfied that our updated platform can compensate for what appears in retrospect

to be long-standing deficiencies in the specification of the operator's own probes. even the slightest change in security measures within a US Telco can be immediately identified and tested by malicious actors.

(U//FOUO TLP: Amber) The unusually high overall volume of violations in this instance merits highlighting as a feature of the unique risk profile of the U.S. network in question. As such a high volume of anomalous activity compounds the task of identifying real threats within the overall violation noise, the vulnerability to advanced Global Opcode-based attacks, and therefore the potential state-level threat presented by same, is exacerbated.

(U) Global Opcode[13] violations have increasingly featured in the most sophisticated attack campaigns we have observed in respect of likely state-level threat activity over recent years. Based on a review of our install base, we believe that the shift towards Global Opcode usage reflects a move away from more basic, and more detectable, attack techniques which were previously favoured by attackers because there was nothing to stop them in real terms, but which had begun to be detected and blocked in a small number of networks globally. It is significant that such a response should have been prompted by the implementation of firewalling in comparatively few operator networks in global terms. This arguably reflects the high risk attached to the successful attribution of activity to the threat actors involved and by extension attests to the potential stakes involved.

(U) The nature of Global Opcode attacks supports this assessment, as the attacks involve not only a greater degree of sophistication, such that enables complete obfuscation of the attack behind the ostensible traffic, and can be complex enough to defeat signalling firewalls up to a certain standard, by simply bypassing them. The development of an attack technique that exploits the particular features of Global Opcodes therefore appears to represent an innovation on the part of attackers. As such, it also represents one of several key markers of an upward trend in complexity and ambiguity in the overall security environment within telecommunications.

The Vulnerability in Context

(U) One of the key features of signalling-enabled attacks is their unique utility to enable a Hostile State Actor to determine which specific network is used by a high priority target by manipulating vulnerable core network nodes into yielding device electronic identifiers such as IMSI and credentials to the attacker. The potential to manipulate a vulnerable network into yielding the location of any targeted device in real-time presents another unique remote surveillance capability afforded to threat actors offering the potential to support espionage operations against strategically-selected targets.

(U) The potential threat attached to this activity should not be considered in isolation from that associated with mobile malware. Indeed, it is important to recognise that wherever networks may be exposed to manipulation and weaponization by Hostile State Actors, the threat presented by the proliferation of mobile spyware is further magnified by signalling vectors by virtue of their unique attack utility earlier cited in the form of:

[13] A Global Opcode is a routing convention allocated to a mobile carrier for routing purposes.

1. (U) Yielding electronic identifiers confirming target acquisition for threat actors, and

2. (U) The capacity for remote real time location acquisition and tracking.

(U) These combine to provide nation state adversaries of the U.S. with a wide range of telecoms-enabled attack capabilities. It merits remarking that signalling protocols have reportedly been directly involved in the remote delivery of mobile spyware to targeted devices[14]. We do not intend to provide insight into the use of IMSI catchers in the US as it is outside the scope of this report. However, we can confirm that significant use of these tools has been witnessed on the Mexican side of the US border.

(U) It is no exaggeration to say that the NSO Group's Pegasus spyware, along with other emerging exploit platforms and the advent of surveillance-as-a-service, is a game changer. Pegasus allows invisible messages to access your phone through the iMessage platform (control plane) and extract data (files, photos, contacts) through the phone's internet connection (user plane), encrypted. We believe the sanctioning of NSO by the U.S. Department of Commerce in November 2021 is the correct step and sends a clear message to those who seek to undermine U.S. telecommunications security. [15]

The Need for Dynamic Zero-Trust Protection

(U) As the above examples illustrate, and as cellular cyberthreats continue to evolve, an effective zero-trust policy means more than simply implementing filtering as per the nominal guidelines set out in GSMA FS.11[16] and other relevant documents. To be effective, a protective framework must not only be more comprehensive in scope, it must also be dynamic; it must comprise rules-based filtering that is proactively updated on an ongoing basis utilizing AI as well as human-supported processes – i.e., supervised machine learning – rather than implementing rules as a static checklist which can inadvertently result in a 'tick the box' approach to security. Timely, reliable, and relevant threat intelligence is also a key component of any security conventions as it is essential especially in telecommunications in order to detect attacks, determine who is attacking, adapt defenses and enable response.

(U) Proactive protection means that, even where the protective system and equipment operate passively with respect to the network traffic involved, the rules for tripping alerts should be actively updated on an ongoing basis. This report applies the term 'proactive zero-trust protection' to capture this dynamic character which involves threat hunting by analysts. Only zero trust architecture sophisticated enough to detect advanced (i.e., those of GSMA Category 3[17] complexity and above) violations coupled with the analytical capability to identify actionable threats within the violation 'noise' can support proactive network defense, and only proactive network defense offers the potential to consistently thwart the efforts of the most advanced and persistent threat actors over time. By identifying and closing off such

[14] For example – SIMjacker, a vulnerability discovered by AdaptiveMobile Security in 2019. See: www.simjacker.com
[15] https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list
[16] https://www.gsma.com/security/resources/fs-11-ss7-interconnect-security-monitoring-and-firewall-guidelines-v6-0/
[17] See: https://www.gsma.com/security/resources/fs-11-ss7-interconnect-security-monitoring-and-firewall-guidelines-v6-0/

vectors, such an approach reduces the potential attack surface available to threat actors, and by extension reduces the state-level espionage threat posed to the U.S.

(U) The examples of potential threat activity given above suggest that the risks facing U.S. telecommunications may increase significantly in the short term as attackers are able to adopt more evasive techniques even where basic firewalling defenses, for example, may be in place. While 5G introduces some security controls to help implement zero-trust, under 5G, signaling protocols and IP protocols converge and legacy vulnerabilities are carried forward, especially in the non-stand-alone (NSA) 5G architectures. This creates an even more challenging threat landscape.

(U) The U.S., while having about 4% of the world's population, generates over 30% of the world's IP traffic.[18] Coupled with the fact that the GSMA projects that 5G will bring over $700 billion in global economic value, with enterprises projected to prosper the most and enterprise representing 68% of the market led by retail, Government, and finance applications, security improvements need to happen now as the lessons of 3G and 4G must be learned. Security cannot be an afterthought and the impact of not properly preparing for it from a regulatory standpoint and security aspect will see network attacks harder to detect and even harder to prevent as both IP (much wider threat surface and more inherent expertise) and signaling protocols converge.

(U) While the potential impact of such threats going unmitigated is difficult to quantify, it is clear that its nature links it to the threat more broadly presented to the U.S. by espionage executed against American individuals and institutions by Hostile State Actors. At the same time, it is clear that undefended U.S. telecoms networks constitute a vulnerable National Critical Function[19], the subversion of which (through disruption, corruption/manipulation, or dysfunction) could have a debilitating effect on the security, national economic security, and national public health / safety of American citizens.

[18] According to the ITU, International Telecommunications Union.
[19] see: https://www.cisa.gov/national-critical-functions

Recommendations

(U) This report provides two key overarching recommendations in terms of approach required, and details specific policy measures for consideration as well as highlighting further factors for attention. If implemented, these will greatly enhance the security of U.S. phone subscribers' data and national communications. Implementing these measures will also expand and enhance the U.S. national cybersecurity framework by providing critically needed protection for U.S. infrastructure.

Recommendation 1: Dynamic Zero-Trust Protection

(U) A potentially severe gap in U.S. cyber defenses might be addressed by (b) (5)

. We recommend that (b) (5)

. Key personnel need to be (b) (5)
. More than this, the capability to (b) (5)

. Large institutions may want to (b) (5)

.

Specific Measures for Consideration:

(U) We recommend the following policy measures for consideration, some of which should be immediately actionable and some which may require long term policy changes. Networks by their very nature require connectivity to function. 'A' needs to connect to 'B', 'B' to 'C', 'A' to 'C' and so on.

1. (U) (b) (5)

. We highly recommend that (b) (5)

. At a minimum, (b) (5)

. Alternatively, (b) (5)

.

2. (U) Similar to how (b) (5)

. This type of (b) (5)

(b) (5)

.

3. (U) U.S. mobile operators should be advised to (b) (5)

. The above information is

(b) (5)

4. (U//FOUO TLP: Amber) Several mobile operators should be (b) (5)

(b) (5), (b) (7)(E) and (b) (5), (b) (7)(E) (b) (5)

(b) (7)(E), (b) (5) and (b) (7)(E), (b) (5) .

5. (U//FOUO TLP: Amber) Mobile signaling carriers process U.S. signaling traffic in foreign facilities in certain cases and may allow interception by foreign jurisdictions. It may be advisable to (b) (5)

.

6. (U//FOUO TLP: Amber) We have shown that SS7/Diameter/GTP-C traffic for U.S. mobile networks is mostly concentrated within a small number of signaling carriers, in particular the U.S.-based companies (b) (7)(E) and (b) (7)(E). We recommend U.S. agencies consider (b) (5)

.

Recommendation 2: (b) (5)

(U//FOUO TLP: Amber) Within the scope of these recommendations, we draw parallels to the U.S. post 9/11 when DHS was created, and the U.S. introduced stringent new regulations for airlines that wished to transit people to the USA. DHS transferred the obligation and onus onto the airlines to be primarily responsible for ensuring that the passengers they carried were legally entitled from a visa standpoint to travel to the USA. We strongly advocate a (b) (5)

.

Specific Measures for Consideration:

Key to this recommendation is that (b) (5)

. We believe this could be (b) (5)

). We are certain this would (b) (5)

. As technically this would be easy to implement , I believe it would (b) (5)

.

(U) The role of the aggregator/SCCP carrier must be (b) (5)

. In simple terms, consider

.

[20] (U) https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report
[21] https://www.bloomberg.com/news/articles/2022-02-08/twitter-tells-senator-it-is-cutting-ties-to-swiss-tech-firm
[22] Possibly including: (b) (7)(E) , and (b) (7)(E) , as well as Mitto's partner networks reportedly included: (b) (7)(E) and (b) (7)(E)

(U) Additional factors for consideration are highlighted throughout the remaining sections of this report where applicable.

Failed Trust Report: U.S. Interconnect Security

Domestic Threats

(U//FOUO TLP: Amber) Our experience and insight unfortunately confirm that there are several entities within the U.S. abusing the trust bestowed on them by the FCC regarding the operation of mobile service in the U.S., by not fulfilling their security obligations. Rural/small carriers such as (b) (7)(E) (b) (7)(E) and (b) (7)(E) have been identified as abusing network access and originating malicious signaling attacks. By abusing, we mean they allow their network connectivity to be used by "international third parties" whose primary objective is to present themselves as US-based telco entities, delivering domestic U.S. traffic. While it may be difficult to determine if the operators themselves are aware of, or are accomplices in such subterfuge, we can confirm the presence of malicious signaling traffic. At best, they are negligent; at worst they operate for foreign services in the exfiltration of data from U.S. subscribers. (b) (5) is recommended. Intelligence data is available.

(U//FOUO TLP: Amber) The landline operator (b) (7)(E) has also been identified as originating malicious traffic. Specifically, malicious traffic relates to traffic that is configured through the "originating" network to dupe the receiving network into betraying their "subscribers" data.

(U) Malicious traffic relates to:

- (U) Call intercept /comms diversion
- (U) Data extraction (files, photos, messages, contacts)
- (U) Phone hijack
- (U) Message proxy (using the network to send messages using your number).
- (U) DDOS, denial of service
- (U) Modification of user profile
- (U) Location tracking

Signaling Services Provided to U.S. Operators Using Non-U.S. Based Facilities

(U) Aggregators/Signaling Connection Control Part (SCCP)[23] carriers are telecom companies that aggregate traffic from multiple non-U.S. carriers to deliver traffic to the U.S. and vice versa in the absence of a "direct connect", i.e., where the carrier has a direct connection to the operator.

(U) SCCPs perform a critical function, in terms of global connectivity but of course are key data hubs which make them the of target nation-state actors for intelligence and surveillance purposes. The majority of these aggregators are based outside of the U.S., with the exception of (b) (7)(E) and (b) (7)(E)

(U//FOUO TLP: Amber) The following signaling carriers have been identified, which may carry signaling for domestic roaming of U.S. persons via facilities located in foreign countries. This presents a significant risk because such traffic could be intercepted, monitored or altered outside of the jurisdiction of the U.S. (as it occurred with GCHQ reportedly intercepting BICS data roaming traffic from 2010 to 2013)[24].

(U//FOUO TLP: Amber) (b) (7)(E) is processing ANSI signaling for (b) (7)(E) in Canada and (b) (7)(E) is processing ANSI signaling for (b) (7)(E) in Germany. In both cases, ANSI traffic for U.S. persons who are roaming domestically could theoretically be carried to and from these countries. Although we don't expect this to be the case, it is suggested to (b) (5), (b) (7)(E)

.

(U//FOUO TLP: Amber) In addition, we believe (b) (7)(E) is transiting domestic roaming traffic via Switzerland (b) (7)(E) and Italy (b) (7)(E), while (b) (7)(E) is transiting such traffic via Spain and Germany (b) (7)(E) , as both operators, according to their IR.21 information, do not have a native ANSI carrier. (b) (5) is recommended as well. By way of explanation, the (b) (7)(E)

.

(U) Several mobile operators are sending their international roaming signaling traffic directly to facilities in foreign countries. This is less critical, and is unlikely to increase the risk of interception, as the traffic would leave the United States anyway.

[23] Further explanation can be found here: https://searchunifiedcommunications.techtarget.com/definition/Signalling-Connection-Control-Part.
[24] See for example: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

Ownership Issues in Today's U.S. Telecommunication Industry

(U) Whereas the U.S. was possibly the first country in the world to deregulate its telecommunication industry with the introduction of the Baby Bells back in 1984, the criticality of telecoms for a nation always raises the thorny question of how much foreign ownership of the sector should be permitted. This primarily depends on the level of regulation (FCC) and enforcement supervision by other agencies, for example the Department of Commerce (DOC), DHS, etc., to ensure the industry, their subscribers and foreign investors operate within the legal and regulatory framework as set down in the U.S., in terms of network coverage, subscriber security, etcetera.

(U//FOUO TLP: Amber) The purchase of (b) (7)(E) by (b) (7)(E) , a (b) (7)(E) is a perfect example and has since become part of the fabric of the U.S. Telecom landscape.

(U) However, the question of foreign ownership remains a difficult one especially when the true ownership maybe hidden behind several "entities/incorporations" designed specifically to hide their real identity. The following operators are partially or fully foreign owned according to documents filed with the FCC and knowledge we have acquired. We presume that this ownership has been reviewed and authorized by the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (formerly "Team Telecom"), but (b) (5)

(U//FOUO TLP: Amber) (b) (7)(E)
(b) (7)(E)

(U) This list is by no means exhaustive and we recommend (b) (5)

.

Operators Using Blacklisted Vendors

(U) The following companies currently use mobile network equipment from vendors which have been blacklisted by the U.S. Government, according to their IR.21 documents and general telecom insight:

- (U//FOUO TLP: Amber) (b) (7)(E)
- (U//FOUO TLP: Amber) (b) (7)(E)
- (U//FOUO TLP: Amber) (b) (7)(E)
- (U//FOUO TLP: Amber) (b) (7)(E)
- (U//FOUO TLP: Amber) (b) (7)(E)
- (U//FOUO TLP: Amber) (b) (7)(E)

(U) We understand that a compensatory fund is in place to refund these carriers for compelling them to desist from using this equipment. (b) (7)(E)

(U) We strongly recommend however that a (b) (5)

.

Operators Using Suspicious Mobile Node Vendors

(U//FOUO TLP: Amber) The following companies use equipment from vendors that are deemed suspicious, but are not currently blacklisted by the U.S. Government:

- (U//FOUO TLP: Amber) (b) (7)(E)
- (U//FOUO TLP: Amber) (b) (7)(E)

(U//FOUO TLP: Amber) (b) (7)(E)
(b) (7)(E)

(b) (7)(E), (b) (5) *should be* (b) (5), (b) (7)(E) .

Non-U.S. Mobile Number Ranges Used

(U//FOUO TLP: Amber) The following companies advertise to the GSMA and to other carriers and third parties, non-U.S. mobile number ranges, in addition to their U.S. mobile number ranges: (b) (7)(E) (Polish number range), (b) (7)(E) (883 non-geographic number range) and (b) (7)(E) (b) (7)(E) (UK number range).

(U) If these number ranges were to be used to serve U.S. based subscribers or devices, there is a possible risk of intercept of communications by law enforcement agencies from a foreign country. Whereas we believe this is not illegal, it certainly is strange and begs the question why they are doing this, other than possibly running IoT (internet of things) services.

Mobile Operators not Broadcasting a Mobile Network or Operating with Expired Licenses

(U//FOUO TLP: Amber) The following operators are not likely to operate a radio network on their assigned spectrum licenses: (b) (7)(E) (does not operate its own network, but those of hosted operators), (b) (7)(E) (because it has not launched commercial operations yet), (b) (7)(E) and (b) (7)(E) .

(U//FOUO TLP: Amber) The following operators operate with an expired or without a spectrum license: (b) (7)(E) and (b) (7)(E) .

(U) When spectrum licenses are assigned by the FCC, there is a requirement that the license holder must begin broadcasting on the spectrum license within a certain amount of time. There is not a good mechanism in place to verify that this is actually happening, until a license comes up for renewal.

(U) (b) (7)(E)

. (b) (5), (b) (7)(E)
, is advisable.

(U//FOUO) At a minimum, (b) (5)

.

Mobile Operators Not in the Traditional Mobile Operator Business

(U//FOUO TLP: Amber) The following companies are not in the traditional mobile operator business as defined by their licenses. Some are involved in malicious activity, providing U.S. network access to foreign third parties. (b) (5) .

- (U//FOUO TLP: Amber) (b) (7)(E) (international roaming sponsor services and MVNE in addition to traditional rural mobile network business)
- (U//FOUO TLP: Amber) (b) (7)(E) (GPS trackers)
- (U//FOUO TLP: Amber) (b) (7)(E) (Local landline telephone company)
- (U//FOUO TLP: Amber) (b) (7)(E) (IOT)
- (U//FOUO TLP: Amber) (b) (7)(E) (private Long Term Evolution (LTE), messaging and value-added services)
- (U//FOUO TLP: Amber) (b) (7)(E) (multi-IMSI mobile service for international travelers and IOT, in additional to traditional rural mobile network business)
- (U//FOUO TLP: Amber) (b) (7)(E) (IOT services and MVNE / multi-IMSI services in additional to traditional rural mobile network business)—we have definitive information regarding this Company and how these networks are abused.
- (U//FOUO TLP: Amber) (b) (7)(E) (hubbing services, roaming services and MVNE)
- (U//FOUO TLP: Amber) (b) (7)(E) (MVNE services and private LTE)
- (U//FOUO TLP: Amber) (b) (7)(E) (IOT)
- (U//FOUO TLP: Amber) (b) (7)(E) (hosted PBX and unified messaging)
- (U//FOUO TLP: Amber) (b) (7)(E) (IOT and global roaming multi-IMSI services)

(U//FOUO TLP: Amber) (b) (7)(E) consumer facing website raised suspicions with our analysts, and upon further investigation, turned out to be linked to (b) (7)(E) , a company manufacturing LTE bubble systems and IMSI catchers, which they claim to sell to the DOD. If (b) (7)(E) is a known supplier to the U.S. government or law enforcement, no further investigation is required. (b) (7)(E), (b) (5

Future Threats

(U) The CBRS (Citizens Broadband Radio Service) spectrum band was set aside by the FCC in recent years for use by a large number of private networks, run by enterprises, universities, venues etc., in the future.

(U) As the first CBRS networks are implemented, the use cases typically require numbering to be allocated to them, and the customers deploying those networks are looking for roaming capabilities (the ability for a subscriber to move from a national mobile network onto the CBRS network and vice versa). These roaming capabilities will likely rely at least in part on SS7 and depending on the exact

manner in which they are implemented, may create hundreds of new entities with SS7 connections and global title assignments.

(U) If the issues existing today within a relatively small number of global title holders are not addressed, in particular, when it comes to the leasing of SS7 resources to third parties, (b) (7)(E)

.

The Mobile Interconnect Ecosystem in the United States

An Introduction to the US Interconnect Network

(U) The domestic interconnect network is where US carriers exchange domestic traffic for other US subscribers on other networks. Signaling is key to this process and SS7 continues to play a key part in conjunction with IP peering. SS7 is a telecommunications network signaling protocol developed in 1975 to control the setup and teardown of voice calls, particularly international calls between operators in different countries. Initially, operators in different countries, which at that time were mostly state-owned and controlled, established direct peer to peer connections over international communications cables to facilitate the exchange of signaling messages. Operators trusted each other not to perform any unauthorized activities over these connections. Over time, new private operators were licensed in different countries making the peer-to-peer connections unpractical, and signaling hubs were introduced. An operator would connect to one or more hubs which in turn would connect to other hubs and other operators, allowing the customer operator to reach any other operator worldwide through a single connection. This web of interconnected hubs is what is commonly referred to as the "SS7 network".

(U) The following diagram illustrates this architecture:



Figure 1: SS7 Network Architecture

(U) In the early 1990s, SS7 MAP signaling was adopted by mobile operators around the world to facilitate GSM roaming. This meant that all mobile operators that wished to offer international roaming services to their customers had to connect their mobile networks to the international SS7 network. Diameter protocol emerged with the arrival of data intensive technologies such as 4G and which contained IP capability but once again presents significant vulnerabilities.

(U) The following are some of the companies around the world that have established themselves as hubs for SS7 and diameter signaling. Some of these, but not all, serve mobile operators in the USA.

(b) (7)(E)

(U)Figure 2: Hubs for SS7 Signaling
(U) Note: Image above is Unclassified

(U) By its original design, the SS7 network did not have any firewalling in place and was based on mutual trust, and any connected operator could freely exchange SS7 messages with nodes in any other connected operator's network.

(U) This architecture enabled any rogue node connected anywhere in the world on the SS7 network to dialogue with any other legitimate node on any other mobile network worldwide. With the multiplication of private mobile operator to develop competition in most countries, as well as the rise of MVNOs in the 2000s, there are thousands of entry points for SS7 traffic on the worldwide SS7 network today, and all it takes is one (often a small operator with few subscribers on an island nation, or a fake MVNO controlled by bad actors) to provide SS7 access to attackers looking to exploit SS7 vulnerabilities that lead to locating subscribers or intercepting their calls and text messages.

Covid has significantly exacerbated the signaling problem as small carriers who became reliant on roaming revenues to stay afloat have seen that revenue stream disappear --- some have turned to leasing SS7 and diameter connection from their networks to third parties who in most instances are little more than a front for nation state security agencies who subsequently abuse this access.

Specific Challenges for the United States

(U) While it is now accepted industry-wide that established mobile operators need signaling firewalls /security platforms to screen incoming SS7, Diameter and GTP messages to prevent outside attacks, U.S. mobile operators face additional complexity due to several unique aspects of the U.S. market.

National Roaming.

(U) The situation pertaining to national roaming is unique to the United States and other large countries (Canada, Russia, and India for example, and more recently Mexico), whereby radio licensing (usually controlled by the Government) is geographically fragmented in order to allow smaller mobile operators to cover rural areas that are not economical for the larger nationwide operators to cover. In the case of the U.S., this creates dozens of different "rural" mobile operators, all of which connect to different SS7 hub providers and exchange a profusion of SS7 signaling messages to ensure that the U.S. consumer can use mobile services in areas as remote as the bottom of the Grand Canyon, Yellowstone National Park, or the Navajo Nation.

(U) This creates an exponential number of SS7/diameter "entry points" within the U.S. that can be abused by the highest paying domestic, or often foreign bad actors to conduct attacks against mobile phones of U.S. persons. Because of the large volume of domestically exchanged SS7/diameter messages, and the complexity of screening them, many operators do not apply the same (or in some cases any) protection to domestic SS7/diameter traffic compared to international SS7 traffic, which is exactly what the bad actors are taking advantage of.

(U) While the foreign bad actors operate mostly outside of the jurisdiction of the U.S. (and often outside of the jurisdiction of other NATO countries), there could be strategies deployed in order to monitor, regulate or limit at least those entry points which are located within the U.S. jurisdiction. Some policies are proposed in the executive summary of this report.

American National Standards Institute (ANSI) Variant of SS7

(U//FOUO) The second unique aspect of the U.S. market is its use of the American National Standards Institute (ANSI) variant of SS7 signaling, which is used exclusively in North America, and different from the International Telecommunications Union (ITU) variant used in the rest of the world. Because ANSI and ITU SS7 use different point code (addressing) structures, there are essentially two parallel SS7 "networks" present in the U.S., with translation nodes responsible for transiting SS7 messages between ANSI and ITU as needed. Due to this architecture, the U.S. operators have in the past felt a false sense of security from international SS7 attacks, as some of these attacks may not pass across the translation nodes and some of the U.S. networks were not historically connected to ITU signaling at all. For example, the code-division multiple access (CDMA) networks of (b) (7)(E) originally were not connected to ITU).

(U) However, as CDMA networks have converted to GSM in recent years, and as bad actors have infiltrated some of the smaller domestic carriers, nefarious traffic is now present on the ANSI network the same as on the ITU network, impacting all U.S. operators.

Exchanging Messages on the Signaling Network

Global Titles (GTs)

(U) Messages between mobile networks are routed using the SCCP layer of the SS7 protocol between addresses called "Global Titles". A global title looks like a phone number with a country code, and a different address is assigned to each node within a mobile network. For example, each (home location register (HLR) in a network will have a different address, and each MSC will have a different address as well. All addresses are selected within the same range, which is assigned by the ITU or, in the case of the U.S., by the North Atlantic Numbering Plan Administrator (NANPA) which has been delegated the +1-telephone number space by ITU and is responsible for its sub allocations.

Example Scenario

(U) Consider the following example:
(U) (b) (7)(E) is a global title range assigned to, and declared by (b) (7)(E) That means that all addresses in the format of (b) (7)(E) are assignable to mobile nodes within the (b) (7)(E) network.
(U) By further assignment of (b) (7)(E), (b) (7)(E) is the global title address for an (b) (7)(E) HLR and (b) (7)(E) is the global title address for an (b) (7)(E) MSC for example.

(U) These global title ranges are then advertised by each operator in a document called IR.21. The IR.21 describes the technical configuration of a network and lists all routing information necessary to interact with a mobile network for roaming purposes. In addition to its global title range (and the mapping of individual global titles to network nodes and their manufacturers and locations), the IR.21 also contains phone number ranges assigned to subscribers, IMSI ranges, SMS and mobile data configuration information, contacts for operator staff responsible for roaming implementation and much more. This is all (b) (7)(E)
.

(U) Therefore, these documents are typically shared within a confidential framework between members of the GSM Association, a trade association that represents all mobile operators in the world and ensures compatibility between networks and the facilitation of roaming. The documents are theoretically only available to other mobile operators, however, (b) (7)(E)
.

(U) Only when a range is first published in an IR.21 document, and the document is picked up and implemented by multiple SCCP carriers (=signaling hubs) and other mobile operators, does the range become "routed" on the SS7 network, and reachable by any other connected mobile network in the world. Therefore, (b) (7)(E)
. The more seasoned the global title, the more respected the issuing network, thus the wider the reach of networks around the world. For example, (b) (7)(E)
.

(U) To obtain access to such global titles, attackers (b) (7)(E)

.

Our threat intelligence analysts confirm to us that they have seen a significant increase in (b) (7)(E)

.

National Security Implications

(U) What does this mean when it comes to the national security of the United States?

(U) An attack seen originating from a foreign country towards U.S. mobile networks does not directly imply an intent or awareness on behalf of the origin country to deliberately attack the U.S. Rather, it is very likely that a privately owned mobile operator in the origin country has rented global title resources to a third party without the knowledge or oversight of the local government. As well, there is no indication as to where this third party may be located as location can be so easily manipulated.

(U) In the U.S., the practice of renting global titles also exists among (b) (7)(E)

.

(U) A notable example of the potential for the subversion of such arrangements implicating U.S. network security is the (b) (7)(E)

.

(U) While the FCC has a framework to protect CPNI information (identifying information of U.S. subscribers) and has a heavy annual reporting requirement on this subject, there is no regulation around (b) (7)(E)

[25] https://www.theguardian.com/world/2021/jul/21/data-leak-raises-new-questions-over-capture-of-princess-latifa
[26] Sensitive attack data can be provided independently of this report.

(b) (7)(E)

(b) (7)(E)

Why Spectrum Licenses Matter for Signaling

(U) If one is not going to lease a global title from an existing mobile operator, how could one obtain direct assignment and control their own U.S. global title resources to be used for nefarious purposes?

(U) The typical route to obtain a U.S. global title is the following:

- (U) A new company acquires a spectrum license for a frequency that is recognized by the GSMA. In most other countries, this is a very expensive endeavor, because such licenses are mostly nationwide, so only 3 to 6 companies in each country end up owning one. However, the U.S. operates differently in this regard, because (b) (7)(E)

- (U) (b) (7)(E)

- (U) (b) (7)(E)

- (U) Finally, the company (b) (7)(E)

- (U) When following this path, it is important for an operator to (b) (7)(E)

(U//FOUO TLP: Amber) This is why it would be useful to (b) (5), (b) (7)(E) (b) (7)(E), (b) (5)

.

Safeguards from Foreign Bad Actors

(U) The FCC has a framework in place to prevent spectrum licenses, which are considered part of national critical infrastructure, falling into the wrong hands. Whenever an application is submitted by a foreign company to control U.S. spectrum licenses, the application is analyzed by "Team Telecom" to confirm that there are no national security risks.

(U) The group formerly called "Team Telecom" has recently been formalized under the "Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector".

(U) This Committee consists of:

- (U) The Secretary of Defense
- (U) The Secretary of Homeland Security
- (U) The Attorney General, who chairs the Committee

(U) In addition, the following serve as Committee advisers:

- (U) The Secretary of State
- (U) The Secretary of the Treasury
- (U) The Secretary of Commerce
- (U) The Director of the Office of Management and Budget
- (U) The U.S. Trade Representative
- (U) The Director of National Intelligence
- (U) The Administrator of General Services
- (U) The National Security Adviser

- (U) The Assistant to the President for Economic Policy
- (U) The Director of the Office of Science and Technology
- (U) The Chair of the Council of Economic Advisers

(U) The Committee reviews applications for issues of national security, foreign policy, and trade policy issue. This review process applies not only when an application is submitted to own a spectrum license, but also for applications to lease a spectrum license by a foreign entity, which are also filed with and tracked by the FCC by law.

(U) It is reasonable to assume that each mobile operator listed in the relevant section of this report, and which is foreign owned, will have undergone the above review process, and the ultimate owners did not deem to pose a national security risk during this review.

(U) However, since there is no framework, oversight or even knowledge about the leasing of U.S. global title resources to third parties (or more widely, the renting of any U.S. numbering resources) a malicious actor who (b) (7)(E)

.

Our experience indicates that the US Federal authorities should be complimented on the structures in place to ensure governance measures are observed. However, we recommend a (b) (5)

. (b) (5)

is also key.

Signaling Carriers/Aggregators Operating in the United States

(U) By analyzing IR.21 documents obtained through the GSM Association, where operators describe the technical configuration of their network, and provide a list of their suppliers for signaling connectivity, a list of signaling carriers known to operate within the United States can be created. These companies, such as a (b) (7)(E) are also known as aggregators/SCCP carriers.

(U) For each listed signaling carrier, ultimate ownership/control is determined using publicly available information, and any known information on the carrier's infrastructure locations is provided. Fortunately, most of the signaling carriers identified are publicly traded, making the ownership structure transparent. Their infrastructure information, however, is for the most part proprietary.

(U) The customers listed in the following tables are those U.S. based mobile operators who have declared that they use the carrier in question in their IR.21 document. Each of the signaling carriers has many more non-U.S. customers around the world. Because it is possible for non-FCC regulated and non GSMA member companies to designate any U.S. number ranges as global titles and have them implemented by smaller signaling carriers who do not require credentials from their customers, it is likely that additional foreign signaling carriers which are not listed below provide signaling services for certain U.S. numbering resources. These services may be entirely provided using non-U.S. based facilities.

The Signaling Carriers Identified as Using Information Listed in IR.21 Documents

(b) (7)(E)

Ownership	
Owner / control:	Owned by (b) (7)(E) , publicly traded
Infrastructure and Connectivity	
ANSI STP location:	USA
ITU STP location:	USA and international
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) prior to going public in October 2021 admitted a 5-year hack of their internal routing and billing records. As this company is critical to the interchange of traffic between U.S. and international carriers, we believe this loss of data could lead to catastrophic security consequences for the U.S. telecoms market.	

(b) (7)(E)

Ownership	
Owner / control:	(U//FOUO TLP: Amber) Owned by (b) (7)(E))
Infrastructure and Connectivity	
ANSI STP location:	Rockhill, SC and Matoon, IL
ITU STP location:	Unknown, possibly peering with (b) (7)(E)
GRX presence in Ashburn, VA:	Yes
Customers	

(b) (7)(E)

Notes
(U) (b) (7)(E) is traditionally the signaling carrier serving many of the small rural U.S. operators. Unlike many of the other signaling carriers, it has very few international customers outside of the Americas.

(b) (7)(E)

Ownership	
Owner / control:	(b) (7)(E)
Infrastructure and Connectivity	
ANSI STP location:	USA
ITU STP location:	NY, USA and Ashburn, USA
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	

Notes
(U//FOUO TLP: Amber) The packet data roaming network (GRX) of (b) (7)(E) was being (b) (7)(E) This could have provided (b) (7)(E) access with data roaming traffic from for U.S. subscribers of the mobile operators using (b) (7)(E) for GRX, namely (b) (7)(E) .

(b) (7)(E)

Ownership	
Owner / control:	Publicly traded, no single owner over 10%
Infrastructure and Connectivity	
ANSI STP location:	Does not provide signaling services
ITU STP location:	Does not provide signaling services
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(b) (7)(E) is strong in mobile messaging where it holds a large market share alongside (b) (7)(E)	

(b) (7)(E)

Ownership	
Owner / control:	(U//FOUO TLP: Amber) Privately owned by (b) (7)(E) (b) (7)(E) , presumably Swiss citizen
Infrastructure and Connectivity	
ANSI STP location:	N/A
ITU STP location:	Lausanne, Switzerland and Bern, Switzerland
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) U.S. operators using (b) (7)(E) for SS7 signaling would connect to STPs in (b) (7)(E) and transmit signaling directly to international facilities.	

(b) (7)(E)

Ownership	
Owner / control:	(U//FOUO TLP: Amber) Publicly traded, 23% owned by (b) (7)(D), (b) (7)(E)
Infrastructure and Connectivity	
ANSI STP location:	N/A
ITU STP location:	Milano, Italy and Rome, Italy
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) U.S. operators using (b) (7)(E) for SS7 signaling would connect to STPs in Milano and Rome and transmit signaling directly to international facilities.	

(b) (7)(E)

Ownership	
Owner / control:	Publicly traded, 13.4% owned by the French government.
Infrastructure and Connectivity	
ANSI STP location:	Unknown
ITU STP location:	Paris, France and Reims, France
GRX presence in Ashburn, VA:	Yes
Customers	
Sierra Wireless; (b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) hosts one (b) (7)(E) which uses (b) (7)(E) for GRX services. (b) (7)(E) uses (b) (7)(E) for Diameter signaling and GRX services. It does not appear that any U.S. operator uses (b) (7)(E) for SS7 signaling according to IR.21 information.	

(b) (7)(E)

Ownership	
Owner / control:	Publicly traded, 39.5% owned by the government of (b) (7)(E)
Infrastructure and Connectivity	
ANSI STP location:	Unknown
ITU STP location:	Unknown
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) hosts one (b) (7)(E) which uses (b) (7)(E) for GRX services. It does not appear that any U.S. operator uses (b) (7)(E) for SS7 signaling according to IR.21 information.	

(b) (7)(E)

Ownership	
Owner / control:	(U//FOUO TLP: Amber) Most likely owned by (b) (7)(E) (b) (7)(E)
Infrastructure and Connectivity	
ANSI STP location:	Unknown
ITU STP location:	Atlanta, GA; Madison, WI; Portland, OR
GRX presence in Ashburn, VA:	N/A
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) This signaling carrier is newer and presumably has very few customers, likely none of which are outside of the U.S. Smaller companies often have weaker security measures in place due to budget constraints, and this company could be an ideal target for someone looking to breach a signaling carrier.	

(b) (7)(E)

Ownership	
Owner / control:	(U//FOUO TLP: Amber) Publicly traded, 45% owned by (b) (7)(E)
Infrastructure and Connectivity	
ANSI STP location:	Montreal, Canada; Toronto, Canada
ITU STP location:	Montreal, Canada; Toronto, Canada
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) SS7 signaling exchanged via links to (b) (7)(E) would connect to STPs in Canada and be transmitted across borders. According to the IR.21 document, this includes ANSI SS7 signaling, which could theoretically include traffic from U.S. subscribers roaming domestically within USA, although this depends on specific routing, since (b) (7)(E) also connects to (b) (7)(E) and (b) (7)(E) for ANSI signaling.	

(b) (7)(E) (b) (7)(E)

Ownership	
Owner / control:	(b) (7)(E) , publicly traded, 32% owned by the (b) (7)(E)
Infrastructure and Connectivity	
ANSI STP location:	Frankfurt, Germany
ITU STP location:	Frankfurt, Germany
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) SS7 signaling exchanged via links to (b) (7)(E) would connect to STPs in (b) (7)(E) be transmitted across borders. According to the IR.21 document, this includes ANSI SS7 signaling, which could theoretically include traffic from U.S. subscribers roaming domestically within USA, although this depends on specific routing, since (b) (7)(E) also connects to (b) (7)(E) for ANSI signaling.	

(b) (7)(E) (b) (7)(E)

Ownership	
Owner / control:	Publicly traded with no shareholder owning over 10% of stocks.
Infrastructure and Connectivity	
ANSI STP location:	Unknown
ITU STP location:	Madrid, Spain and Frankfurt, Germany
GRX presence in Ashburn, VA:	Yes
Customers	
(b) (7)(E)	
Notes	
(U//FOUO TLP: Amber) Since (b) (7)(E) does not list an ANSI SS7 carrier in its IR.21, it is likely that domestic SS7 traffic of U.S. subscribers is partially exchanged via links going to (b) (7)(E) in Spain and Germany (the company's other ITU SCCP carrier (b) (7)(E), has points of presence in USA).	

Threat Canvas from Aggregators

(U//FOUO TLP: Amber) Aggregators /SCCP carriers present a massive threat canvass for Nation State adversaries due to the vast amount of data they carry and route from all over the world both into and out of the U.S. This was manifest in the most (b) (7)(E) of this year of the loss over a 5 year period of interconnect data for every U.S. carrier and a wide selection of global carriers. The true impact of this hack is yet to be felt (one analyst referred to it as "the telecoms market 9/11") but one must ask that, if necessary, enforcement/checks had been in place, this type of data bleed would never happen. The model under which these aggregators/SSCPs operate is also hopefully outdated, as in most cases, they are paid according to the amount of traffic delivered which gives little if any incentive to them to ensure the traffic is free of malicious intent. From the above list of companies, it becomes apparent that a small number of companies control the SS7/Diameter signaling traffic for a large number of mobile operators. In the case of the U.S., those companies are (b) (7)(E) and (b) (7)(E), and both happen to be U.S.-based and U.S. owned. (b) (7)(E) controls a large portion of the SS7/Diameter signaling traffic worldwide, not only in the U.S.

(U//FOUO TLP: Amber) The aforementioned makes both companies very interesting from an intelligence point of view, and the following should be considered:
(U) (b) (7)(E), (b) (5)

(U//FOUO TLP: Amber) On the flipside, any (b) (7)(E), (b) (5)

(U) The following table obtained from a GSMA report shows the distribution of mobile operator customers among Internet Protocol Exchange (IPX) carriers. IPX is used for the transmission of

Diameter signaling, which can provide similar information to SS7 regarding subscriber registration, if properly monitored

(U//FOUO TLP: Amber) While (b) (7)(E) is not the worldwide leader in IPX market share in this table, its market share is still significant. The recent revelation of a 5-year hack of (b) (7)(E) and the subsequent controlled secrecy surrounding the actual data loss, should be a source of great concern for all regulatory/security bodies in the U.S. charged with protecting and securing the U.S. citizen and their communications.

(b) (7)(E)

Source: HOT TELECOM's report: 'IPX Competitive Analysis 2015'

Table 1: IPX Providers and Customers

(U) The table below summarizes the SS7, Diameter (IPX) and GRX vendor or vendors for each U.S. mobile operator according to the IR.21 documentation analyzed.

(b) (7)(E)

Table 2: SS7, Diameter (IPX) and GRX Vendors for US MNOs

United States Global Title Owners

(U) Since interacting on the SS7 network effectively requires global titles that are advertised to SCCP carriers and to other mobile operator via IR.21 documents, we can establish a list of U.S. actors that can signal on the SS7 network by analyzing U.S. entities that have published IR.21 documents to the industry (other mobile operators and SCCP carriers) within the framework of the GSMA. Even though these documents are normally deemed confidential, it is not difficult for any interested party to get access to them, as we have done in the course of this research.

(U//FOUO TLP: Amber) Because the information published in IR.21 documents can be accessed by the wrong people (it has been reported for example that an U.S. intelligence agency has harvested IR21 document information several years ago), several foreign countries have advised operators to redact some information from public IR.21 documents, or to no longer distribute documents via the GSMA's document repository, to make it a bit more difficult (but not impossible) for bad actors to get access to them. Perhaps (b) (5) .

(U) The following information has been used to compile the list of entities below.

Non-public information

- (U) IR.21 documents advertised by all U.S. operators were obtained, to generate a list of entities, and analyzed to determine information such as their numbering resources (global titles), signaling carriers used and the hardware and software vendors used in each network.
- (U) Information generally known within the industry was added where relevant and available

Public information

- (U) The FCC licensing database was searched to obtain record for the above entities, in particular when it pertains to spectrum license geography, shareholders, and foreign ownership
- (U) Stock holding information was researched for publicly traded companies
- (U) Any foreign nationals appearing as principals or large shareholders for any of the companies were cross checked against OFAC lists.

(U) It is important to note that certain entities are able to get global titles implemented by signaling carriers, without being an FCC regulated mobile operator, and without GSMA membership. In this case, there does not exist a directory or repository where these global titles can be found and there are no regulations or reporting requirements in this regard, so the only way to learn about them is to see them in activity. Therefore, this list is not an exhaustive list of every company that holds U.S. global title resources.

(U) The OFAC manages lists of foreign individuals with whom U.S. companies are not permitted to do business, according to various policies of the United States (mainly trade embargoes or security risks). All names of foreign citizens associated with any of the companies below have been cross referenced

against OFAC embargo lists, but as expected, none of the names were found on any such lists, since this task presumably was already a part of the review by the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (formerly "Team Telecom").

(U) The points below describe the significance of some of the information provided for each operator:

1. (U) An operator's website is interesting because it reveals the services offered by the operator. For example, for some of the companies listed, the website clearly shows that the company is not in the traditional operator business. Furthermore, the level of sophistication or age of the website can sometimes give clues as to whether a company is actively seeking end users for a legitimate mobile service, or if the operation could merely be a front for other non-end-user facing activities.

2. (U) The question of whether a company operates a radio network or not, can again shed some light as to whether the company is actively pursuing a legitimate mobile operator business, or if the sole purpose of obtaining a spectrum license is to join the GSMA and obtain access to numbering resources used for global titles and signal on the SS7 network. Furthermore, not operating an active radio network can lead to cancellation of a spectrum license (if brought to the attention of the FCC), which in turn could lead to termination of GSMA membership (if brought to the attention of the Association).

3. (U) The licensed area is of interest to see if it matches the geography in which the company operates or claims to offer services or markets services. Some companies are setup for the sole purpose of obtaining national roaming agreement to access the networks of the nationwide operators at a wholesale price, and then resell this service for various purposes. A company marketing services to clients nationwide, but without nationwide spectrum licenses, would be a clear indication for this behavior. Furthermore, a company having a spectrum license in a certain area, and its main offices in a completely different area, can also indicate an ulterior motive and is often a good reason to look further into a company's activities.

4. (U) The FCC Registration Number (FRN) uniquely identifies the company in the databases of the FCC. Using this identifier, it is possible to easily lookup which spectrum licenses are assigned to the company, what the company's ownership is, and any infractions committed by the company. The FRN for a company can be searched here: https://apps.fcc.gov/coresWeb/simpleSearch.do

5. (U) Any spectrum licenses assigned to a company anywhere in the U.S. can be searched by FRN or entity name here: https://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp

6. (U) The GSMA membership indicates whether the company is an active member of the GSM Association. Full membership in the Association generally requires a spectrum license for a frequency approved for GSM service, and this membership is generally required to advertise numbering resources on the SS7 network and communicate with other operators domestically and internationally.

7. (U) The IMSI range, which in the United States is currently managed by iconectiv, is used to uniquely identify subscribers of each operator. When conducting attacks against subscribers, the IMSI identifier of the target subscriber is often required. Using the ranges allocated here, it is possible to identify which operator a subscriber originates from, which can be useful when investigating forensic attack data. Law enforcement routinely picks up IMSI identifiers when conducting surveillance using IMSI catchers for example and would use IMSI ranges to identify to which operator it may have to submit a warrant for further lawful intercept.

8. (U) The global title range is the range of global titles authorized to send and receive SS7 messages on behalf of each operator. These numbers are assigned to operators as telephone number ranges under the NANPA, which in United States is currently managed by Somos Inc.

9. (U) The SCCP, IPX, and GRX carriers are companies to which each mobile operator connects in order to exchange signaling messages with other operators (domestically and internationally) for the purpose of roaming. Some operators connect to multiple carriers for each vendor for redundancy and routing diversity purposes.

ANSI SCCP

(U) ANSI SCCP is the carrier used by operators to exchange SS7 messages natively with other North American operators for the purpose of domestic roaming. Traditional rural mobile operators without nationwide coverage have an ANSI SCCP carrier which they use to exchange messages for national voice and SMS roaming. Some operators do not list an ANSI SCCP carrier. In this case, it is still possible to communicate with other North American operators using the ITU SCCP connection (ITU is the international format of SS7 messages), but messages will be converted back and forth between ANSI (North American) format and ITU (International) format by one of the SCCP carriers in the chain. In most cases, those ITU messages will transit outside of the United States into a foreign country (where they can be monitored or intercepted) and back to the United States. This also typically adds a cost to the operator versus exchanging straight ANSI messages.

(U) The diagram below shows the signaling path in this scenario:

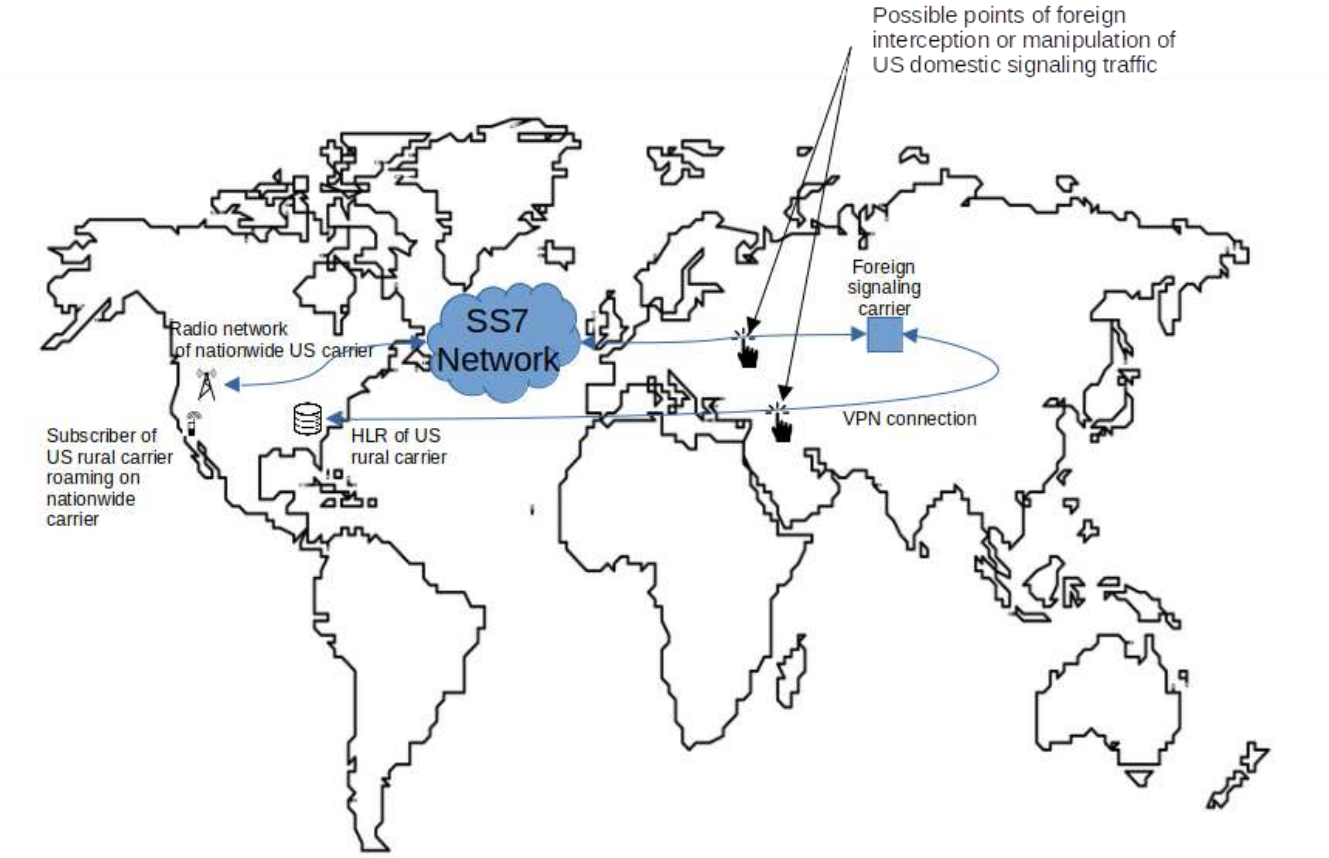


Figure 3: ANSI SCCP - ITU SCCP Signaling Path

Key Factors for consideration:

- (U) An operator who does not have a native ANSI connection deserves additional scrutiny because it may not have a traditional North American mobile operator business and could be a front for other activities.

- (U) Note that every operator which does not list an ANSI SCCP carrier should not automatically be suspicious, as some operators simply do not know how to fill out the mandatory GSMA documentation. Other factors must be considered, and a combination of unusual attributes is what makes an operator suspicious.

- (U) ITU SCCP is the carrier used to exchange SS7 messages (for voice and SMS roaming) with operators outside of North America. These messages typically leave the United States, regardless of whether they are carried by a U.S. or non-U.S. signaling carrier and are used for international roaming purposes. Most operators have this type of connection if they wish to offer international roaming services to their subscribers.

- (U) IPX carrier is the carrier used to exchange Diameter messages used for LTE roaming. In the case of LTE, both messages for North American and international operators go over the same connection. If this IPX carrier is located overseas, then all Diameter signaling messages will leave the United States to a foreign country, where they can be monitored or intercepted, even in the case of U.S. domestic roaming. Note that the interception in this case applies only to the signaling messages, not to any payload.

- (U) GRX carrier is the carrier used to exchange packet data (i.e., IP traffic) for data roaming. As in the case of Diameter, both messages for North American and international operators go over the same connection, so if the GRX carrier is located overseas, then all data roaming traffic will leave the United States to a foreign country (and return in case of domestic roaming). Unlike Diameter messages, (b) (7)(E)

- (U) The list of network element vendors allows us to discover which operators are using foreign made network equipment that may have been prohibited by the U.S. government, or that could be of future concern. Note also that most network equipment vendors usually have VPN connectivity into the mobile operator networks in which they have installed equipment, in order to fulfill their support contracts. This connectivity is typically used from support centers located in foreign countries, where wages are lower and the opportunity for bribery higher.

- (U) Better secured operators have VPN connections that are firewalled such that CPNI information for U.S. subscribers is not accessible, and the best secured operators only enable VPN connections during specific windows when maintenance is needed. (b) (7)(E)

- (U) It is also worth mentioning that while the FCC has strict rules in place when it comes to limiting access to CPNI information for U.S. subscribers, operators need to provide a report on their methods for securing such data annually. Most mobile network node (an MSC for example) can write call detail records as part of their normal operations or special logging functions, and any offshore employee of the equipment vendor in charge of supporting/maintaining such an MSC would have full access to these records (or would be able to enable logging to start producing these records, if they are not produced by default. There is no way to prevent this. In a similar way, employees of the HLR vendor would have full access to its internal database that ties Mobile Station International Subscriber Director Number (MSISDNS) to IMSIs, and

employees of the SMSC vendor would have access to internal logs of the SMSC which could contain payloads of certain messages or be able to activate such logs, if they are not active by default. So many more people have potential access to CPNI than just those with direct access into consumer facing systems of an operator.

- (U) Recently, there have been reports of mobile equipment connected to the SS7 network generating attacks towards third parties, of which the operator was not aware and not a part of. It is easy to imagine that such attacks could have been carried out by employees of the equipment manufacturer having access to such nodes.

- (U) Because the access is inevitable, a good practice is to implement privileged session monitoring systems, where sessions of everyone accessing key systems are recorded for later audit if necessary.

- (U) The signaling firewall deployment indicates if according to our information, the operator has deployed a signaling firewall solution to protect its network.

- (U//FOUO) The key person identified for each operator could be of interest either if the person is known as a possible bad actor, subject to a current investigation, or to identify operations that may be managed or controlled by the same individuals.

- (U) Foreign ownership shows whether the operator is foreign owned or controlled according to information reported to the FCC. By analyzing this information, we were able to identify some surprising situations.

- (U) Any additional information of interest or well-known industry information has been added in the Notes section in each table respectively hereunder.

List of Entities Controlling U.S. Global Title Resources:

Nationwide Operators

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Nationwide mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Nationwide
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310016; 310030; 310070; 310080; 310090; 310150; 310170; 310280; 310380; 310410; 310670; 310680; 310950; 311070; 311090; 311180; 311190; 312090; 312670; 312680; 313210
Global Title Range	131231; 170450; 120990; 126053; 197037; 126057; 136033
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Yes, Adaptive Mobile
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Publicly traded, no shareholder owns more than 10% stock.
Notes	
(b) (7)(E) operates a maritime network extension which provides coverage (b) (7)(E) that move around the world.	
Additional IMSI ranges used for (b) (7)(E) : 313100; 313110; 313120; 313130; 313140	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Nationwide mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Nationwide
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310160; 310200; 310210; 310220; 310230; 310240; 310250; 310260; 310270; 310310; 310490; 310660; 310800; 310120; 310830; 311260; 311490; 311870; 311880; 311882; 311940; 312190; 312240; 312250; 312530; 316010
Global Title Range	140445; 150351; 156227; 150545; 180825; 140547; 133433; 164662; 170434; 120631
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	(b) (7)(E)
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) (b) (7)(E) (b) (7)(E)

Notes

(U//FOUO TLP: Amber) (b) (7)(E) connects to ANSI STPs located in (b) (7)(E) which could theoretically cause SS7 signaling traffic for U.S. persons roaming domestically to transit through (b) (7)(E) .

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Nationwide mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Nationwide
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310010; 310010; 310012; 310013; 310350; 310590; 310591; 310592; 310593; 310594; 310595; 310596; 310597; 310598; 310599; 310820; 310890; 310891; 310892; 310893; 310894; 310895; 310896; 310897; 310898; 310899; 310910; 311110; 311270; 311271; 311272
Global Title Range	1903702; 1903638; 1903932
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	(b) (7)(E)
Other information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Owned by (b) (7)(E) which is publicly traded with no single shareholder owning over 10% of stocks.
Notes	
Operator is publishing a dedicated IMSI range on IR.21 used for IOT services	

Large Regional Operators

(b) (7)(E)	(b) (7)(E)
Operation	
Type of operator:	Regional mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	23 states
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310730; 311220; 311580
Global Title Range	1773
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	
ITU (International) SCCP carrier:	
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

Small Operators

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Alaska
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310050; 310190
Global Title Range	1907444
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other information	
Key person:	(U//FOUO TLP: Amber) (b) (7)(E)
Foreign ownership/control:	No
Notes	
Hosts a (b) (7)(E) mobile network with the identifier (b) (7)(E)	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Alaska
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	312760
Global Title Range	1907367
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Cooperative owned by its members.
Notes	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	IOT Connectivity provider
Radio network deemed to be operating:	No
Licensed area:	Minnesota
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	312210
Global Title Range	1320330; 1915222
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) (b) (7)(E) (b) (7)(E)

Notes

(U//FOUO TLP: Amber) (b) (7)(E) had access to mobile spectrum via a lease (b) (7)(E) (b) (7)(E) There is no evidence of active radio network operators and the company claims to sell GPS tracking devices. Even though the (b) (7)(E) , it is likely that the company or some of its employees still have access to global title and IMSI resources and may still be actively communicating on the SS7 network.

(U//FOUO TLP: Amber) The IR.21 document (b) (7)(E) . If this number range were to be used to serve U.S. based customers or devices, there is a possible risk of intercept of communications by law enforcement agencies from a foreign country.

(b) (6) is known in the industry for being involved in multiple companies with access to spectrum and signaling resources, and no legitimate radio network operations. There is however no indication that resources were used for nefarious purposes in any of his ventures.

(U//FOUO TLP: Amber) The (b) (7)(E) , indicating that the company may be in (b) (7)(E) .

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	CLEC (local telephone provider, non-cellular)
Radio network deemed to be operating:	No
Licensed area:	New York
FCC FRN:	(b) (7)(E)
GSMA membership:	No
Numbering	
IMSI Range	None
Global Title Range	12018851; 15167080; 19299990; 16466991; 17182890; 18459159
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	Unknown
ITU (International) SCCP carrier:	Unknown
IPX carrier:	N/A
GRX carrier:	N/A
Network element vendors:	Unknown
Signaling firewall deployment:	N/A
Other information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) The company is owned by (b) (7)(E) . The ownership of that company is unknown. Its CEO is (b) (7)(E), (b) (6).

Notes

(U//FOUO TLP: Amber) (b) (7)(E) . It is included in this list because it was detected by Adaptive Mobile's SIGIL system as transmitting nefarious SS7 traffic using GTs which are landline numbers assigned to the company. This is one example of a company who has been able to get its number ranges implemented and routed by signaling carriers, even though (b) (7)(E)

(U//FOUO TLP: Amber) (b) (6) of (b) (7)(E) , operates a company specializing in surveillance solutions. Although the solutions are depicted as CCTV solutions, it could be more than a coincidence that (b) (6) is also active in the surveillance industry.

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	LA, TX
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310570
Global Title Range	1318854; 1406597
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E)
Network element vendors:	(U//FOUO TLP: Amber) (b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	NC
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310130; 312470
Global Title Range	1336426
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6) , CEO
Foreign ownership/control:	No. Owned by 2 cooperatives
Notes	

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator. Also provides MVNO hosting and global roaming services under the (b) (7)(E) .
Radio network deemed to be operating:	Yes
Licensed area:	TX
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310630
Global Title Range	1940238
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) 100% owned by (b) (7)(E) dual national

Notes

(U//FOUO TLP: Amber) The company is known in the industry for reselling U.S. IMSI ranges to foreign entities to allow domestic roaming on U.S. networks at reduced costs.
(U//FOUO TLP: Amber) The company also hosts a network node manufactured by (b) (7)(E) (b) (7)(E) (b) (7)(E) , (b) (7)(E), (b) (6) (b) (7)(E), (b) (6) a well-known geolocation company.
(U//FOUO TLP: Amber) Of the several nodes provided by (b) (7)(E) listed on the IR.21, at least one has been detected generating malicious signaling traffic.
(U//FOUO TLP: Amber) When such traffic originates from U.S. global titles assigned to (b) (7)(E) low end signaling firewalls from U.S. operators may be bypassed in some cases.
(U//FOUO TLP: Amber) (b) (7)(E) (b) (6) also control foreign global titles via various leasing agreements, from which nefarious traffic may be originated. In addition to the signaling from providers listed on the IR.21, signaling may also be carried through (b) (7)(E) with whom the company has an IMSI resale agreement.

(b) (7)(E)	(b) (7)(E)
Operation	
Type of operator:	Provides roaming coverage in unserved areas. Operates retail service under (b) (7)(E) brand which is unrelated to the rural mobile operator of the same name.
Radio network deemed to be operating:	Yes
Licensed area:	CA, NV, AZ, UT, CO, ID, NM, WY, MT
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311550; 312370; 311040; 311320
Global Title Range	13033197; 13407719
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) No. Owned by (b) (7)(E) publicly traded. Largest shareholder (b) (7)(E) , owns 26%.
Notes	
The holding company (b) (7)(E) also owns cellular operations in the countries of Guyana, Bahamas and U.S.VI. (b) (7)(E) leases global titles to SMS messaging companies as well as signaling security auditing companies.	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	KY
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310750; 312120; 312130; 312910
Global Title Range	1913814
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	IOT provider with focus on agriculture
Radio network deemed to be operating:	No
Licensed area:	WA
FCC FRN:	(b) (7)(E)
GSMA membership:	No
Numbering	
IMSI Range	312410
Global Title Range	Unknown
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	Unknown
ITU (International) SCCP carrier:	Unknown
IPX carrier:	Unknown
GRX carrier:	Unknown
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural wireless internet provider
Radio network deemed to be operating:	Yes
Licensed area:	KS, LA
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310610
Global Title Range	1620360; 1214658
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E)
Network element vendors:	NSN
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (7)(E)
Foreign ownership/control:	No
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Offers private LTE, messaging, and VAS services
Radio network deemed to be operating:	No
Licensed area:	TX
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310990
Global Title Range	1512777
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	
(U//FOUO TLP: Amber) This type of MVNE business is often involved in leasing global titles from or to others, although we have no specific information that this company is doing so.	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Most likely
Licensed area:	PA
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311030
Global Title Range	1570858
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Multi-IMSI mobile service for international travelers and IOT
Radio network deemed to be operating:	The radio network was operating as of circa 2008. It is most likely still operating.
Licensed area:	MT
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310300
Global Title Range	1406312
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	
Foreign ownership/control:	(U//FOUO TLP: Amber) (b) (7)(E) , which is 80.59% indirectly owned by (b) (6) and (b) (6) , both Russian citizens. Hence the company is majority Russian controlled.

Notes

(U//FOUO TLP: Amber) Company controls multiple IMSI ranges and GT ranges from operators in different countries and is licensed as a facilities-based MVNO in several foreign countries.

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator that also sells IOT services and wholesale mobile services (MVNE) / multi-IMSI services
Radio network deemed to be operating:	Yes
Licensed area:	PA
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310690; 311600; 312180; 90166
Global Title Range	1610468; 1610302; 1570716; 1814222; 883290
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	Not according to FCC filings

Notes

(U//FOUO TLP: Amber) This operator was originally called (b) (7)(E) (b) (7)(E) and was known in the industry for reselling its IMSI ranges to foreign companies, providing access to (b) (7)(E) and (b) (7)(E) national roaming coverage at local rates.
(U//FOUO TLP: Amber) (b) (7)(E)
It went (b) (7)(E) in 2019. According to FCC filings, it is currently owned strictly (b) (7)(E) , however its website claims affiliation to the (b) (7)(E) , and its shareholders operate other similar businesses in (b) (7)(E), for example (b) (7)(E) which has been associated to nefarious SS7 traffic in the past.
(U//FOUO TLP: Amber) The company is advertising (b) (7)(E) (b) (7)(E) on its IR.21.
(U//FOUO TLP: Amber) The company has a reputation of renting global title resources to third parties. (b) (7)(E) used to have access to global title resources from various countries, both via licensing as facilities based MVNO and via rental agreements before its bankruptcy. Operations currently remain (b) (7)(E) .

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	KS
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310340
Global Title Range	16205755
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Owned by a cooperative which is owned by its members.
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Provides hubbing services, roaming services and MVNE
Radio network deemed to be operating:	No
Licensed area:	MN
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311240; 313070; 311700
Global Title Range	1907429; 1907292
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No

Notes

(U//FOUO TLP: Amber) The GT range is located in Alaska, assigned to (b) (7)(E) , and inconsistent with the radio license area. The IMSI range 311240 is assigned to (b) (7)(E) (b) (7)(E) as well. Either (b) (7)(E) provides MVNE services to (b) (7)(E) (b) (7)(E) has leased its Global Title Range to Midwest Network Solutions Hub.

(U//FOUO TLP: Amber) Furthermore, the signaling carrier (b) (7)(E) used by the company is very unusual, and this company in turn claims to be offering network hosting and MVNE sponsoring.

(U//FOUO TLP: Amber) These types of MVNE businesses are often involved in leasing global titles from or to others, although we have no specific information that this company is doing so.

(U//FOUO TLP: Amber) (b) (6) is known in the industry for being involved in multiple companies with access to spectrum and signaling resources, and no legitimate radio network operations. There is however no indication that resources were used for nefarious purposes in any of his ventures.

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator (according to website)
Radio network deemed to be operating:	The website claims that a radio network exists
Licensed area:	MO
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	312630
Global Title Range	1660570
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	None listed
ITU (International) SCCP carrier:	(b) (7)(E) (Milano and Rome)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) Ownership information not available in FCC database (this is unusual)

Notes

(U//FOUO TLP: Amber) Based on several unusual characteristics of this operation (unprofessional website, use of smaller foreign signaling carriers, missing information etc.), further investigation was conducted.

(U//FOUO TLP: Amber) It appears that the officers of the company are the same than those of the company (b) (7)(E) which manufactures LTE bubble systems and IMSI catchers among other things and claims to have contracts with DOD. The operation in (b) (7)(E) does not look like a normal rural mobile operator business, and it is questionable whether actual network coverage exists. The business address for (b) (7)(E) is the same as the address of (b) (7)(E) in (b) (7)(E) .

(U//FOUO TLP: Amber) Unless this company is a legitimate supplier known to the U.S. government, (b) (7)(E), (b) (5)

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	MVNE services and private LTE
Radio network deemed to be operating:	Probably not. The company's own spectrum license expired in 2010. However, the company probably broadcasts multiple radio networks on behalf of the operators which it hosts.
Licensed area:	Formerly MN
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311530; 310460
Global Title Range	1320469
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No

Notes

(U//FOUO TLP: Amber) The company is a GSMA member, even though it currently does not meet requirements (b) (7)(E)

(U//FOUO TLP: Amber) This type of MVNE business is often involved in leasing global titles from or to others, although we have no specific information that this company is doing so.

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	KS
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311100; 312420
Global Title Range	1785639
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No, owned by cooperatives which are in turn owned by their members
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	WI
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310510; 311840; 311850
Global Title Range	1920; 1715; 1534; 1906 (information is likely filled in incompletely in the IR.21, as the ranges should be longer)
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	
(U//FOUO TLP: Amber) The company is publishing a dedicated IMSI subrange for M2M operations in its IR.21, so it is likely active as a IOT service provider.	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	IOT operator
Radio network deemed to be operating:	No
Licensed area:	(U//FOUO TLP: Amber) There is no evidence that the current company owns any spectrum license.
FCC FRN:	
GSMA membership:	(U//FOUO TLP: Amber) Yes. GSMA membership was probably obtained via one of the wireless networks acquired in the past.

Numbering	
IMSI Range	310440; 310640
Global Title Range	1920707; 1920713; 1920292; 1770661

Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E) . Some of the MVNOs hosted by the company use (b) (7)(E) in addition to (b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown

Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) Although this is not disclosed, due to the lack of FCC jurisdiction, the company is presumably owned by (b) (7)(E) which is a publicly traded company. The largest shareholder is private equity firm (b) (7)(E) with 12% ownership.

Notes

(U//FOUO TLP: Amber) (b) (7)(E) was acquired by (b) (7)(E) in 2017, and the following additional networks have been merged into the same over time: (b) (7)(E) , (b) (7)(E) The company hosts (b) (7)(E) (b) (7)(E) If these networks were to be used to serve U.S. based customers or devices, there is a possible risk of intercept of communications by law enforcement agencies from a foreign country. Since the company does not own a spectrum license, it is not subject to FCC oversight, for example when it comes to foreign ownership.

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Greenfield rural mobile operator in Unalaska, Alaska
Radio network deemed to be operating:	No
Licensed area:	Alaska
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	313380
Global Title Range	1907872
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) Unknown, citizenship information for (b) (6) is missing in FCC records. He is most likely a U.S. citizen though.

Notes

(U//FOUO TLP: Amber) The company is building a new LTE wireless network from scratch using (b) (7)(E) The network does not seem to have launched yet.
While this type of operations often has other angles (roaming resale, multi-IMSI etc.), (b) (7)(E) seems to be genuinely focused on serving (b) (7)(E) based on various information reviewed by the analyst.

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	AK
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311560
Global Title Range	1907995
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Cooperative owned by its members.
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	OK, TX
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311450
Global Title Range	1580206
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	Unknown
Foreign ownership/control:	No. Cooperative owned by its members
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	OK
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311080
Global Title Range	1580306
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(U//FOUO TLP: Amber) (b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	(b) (7)(E)
Radio network deemed to be operating:	No
Licensed area:	TX
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311730
Global Title Range	(U//FOUO TLP: Amber) Unknown (It is highly unusual that a Global Title range is not listed in the IR.21 document)
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	
Network element vendors:	Unknown
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) an active member of the GSMA.	the company is

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	MT; ND
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	312480; 312600
Global Title Range	1701601; 1406688
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(U//FOUO TLP: Amber) (b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Cooperative owned by its members.
Notes	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	AZ
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310320
Global Title Range	19283061; 1928434
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	
This company is one of few providing service across (b) (7)(E)	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	GA, AL, MS
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	312720; 313590; 316011
Global Title Range	1312 (information is likely filled in incompletely in the IR.21, as the ranges should be longer)
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	
ITU (International) SCCP carrier:	
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No. Owned by (b) (7)(E) which is publicly traded, no single party holds over 10%
Notes	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	AK
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	311740
Global Title Range	1907391
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber)(b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	IOT and global roaming multi-IMSI provider
Radio network deemed to be operating:	No
Licensed area:	MO
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310840; 312300
Global Title Range	1417400; 14172968; 14173913; 14176988
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	
ITU (International) SCCP carrier:	(b) (7)(E) (STP in Brussel); T(b) (7)(E) (STPs in Frankfurt and Madrid)
IPX carrier:	(b) (7)(E)
GRX carrier:	
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) 100% indirectly foreign owned, with Canadian, Hungarian and Polish ownership. Hungarian ownership leads to obscure structure with Caribbean trusts and an entity related(b) (7)(E)

(U//FOUO TLP: Amber) (b) (7)(E) is a mobile network node infrastructure manufacturer which was most recently controlled by a group of people in China. The IR.21 document lists a UK number range of 44718. If this number range were to be used to serve U.S. based customers or devices, there is a possible risk of intercept of communications by law enforcement agencies from a foreign country. In addition to the signaling from providers listed on the IR.21, signaling may also be carried through (b) (7)(E) with whom the company has an IMSI resale agreement.

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Utah
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310960; 311860; 312290
Global Title Range	1435 (information is likely filled in incompletely in the IR.21, as the ranges should be longer)
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	
ITU (International) SCCP carrier:	
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E) (b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	Wyoming
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310020
Global Title Range	1307702
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(U//FOUO TLP: Amber) (b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E)——————————(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be	Yes

operating:	
Licensed area:	CO, NE, KS, WY
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310740; 310450
Global Title Range	1970467
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(U//FOUO TLP: Amber) (b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	(U//FOUO TLP: Amber) Unknown. Citizenship information missing in FCC records.
Notes	

(b) (7)(E)——————(b) (7)(E)

Operation	
Type of operator:	Wireless internet for rural areas
Radio network deemed to be operating:	Yes
Licensed area:	Vermont
FCC FRN:	(b) (7)(E)

GSMA membership:	Yes
Numbering	
IMSI Range	311990
Global Title Range	1802692
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber)(b) (6)
Foreign ownership/control:	No
Notes	

(b) (7)(E)

(b) (7)(E)

Operation	
Type of operator:	Rural mobile operator
Radio network deemed to be operating:	Yes
Licensed area:	TX
FCC FRN:	(b) (7)(E)
GSMA membership:	Yes
Numbering	
IMSI Range	310180; 310860; 311000

Global Title Range	1325263; 1325763
Infrastructure and Connectivity	
ANSI (Domestic) SCCP carrier:	(b) (7)(E)
ITU (International) SCCP carrier:	(b) (7)(E)
IPX carrier:	(b) (7)(E)
GRX carrier:	(b) (7)(E)
Network element vendors:	(b) (7)(E)
Signaling firewall deployment:	Unknown
Other Information	
Key person:	(U//FOUO TLP: Amber) (b) (6)
Foreign ownership/control:	No
Notes	

Map of Mobile Operators with Spectrum License

The map below depicts the mobile operators described in the section above according to the area in which they have a spectrum license.

Figure 4: Map of Mobile Operators with Spectrum License

(b) (7)(E)

Mobile Node Vendors

The following table summarizes the mobile node vendors used in each U.S. mobile network according to its IR.21 documents.

(U//FOUO TLP: Amber) Highlighted are those vendors that could be deemed problematic and unwanted in U.S. mobile networks.

(b) (7)(E)

Table 3: Mobile Node Vendors

(U//FOUO TLP: Amber) Table: Mobile node vendors used in each U.S. mobile network

(U) Huawei and ZTE equipment are banned by the U.S. Commerce department due to concerns over equipment being used for espionage. In July 2021, the FCC approved a program to finance the replacement if Huawei equipment in U.S. rural networks, and it should be ensured that the entities listed above follow through with such replacement within a reasonable amount of time.

(U//FOUO TLP: Amber) The equipment produced by (b) (7)(E) could be of concern for similar reasons because the company is a small private Chinese company, its equipment is deployed within a small number of mobile operators worldwide, and there is minimal oversight or accountability.

(U//FOUO TLP: Amber) The equipment produced by (b) (7)(E) is of concern because (b) (7)(E) shares founders/owners with (b) (7)(E) a geolocation company located in Cyprus. (b) (7)(E) is

purported to access the SS7 network and various global titles via (b) (7)(E) nodes deployed worldwide, among other things. Furthermore, malicious SS7 traffic detected as originating from the U.S. mobile operator (b) (7)(E) , was originating from a node identified as (b) (7)(E) in the IR.21 of the operator.

(U//FOUO TLP: Amber) Both (b) (7)(E) and (b) (7)(E) should be investigated further, to determine if they should be added to the list of blacklisted equipment vendors.

Other Major Telecom Security Gaps Which are Used to Undermine U.S. National Security

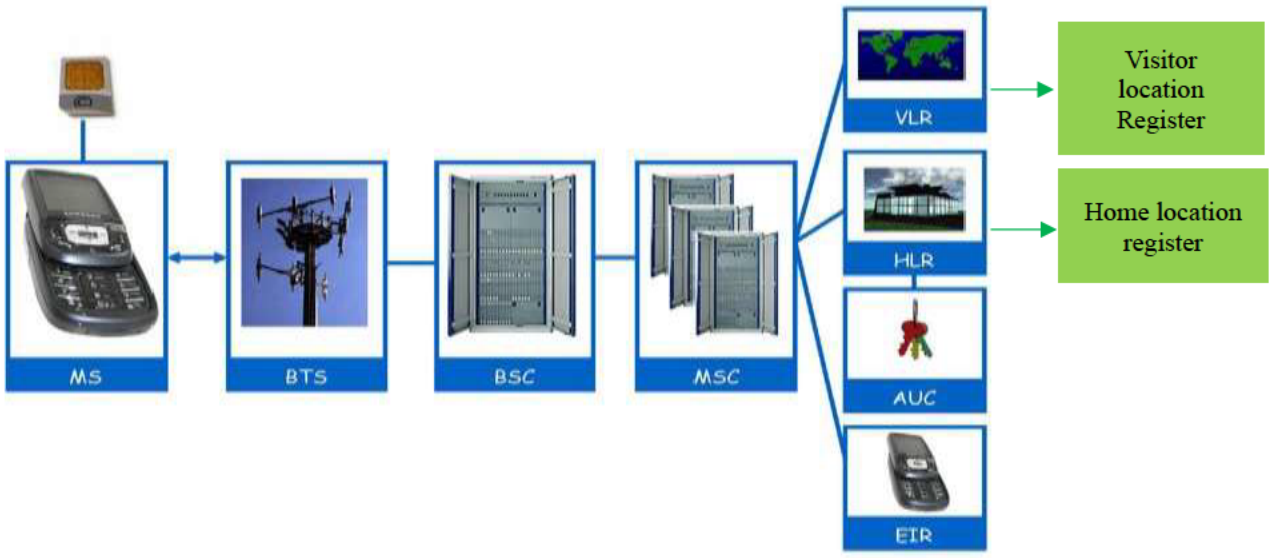


Figure 5: Additional Telecom Security Gaps

(U) US mobile subscribers' key mobile identifiers are held on a piece of telecom equipment called the HLR (Home Location Register). This register holds the MSISDN (phone number), IMSI (identifies the network) and IMEI (equipment identifier –confirms what type of device) – these are all critical data points. Once the attacker, has phone number, will try to acquire the IMSI to facilitate call interception, location, file extraction etc. There is a combination of strong and moderate security protecting these data resource in the US.

(U) However, if roaming in the US from overseas, i.e., a non-US subscriber, you will reside on the VLR, the visitor location register. On the basis that US carriers are not obliged to provide security for non-customers (it would be a hard sell), so there is not and never has been any security for VLRs. This is a well-known fact and is exposed by several national security agencies, checking to see who is in the US, at specific areas at specific times.

(U//FOUO TLP: Amber) We have seen many attacks in the US on VLRs, especially in the DC, New York (UN), Virginia, Maryland (Gaithersburg) area which we believe are connected to visits to major US security industry companies. We recommend a (b) (5) .

Recorded Attacks Originating from U.S. Global Title Holders

(U//FOUO TLP: Amber) By sitting in the signaling path of large operators who receive vast amounts of signaling messages, it is possible to analyze the signaling messages sent by many different roaming partners from around the world, and identify the senders of unpermitted messages, considered attacks. This analysis can be conducted down to individual sending global titles, such that the sending operators

could later be approached and possibly identify the individual applications, node vendors or lessee behind each global title.

(U//FOUO TLP: Amber) AdaptiveMobile Security conducts this type of analysis through a number of firewall installations in large operators worldwide, with their consent. Where permitted by the operator, anonymized data is gathered and centrally reported through Adaptive Mobile's SIGIL platform.

(U) Detecting an attack originating from a U.S. operator does not automatically mean that the operator in question is directly behind the attack. There are different possible scenarios in which the activity may reflect abuse of access in unauthorized and/or unlawful activity by (or on behalf of) a threat actor.

(U) Scenario 1: the U.S. rural carrier may have leased global titles to a third party (often foreign) and may not be aware what the third party is doing with the leased resources. Often, the parties leasing the resources have a cover business, such as an SMS messaging business, under which pretenses they enter into the agreement.

(U) Scenario 2: The U.S. rural carrier is not an accomplice in the scheme, but its resources are used by foreign equipment vendors' personnel that have access into the network, without the carrier's knowledge.

(U) Scenario 3: The U.S. rural carrier is a front for foreign bad actors. This possibility is greater when the rural carrier is foreign owned or if its operations do not seem like those of a normal rural mobile operator and it is not broadcasting a radio network.

(U) The following diagram shows how third parties located in a foreign country can remotely access and control U.S. global title resources and target other U.S. mobile carriers and their U.S. subscribers.

(b) (7)(E)

(U//FOUO TLP: Amber) We have analyzed data for suspicious signaling message recorded in (b) (7)(E) during the past 12 months that originated from global titles of U.S. number ranges.

(U//FOUO) The following attacks have been detected.

(U//FOUO TLP: Amber) (b) (7)(E)	
Offending GTs:	12018851498, 15167080960, 19299990890, 16466991840, 17182890530, 18459159860
Type of attacks:	Resolution of IMSI; Geolocation
Part of coordinated multi-country attacks:	Yes
(U//FOUO TLP: Amber) Notes	
(U//FOUO TLP: Amber) This company is a landline carrier (CLEC) and one of few that has managed to activate its landline numbers as GTs with signaling carriers, even though it is not active in the mobile industry. The GTs come from multiple ranges, all of them assigned to the company in both New York and New Jersey. The company could theoretically have new number ranges assigned and routed at will if previously used numbers got blocked.	

(U//FOUO TLP: Amber) (b) (7)(E)	
Offending GTs:	13033197374
Type of attacks:	Geolocation; Advanced attacks
Part of coordinated multi-country attacks:	No
Notes	
(U//FOUO TLP: Amber) This global title is leased to The (b) (7)(E) which uses it to conduct legitimate penetration tests. The usage of this global title is legitimate.	

(U//FOUO TLP: Amber) (b) (7)(E)	
Offending GTs:	13204699481, 17632073009, 17632073017
Type of attacks:	IMSI resolution
Part of coordinated multi-country attacks:	No
Notes	
(U//FOUO TLP: Amber) (b) (7)(E) hosts multiple wireless networks on its core network nodes, so it can be difficult to identify specifically who had access to which resources at a specific time.	

(U//FOUO TLP: Amber) (b) (7)(E)	
Offending GTs:	16104680058, 16104680077
Type of attacks:	Geolocation

Part of coordinated multi-country attacks:	Yes

Notes
(U//FOUO TLP: Amber) These GTs have been linked to one of the leading geolocation platforms which services are offered for sale to law enforcement worldwide at surveillance industry trade shows

(U//FOUO TLP: Amber) (b) (7)(E)	
Offending GTs:	19402389973, 19402389941
Type of attacks:	Call interception precursor
Part of coordinated multi-country attacks:	No

Notes
(U//FOUO TLP: Amber) This company is the only mobile operator in the U.S. to declare hosting an (b) (7)(E) equipment (company affiliated to (b) (7)(E)) in its network, and one of the suspicious messages detected originates from one of the (b) (7)(E) nodes, according to the IR.21 information.

(U//FOUO TLP: Amber) It is recommended to (b) (5)

Conclusion

(U//FOUO) With massive reported data losses over the past decade such as the Office of Personnel Management data breach in 2015, the "hijacking" and [27](b) (7)(E) , and the five-year breach at (b) (7)(E) from 2016 to 2021, the US has potentially lost significant valuable data to adversaries. Such breaches reinforce the requirement for immediate mitigation to reduce the attack surface by closing gaps in telecom cyber defenses against adversaries seeking to compromise the national security of the United States of America.

(U) Under 5G, signaling protocols and IP protocols converge. The U.S., while having 4.3% of the world's population, generates 33% of the world's IP traffic[28]. Coupled with the fact, that the GSMA projects that 5G will bring over $700 billion in global economic value and a $1.5trn[29] addition to US GDP with enterprise representing 68% of the market led by retail, Government, and finance applications, something needs to happen because security must not be an afterthought.

(U//FOUO TLP: Amber) It is important to highlight that, although the potential threat activity described in examples (2) and (3) earlier in this report was successfully detected and blocked by AdaptiveMobile Security, the attack outlined in example (1) Likely Surveillance of Inbound Roamer – is assessed as likely to have succeeded, as are others similarly directed, due to a gap in the operator's defences (note: lying outside the scope of the contract between AdaptiveMobile Security and the operator). It is also important to highlight that the most persistent, aggressive, and well-resourced threat actors continually conduct reconnaissance of the networks of a targeted country so as to identify the gaps in national defense. The unique prevalence of national (domestic) roaming arrangements within the U.S. telecoms ecosystem means that certain gaps (in the form, for example, of potentially compromised or compromisable operators) can potentially present a single point of failure in U.S. national security. For that reason, there is no such thing as a 15% problem where for example, 15% of U.S. traffic might be determined to be unprotected by dynamic zero-trust architecture, rather a 15% gap must be considered to represent 100% of the potential national security threat as that gap is where the most significant threat activity is likely to be directed by Hostile State Actors. In other words, mitigation of the potential threat means implementing threat protection at a national level for all traffic.

(U) Accordingly, based on our global experience of telecom security, we present several recommendations to CISA who has the mission to protect the Cybersecurity Infrastructure of the United States –Telecoms as a National Critical Function at the heart of that infrastructure. These recommendations have centered on key principles of (b) (5) , and (b) (5) .

[27] https://digitalcommons.usf.edu/mca/vol3/iss1/7/
[28] https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom-State-of-Industry-2020.pdf
[29] https://www.accenture.com/ie-en/insights/high-tech/5g-economic-impact#:~:text=U.S.%20economy%20will%20drive%20up,be%20felt%20in%20every%20industry.

(b) (5)

(U) As indicated earlier in this report, telecom traffic since the inception of networks has been exchanged on the basis of "trust", defined in the following points:

- (U) Trust that it is from the country and person it purports itself to be from.
- (U) Trust that the communication contains no malicious intent, i.e., malware
- (U) Trust that the content (message), connection (call) is not distorted, misconfigured, or diverted by a malicious intermediary.

(U) Trust as a 20th century design principle is not fit for purpose in a 21st century security environment. How can any receiving network know that the traffic originating network has the same commitment to security that they do? Quite simply they cannot. Today no carrier, external to the U.S. and sending traffic, should be trusted. (b) (5)
must be adopted.

(b) (5)

(U) Post 9/11, the U.S. Government imposed strenuous conditions on international airlines ensuring they did not carry passengers or visitors to the U.S. who did not have the correct permission to travel. By doing this the onus was transferred the to the airlines, compelling them to ensure the avoidance of a fine or ultimately a ban, the airlines made sure each passenger was suitably cleared for travel.

(U//FOUO TLP: Amber) We believe the same mechanism should be considered used for the transit of telecom traffic into the U.S. This, we believe could be achieved seamlessly. Almost 100% of international mobile roaming traffic is transited to the U.S. through aggregators (e.g., (b) (7)(E)
interconnect carrier services) some of which do not have POPs (points of presence) in the U.S., and mostly arrives through (b) (7)(E) or those aggregators who have points of presence in the U.S. By regulating/legislating these aggregators are responsible for ensuring they are not carrying or distributing malicious traffic into the U.S. which transfers the security onus on to them as opposed the existing model which encourages from a financial standpoint of transiting as much traffic as possible so as to get compensated on the volume of traffic delivered. A (b) (5)

would in our view change the dynamic very quickly.

Glossary

ANSI (American National Standards Institute)
(U) The American National Standards Institute is a U.S. organization that recommends standards for many products in various industries. As it pertains to the telecommunications industry, ANSI refers to a variant of SS7 signaling used in North America which is different and not directly compatible with the ITU variant used in most of the rest of the world. ANSI SS7 uses different types of point codes, valid only within North America, and a special translation service is required in order to convert between ANSI SS7 messages and ITU SS7 messages.

CBRS (Citizens Broadband Radio Service)
(U) CBRS is shared wireless spectrum in the U.S. that is set aside for private broadband radio networks. This spectrum has a light licensing framework which allows more entities to deploy CBRS networks. Some CBRS networks will have interworking capabilities with traditional GSM networks.

CPNI (Customer Proprietary Network Information)
(U) CPNI is confidential information about a customer's purchase and use of telecommunications services, including call detail records, location information and billing information.

DRA (Diameter Routing Agent)
(U) A Diameter Routing Agent (DRA) is a functional element in a mobile network that provides real-time routing capabilities for Diameter messages. It performs the same functionality as a STP, but for Diameter signaling.

eSIM
(U) An embedded-SIM (eSIM), or embedded universal integrated circuit card (eUICC), is a form of programmable SIM that is embedded directly into a device's storage/memory. eSIMs are used in IOT devices and increasingly in mobile phones and tablets, due to the ability for MNOs to provision them via the Internet without having to mail physical SIM cards.

Geolocation
(U) Geolocation, aka tracking, is the ability to obtain, usually surreptitiously, the location of a subscriber from the mobile network.

Global Title
(U) A global title is an address used to route SS7 messages and looks like a phone number with a country code. A different address is assigned to each node within a mobile network. For example, each HLR in a network will have a different address, and each MSC will have a different address as well.

GSM (Global System for Mobile Communications)
(U) The Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunications Standards Institute to describe the protocols for digital cellular networks used by mobile devices such as mobile phones and tablets.

GSM Association
(U) The GSM Association or GSMA is a trade association based in London, in which most MNOs in the world are a member. The GSMA facilitates roaming between its members and facilitates the exchange of IR.21 documents between members.

GGSN (Gateway GPRS Support Node)
(U) A node used for data service in the mobile network. The GGSN receives data packets from the SGSN and outputs these packets on the Internet, allowing subscribers to consume data services.
The GGSN is connected to both the public Internet, and to the GRX in order to allow for data roaming.

GRX (GPRS Roaming Exchange)
(U) A worldwide private data network used by mobile operators to peer together in order to enable seamless data roaming between their subscribers. Mobile operators usually access the GRX network via a subscription from a GRX carrier.

HLR (Home Location Register)
(U) The Home Location Register (HLR) is a database that is maintained by each mobile network operator to store details of their subscribers for authentication and service provisioning purposes, as well as for the purpose of delivery incoming calls and text messages. The HLR database includes a unique identifier (IMSI) for each SIM card, the telephone number (MSISDN) currently assigned to that IMSI, details about which services the SIM card is allowed to access and which Mobile Switching Center (MSC) and Visitor Location Register (VLR) is currently servicing the subscriber.

IMEI (International Mobile Equipment Identity)
(U) The International Mobile Equipment Identity (IMEI) is a number that uniquely identifies a device used on a mobile phone network. The IMEI number is unique and typically 15 or 17 digits made up of an 8-digit prefix (the Type Allocation Code / TAC) which is the same prefix for each model of the device and can be used to identify the type of device used by a subscriber. The remainder of the IMEI is unique to each device and randomly generated by the manufacturer of the device.

IMSI (International Mobile Subscriber Identity)
(U) An International Mobile Subscriber Identity (IMSI) is a unique number, usually fifteen digits, that is issued by a Mobile Network Operator and stored within a SIM card. The IMSI uniquely identifies the SIM card and is used to lookup the user profile in the HLR to determine the services available to the user, and to route calls and SMS messages to his device.
The IMSI number is composed of the Mobile Country Code (MCC) followed by the Mobile Network Code (MNC) followed by a unique Mobile Subscriber Identification Number. All IMSIs generated by one Mobile Network Operator will begin with the same MCC and MNC prefix, unless an operator has exhausted all available IMSIs within their allocated range, in which case they can request an additional MNC to be allocated to them by their national regular.
In the United States, several large mobile operators use a large number of different MNC numbers due to acquisitions of smaller (rural) mobile operators over time.

IMSI catchers
(U) An IMSI catcher is a surreptitious device that is able to collect IMSIs of subscribers attaching to cell towers in the vicinity of the device. More sophisticated "active" IMSI catchers are also able to intercept voice, SMS, and data communications of subscribers in its vicinity.
IMSI catchers are not allowed to be used in the United States outside of government, army, and law enforcement operations.

Inbound roamer
(U) Refers to a third-party subscriber roaming onto a network, for example, when talking about (b) (7)(E) a British subscriber roaming onto (b) (7)(E) or a subscriber of a small rural operator roaming onto (b) (7)(E) network.

IoT (Internet of Things)
(U) The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
A large number of IoT enabled devices rely on Internet connectivity provided via mobile networks. Mobile subscriptions dedicated to IoT devices were previously called M2M subscriptions.

IR.21
(U) An IR.21 is a document published by each MNO within the GSM Association and which describes the technical architecture of a mobile network. IR.21 documents contain confidential routing information which can be used to perform SS7-based attacks.

ITU (International Telecommunication Union)
(U) The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for all matters related to information and communication technologies. The ITU promotes the shared global use of the radio spectrum, facilitates international cooperation in assigning satellite orbits, assists in developing and coordinating worldwide technical standards, and works to improve telecommunication infrastructure in the developing world. It is also active in the areas of broadband Internet, wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, TV broadcasting, and next-generation networks.

LTE (Long Term Evolution)
(U) Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements.

M2M (Machine to Machine)
(U) Machine-to-machine, or M2M for short, refers to the automated exchange of information between devices without manual intervention by humans. MNOs often refer to M2M service or M2M subscriptions when talking about mobile services consumed by devices rather than human subscribers. In recent years, the term M2M has increasingly been replaced by the term IOT (Internet of Things).

MCC (Mobile Country Code)
(U) A 3-digit number which uniquely identifies a country. The MCC is different from the international telephone country codes. It is defined in E.212 by the ITU.

MNC (Mobile Network Code)
(U) A 2-to-3-digit number that uniquely identifies a Mobile Network Operator within a country. Most countries in the world use 2-digit MNCs, but larger countries like the United States, Canada, India, and others use 3 digits due to the large number of licensed operators.

MNO (Mobile Network Operator)
(U) A telecommunications company that provides mobile services to end-users and broadcasts their own radio network on licensed radio spectrum. In United States, this radio spectrum is licensed by the FCC.

MVNO (Mobile Virtual Network Operator)
(U) A telecommunications company that provides mobile services to end-users but does not broadcast its own radio network. Instead, an MVNO uses the radio network of an MNO, via a private commercial agreement, to deliver communications to and from the MVNO's customers.

MSC (Mobile Switching Centre)
(U) A Mobile Switching Centre (MSC) acts as a control center for multiple cell towers within one geographical area and is responsible for delivering voice and SMS service to and from the subscriber. If a call is in progress and the subscriber moves into a new cell tower coverage area, then the call is handed off by the MSC to a new tower without dropping. The MSC keeps the VLR up to date with location information such that new voice calls and SMS can be delivered to the subscriber.
In small countries such as island nations, a single MSC can service the entire country, while nationwide operators in the United States can have hundreds of MSCs.

MSISDN (Mobile Station International Subscriber Directory Number)
(U) A telephone number used to uniquely identify a user's subscription within a mobile phone network. The MSISDN is a maximum of 15 digits and is defined by the ITU's E.164 recommendation. The number includes the internationally recognized country code as a prefix, followed by a nationally assigned network or operator code (in USA, the NPA-NXX), and a subscriber number.
In a mobile network, the same MSISDN is used to deliver both voice calls and SMS messages to and from a user.

Multi-IMSI
(U) A type of mobile service subscription where a user profile is made up of multiple IMSIs from different mobile operators, to provide service to a user globally, usually under a single phone number. The active IMSI (the IMSI used to provide service at a specific point in time) is selected in each country based on a particular algorithm, often to optimize the cost of service based on roaming rates. Providing multi-IMSI services to subscribers usually requires a multi-IMSI capable HLR, or a specialized signaling translation platform.

MVNE (Mobile Virtual Network Enabler)
(U) A Mobile Virtual Network Enabler is a telecommunications company that usually operates a mobile core network that is connected to one or more MNOs and is rented out or partitioned to multiple MVNOs to allow the MVNOs to outsource most of their technical operations.

NANPA (North American Numbering Plan Administrator)
(U) NANPA holds overall responsibility for the neutral administration of NANP numbering resources, subject to directives from regulatory authorities in the countries that share the NANP. NANPA's responsibilities include assignment of NANP resources, and, in the U.S. and its territories, coordination of area code relief planning and collection of utilization and forecast data.

NPA-NXX
(U) NPA and NXX are used in the +1 international numbering plan, which covers North America including the Caribbean.
The NPA identifies the 3-digit Numbering Plan Area (Area Code) while the NXX identifies the Central Office (aka. Exchange) within the NPA

OFAC (Office of Foreign Assets Control)
(U) The Office of Foreign Assets Control is a financial intelligence and enforcement agency of the U.S. Treasury Department. It administers and enforces economic and trade sanctions in support of U.S. national security and foreign policy objectives.

OTT applications (Over-the-top application)
(U) An over-the-top (OTT) application is an application offering a service directly to subscribers via the Internet. OTT bypasses telephone, cable and ISP providers. In our context, it is used to describe applications that enable users to communicate with other users directly via voice, SMS, or video call without visibility to, or billing by the MNO.

Outbound roamer
(U) Refers to a home subscriber roaming onto a third-party network, for example, when talking about (b) (7)(E) an (b) (7)(E) subscriber roaming onto a network in United Kingdom, or an (b) (7)(E) subscriber roaming onto a small rural network in an area where (b) (7)(E) does not offer native coverage, for example at the Grand Canyon.

PBX (Private Branch eXchange)
(U) A Private Branch eXchange is a private business telephone system that offers multiple inbound and outbound lines, call routing, voicemail, and call management features.

Point code
(U) An SS7 point code is similar to an IP address in an IP network. It is a unique address for a node (Signaling Point, or SP), used in MTP layer 3 to identify the destination of a message signal unit. Signaling messages usually contain an OPC (Originating Point Code) and a DPC (Destination Point Code).

PSTN (Public Switched Telephone Network)

(U) The Public Switched Telephone Network (PSTN) provides infrastructure and services for public telecommunication. Each telephone company in the world maintains its own network infrastructure but connects to other telephone companies so that all MSISDNs are reachable by all subscribers in the world. This, as a whole, forms the PSTN.

Roaming

(U) The ability for a subscriber to receive services on a GSM network other that his home network, while being billed by his home network. A common application for roaming is the ability for a U.S. subscriber to receive service on foreign networks, while still being reachable on their usual U.S. MSISDN. A subscriber roaming on another network is referred to as a roamer, specifically an outbound roamer.

SCCP (Signaling Connection Control Part)

(U) SCCP is the layer of the SS7 signaling stack which is used to address signaling messages using origin and destination global title numbers. Messages are carried around the world by SCCP carriers whose networks are interconnected.

SGSN (Serving GPRS Support Node)

(U) A node used for data service in the mobile network. The SGSN is located close to radio network and transfers data packets from the subscriber's mobile equipment to the GGSN.
It is normally not connected to the Internet, but connects to the GRX to allow for data roaming.

SIM (Subscriber Identity Module)

(U) A SIM (Subscriber Identity Module) card is a portable memory chip used as subscriber credentials in GSM phones. It stores the unique IMSI identifier for the subscriber, as well as an encryption key, which allows it to authenticate on the mobile network. Some SIM cards are able to store additional information such as a user's phone book contacts and text messages, which can be useful in forensic investigations.
A common misconception is that the user's telephone number is stored within the SIM. This is incorrect as the telephone number is stored in the operator's HLR, and the phone number could be changed without the physical SIM card being changed.

SMSC (Short Message Service Center)

(U) The core network node responsible for the delivery of SMS messages to and from subscribers.

STP (Signaling Transfer Point)

(U) The core network node responsible for routing SS7 messages. Typical mobile networks have two STPs, constituting a redundant pair and located at the edge of the network. The STPs provide the interface between the SCCP carrier or carriers on the outside of the network, and the mobile network nodes inside the network.
Large networks can have dozens of different STPs.
STPs sometimes contain filters and routing tables which screen the destinations to which SS7 messages can be routed.

VLR (Visitor Location Register)

(U) The Visitor Location Register (VLR) is a database that contains a subset of information about subscribers who are currently roaming within a Mobile Switching Center's coverage area. The VLR temporarily includes subscription details for each subscriber being serviced, including both the home network's own subscribers as well as inbound roamers.

The VLR is also the database that stores the cell site information where the SIM card is geographically located. The VLR does not pass the cell tower location information of a subscriber to the HLR, so the most granular location data is stored in the VLR and not the HLR.

VoIP (Voice over Internet Protocol)

(U) Voice over Internet Protocol (VoIP) is a technology used for delivering data from a source to a destination using the Internet. VoIP is most often used for telephone calls, which are often free.

VPN (Virtual Private Network)

(U) A VPN is an arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.