Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

Reply Comments of
Dr. Eric Wustrow
Dr. Dirk Grunwald
Dr. Sangtae Ha
Joseph Lorenzo Hall
Yomna Nasser
Marcus Prem
Ashley Wilson
Electronic Frontier Foundation (EFF)
Public Knowledge
Eye on Surveillance

via electronic filing
March 3, 2020

Samuelson-Glushko Technology Law & Policy Clinic (TLPC) • Colorado Law

Blake E. Reid
Director

Andrew M. Leddy
Parker L. Nagle
Kennedy Smith
Student Attorneys

blake.reid@colorado.edu

Dr. Eric Wustrow*
Assistant Professor of Computer Engineering
University of Colorado Boulder
ewust@colorado.edu
425 UCB, Boulder, CO 80309
https://www.colorado.edu/ecee/eric-wustrow

Dr. Dirk Grunwald*
Professor of Computer Science
University of Colorado Boulder
dirk.grunwald@Colorado.edu
430 UCB, Boulder, CO 80309
https://www.colorado.edu/cs/dirk-grunwald

Dr. Sangtae Ha*
Assistant Professor of Computer Science
University of Colorado Boulder
sangtae.ha@Colorado.edu
430 UCB, Boulder, CO 80309
https://www.colorado.edu/cs/sangtae-ha

Joseph Lorenzo Hall*
SVP Strong Internet
Internet Society
hall@isoc.org
11710 Plaza America Drive, Suite 400
Reston, VA 20190
https://www.internetsociety.org/

Yomna Nasser
Mobile Security Researcher
yomna@eff.org

Marcus Prem
Mobile Security Researcher
info@dm-development.de
https://smartphone-attack-vector.de

Ashley Wilson
Mobile Security Researcher
ash.d.wilson@gmail.com
https://ash-wilson.com/

Electronic Frontier Foundation (EFF)
Cooper Quintin
Senior Staff Technologist
cooperq@eff.org
Ernesto Falcon
Senior Legislative Counsel
ernesto@eff.org
815 Eddy Street
San Francisco, CA 94109
https://www.eff.org/

Public Knowledge
Harold Feld, Senior Vice President
hfeld@publicknowledge.org
1818 N Street, NW, Suite 410
Washington, DC 20036
https://www.publicknowledge.org/

Eye on Surveillance
Marvin Arnold
info@eyeonsurveillance.org
1307 Oretha Castle Haley Blvd.
New Orleans, LA 70113
https://eyeonsurveillance.org/

**affiliation listed for identification purposes only*

Summary

There are numerous vulnerabilities in the American cellular network that malicious actors exploit in ways that threaten consumers' safety and security. While this dynamic has existed since the inception of network, the growing ubiquity of wireless technology in daily life necessitates greater attention to and action around better security.

While the Commission's Order and FNPRM in this proceeding is a step in the right direction towards tackling threats plaguing the network, the particular network equipment and service providers targeted by the Order do not pose the sole, or even most material, security threats to the network. It is critical for the Commission to embark on a much more expansive inquiry into cellular network vulnerabilities and the technical and policy strategies that might provide the most feasible and effective solutions.

The increased focus on securing the cell network—led by independent security researchers and academics—has exposed even more vulnerabilities in the most recent cellular generations. In addition to location tracking and communication interception, researchers have recently discovered ways to spoof the Wireless Emergency Alert (WEA) system to send fake Presidential Alerts to thousands of phones simultaneously. Moreover, there are a host of related vulnerabilities that threaten user privacy and the network's integrity, which have endured across cellular network generations and will likely continue into 5G.

These persistent problems are, in part, the result of unaddressed components of the network's specifications and architecture. Namely, advances in network security in 4G LTE, and now in 5G, have failed to address the inherent trust between user devices and cellular towers during the "pre-authentication" connection phase. Recent security improvements likewise have failed to address vulnerabilities that result from the network's reliance on Signaling System 7 (SS7), the backbone that enables

communication between carriers. The growing pervasiveness of the Internet of Things, amplified by 5G networks, will exacerbate the consequences of these vulnerabilities.

Even though many vulnerabilities continue to persist even after they are identified, some solutions to pre-authentication and SS7 vulnerabilities have been contemplated and developed. The most recent 5G specification includes stronger authentication and encryption using Public Key Infrastructure (PKI), which could mitigate many privacy and security issues associated with pre-authentication. However, this solution is unlikely to be effective in practice because carriers are not required to implement these specifications on their networks. Moreover, PKI will do nothing to protect current 4G LTE networks, which will likely remain vulnerable to pre-authentication attacks indefinitely.

Furthermore, the Communications Security, Reliability and Interoperability Council (CSRIC) has outlined several ways that SS7 vulnerabilities could be mitigated. Potential solutions include adding mutual authentication firewalls between networks, or even sunsetting SS7 altogether and transitioning over to the newer "Diameter" protocol, which supports all of SS7's functionality and more. Whether or not such solutions will ever be deployed is another story. Without intervention, SS7 could remain a vulnerable necessity on which networks will continue rely to communicate with one another.

The Commission is uniquely positioned to spearhead a wide-ranging, whole-of-government inquiry into the vulnerabilities plaguing the cell network and the potential solutions that may warrant implementation. Contrary to the arguments of some industry commenters, the Commission possesses broad authority across multiple titles of its authorizing statute to not only lead a thorough examination of the vulnerability landscape coordinated with other agencies, but also encourage or require implementation of feasible solutions identified during the inquiry.

Table of Contents

Discussion

The above-signed security researchers and public interest organizations with an interest in the security of the cellular network respectfully reply to comments on the Commission's 2019 National Security Order and FNPRM.[1]

We agree with other commenters that securing the cellular network supply chain should be a priority.[2] However, there are numerous other vulnerabilities that persist across the American cellular network stemming from root causes other than network's supply chain. We urge the Commission to expand its investigation to the broader universe of existing vulnerabilities threatening the network.

This reply comment outlines some of the most prevalent and troubling cell network vulnerabilities not discussed in the 2019 National Security Order, provides a brief overview of potential technical solutions to these vulnerabilities, and, finally, explains the Commission's broad legal authority to tackle these technical challenges in a meaningful way.

I. There are existing, unaddressed vulnerabilities in our cellular communications network infrastructure that threaten the integrity of the network and privacy of its users.

The number of people using mobile devices in the world is estimated to reach five billion in 2020.[3] Alongside development of new communications technologies, malicious actors have followed closely behind, posing a threat to mobile privacy and security. Since the advent of wireless cellular communication, malicious actors have taken advantage of

---

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd. 11,423 (Nov. 26, 2019) (*Cellular Security Order*), https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

[2] *CTIA Comments* at 4; *USTelecom Comments* at 3; *NCTA Comments* at 1, 3.

[3] *Mobile phone users worldwide 2015-2020*, Statista, https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide (last visited Feb. 17, 2020).

vulnerabilities in mobile functionality to gather location data, eavesdrop on phone calls, and read other users' text messages.[4]

As wireless communication becomes ubiquitous in communication and commerce, malicious exploitations of network vulnerabilities have the potential to compromise the integrity of the networks and their users. From self-driving cars[5] to military bases[6] and first responder networks relying on 5G,[7] the push towards wireless technologies necessitates immediate action to ensure the integrity of the networks these technologies rely upon.[8]

CTIA highlights the security advances that the wireless industry has already implemented in 4G LTE and additional enhancements that should bolster security in future 5G networks—namely, the introduction of cryptographic and mutual authentication in 4G LTE.[9] CTIA also references innovations in network design and edge computing that may increase the security in 5G networks.[10]

---

[4] Sharyn Alfonsi, *Hacking Your Phone*, CBS News (April 17, 2016), https://www.cbsnews.com/news/60-minutes-hacking-your-phone/.

[5] "Advanced driver assistance systems are advancing at a rapid pace and all major companies started investing in developing the autonomous vehicles. But the security and reliability are still uncertain and debatable. Imagine that a vehicle is compromised by the attackers and then what they can do. An attacker can control brake, accelerate and even steering which can lead to catastrophic consequences." Amara Dinesh Kumar, et al., *A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities* (Oct. 3, 2018), https://arxiv.org/abs/1810.04144.

[6] *DOD Names First Bases to Host Initial 5G Testing and Experimentation* (October 31, 2019), U.S. Dep't. of Def., https://www.defense.gov/Newsroom/Releases/Release/Article/2005041/dod-names-first-bases-to-host-initial-5g-testing-and-experimentation.

[7] FirstNet, *First Responder Network Authority Roadmap*, https://firstnet.gov/system/tdf/FirstNet_Roadmap.pdf?file=1&type=node&id=1055.

[8] NIS Cooperation Group, *EU coordinated risk assessment of the cybersecurity of 5G networks* (Oct. 9, 2019), https://www.politico.eu/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

[9] *CTIA Comments* at 4.

[10] *Id*.

Indeed, these advances are a step forward from 2G and 3G network security. However, these improvements fail to address many vulnerabilities that still exist in 4G LTE and new vulnerabilities in 5G that researchers have already identified.[11]

Vulnerabilities that allow malicious exploitations are largely the result of the network's architecture. Before a cell phone establishes a secure connection to a nearby tower, there is a "pre-authentication" period that leaves the device vulnerable to malicious attacks.[12] Further, there are a host of vulnerabilities that have persisted across cell network generations due to the reliance on an antiquated component of the network infrastructure: Signaling System 7 (SS7).[13]

A. The pre-authentication phase is unsecure and allows for a myriad of malicious attacks.

Pre-authentication, also known as the "handshake" or "bootstrapping" phase of cellular connectivity, is the process whereby a user device, e.g. a cell phone, and nearby cell tower acknowledge each other's existence before attempting to establish a secure connection.[14] During this phase, both the user device and the tower try and determine whether the other is authentic and therefore can be trusted.[15] This communication between the user device and cell tower is based on implicit trust and thus is neither encrypted nor authenticated.[16] The user device obeys the cell tower's commands, even if

---

[11] Roger Piqueras Jover & Vuk Marojevic, *Security and Protocol Exploit Analysis of the 5G Specifications*, IEEE Access (Mar. 7, 2019), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8641117.
[12] *Id*.
[13] Karl Bode, *SS7 Cellular Network Flaw Nobody Wants To Fix Now Being Exploited To Drain Bank Accounts* (Feb. 11, 2019), Techdirt, https://www.techdirt.com/articles/20190131/10492341502/ss7-cellular-network-flaw-nobody-wants-to-fix-now-being-exploited-to-drain-bank-accounts.shtml.
[14] David Rupprecht et al., *On Security Research Towards Future Mobile Network Generations*, IEEE Communications Surveys & Tutorials (October 2017), https://arxiv.org/pdf/1710.08932.pdf.
[15] *Id*.
[16] *Id*.

the cell tower is not an authentic, genuine cell tower.[17] As a result, the pre-authentication phase provides a window for malicious actors to deceive the network and users for various insidious purposes.

Pre-authentication vulnerabilities still exist and are open to malicious exploits. Moreover, the increased number of cell towers in 5G will increase the frequency of mobile devices engaging in the handshaking phase. In turn, this will increase the amount of opportunities that a device can be exploited. Exploits of these vulnerabilities include:

- IMSI catching, which can result in privacy threats and location leaks;
- Man-in-the-middle attacks via IMSI catchers and subsequent service downgrading, of which the latter can result in communication interception; and
- Manipulation of the Wireless Emergency System, which can result in mass panic from spoofed messages stating they are "Presidential Alerts."

IMSI Catchers. During the pre-authentication phase, a user's IMSI (a phone's unique International Mobile Subscriber Identity)[18] can be deceitfully recorded or "caught" using a fake cell tower (also known as a rogue base station). Using the IMSI numbers, a malicious actor can gather and store subsequently transmitted information such as location data and phone numbers and deny service to the devices of unsuspecting users.[19]

More specifically, when a user device attempts to connect to a cellular tower, the device begins by scanning for System Information Block (SIB) messages that nearby cell

---

[17] *Id*.

[18] *International Mobile Subscriber Identity (IMSI)*, Techopedia, https://www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi (last visited Feb. 17, 2020).

[19] Syed Rafiul Hussain et al., *LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE* (Feb. 18, 2018), https://assets.documentcloud.org/documents/4392401/4G-LTE-attacks-paper.pdf.

towers emit.[20] The user device then negotiates these messages to establish a connection with the tower that the device perceives to have the strongest signal.[21]

A rogue base station can take advantage of this exchange. During the connection negotiation, a rogue base station sends an Identity Request to a user device. In return, a user device sends the rogue base station its IMSI.[22] The cell network needs to ensure a user is a paying customer, so the user device is programmed to send its IMSI to the base station to confirm this information in response to an Identity Request.[23] The malicious actor can collect and store hundreds or thousands of IMSIs.[24]

Both law enforcement and malicious actors can then use the IMSI to gather user data such as the user's phone number and location tracking capabilities.[25] A malicious actor can also use an unsuspecting victim's IMSI in conjunction with a malicious user device to deny the victim's device cell service.[26] The analogous identifier in 5G is referred to as a Subscription Permanent Identifier (SUPI).[27] While SUPI catching is seen as more difficult

---

[20] *Id*.

[21] Syed Rafiul Hussain et al., *Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil* (May 17, 2019), https://relentless-warrior.github.io/wp-content/uploads/2019/05/wisec19-preprint.pdf. In later generations including LTE, attacks exploiting similar handshake processes via impersonation are possible, but more complex. *See* Hussain, *supra* note 19.

[22] Yomna Nasser, *Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks*, Electronic Frontier Foundation (June 28, 2019), https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks#fn3.

[23] *Id*.

[24] *Id*.

[25] *Bolstering Data Privacy and Mobile Security: An Assessment sf IMSI Catcher Threats: Hearing Before the H. Committee of Science, Space, & Technology Subcommittee on Oversight*, 115th Cong. (2018), https://science.house.gov/hearings/bolstering-data-privacy-and-mobile-security-an-assessment-of-imsi-catcher-threats (statement of Jonathan Mayer, Assistant Professor of Computer Science and Public Affairs, Princeton University).

[26] Hussain, *supra* note 19.

[27] *Id*.

than IMSI catching, a rogue 5G base station could potentially trick a UE into disclosing its SUPI.[28]

Downgrade Attacks. In addition to IMSI catching, a rogue base station can also downgrade a user's service, opening it up to the less secure 2G or 3G networks. Service downgrade attacks, again, exploit the network's lack of authentication in the initial, pre-authentication connection phase.[29] When a user device picks up the signal from a nearby rogue base station, assuming the signal is stronger than that coming from the nearest legitimate base station, the user device will attempt to connect to the fake tower instead. Once connected to the user device, the malicious actor can utilize the rogue base station to overwhelm the device with signals (i.e. jamming), resulting in a downgrade of service down to 2G.

In more sophisticated attacks, the rogue base station does not need to jam the device, but can merely set the user device's configuration settings to downgrade to 2G.[30] This downgrading is done silently, and once it has been completed, the rogue base station then intercepts and emulates communications between the user device and a legitimate base station, even though the user device and legitimate base station never actually communicate directly with each other.

Communication interception is often achieved through this kind of exploitation, often attained by a man-in-the-middle ("MitM") attack. Generally speaking, a MitM attack occurs when a malicious actor masquerades as both a cellular tower and a user device at the same time.[31] Typically, neither the real cell tower nor the user device can

---

[28] Jover, *supra* note 11.

[29] Joseph Cox, *With $20 of Gear from Amazon, Nearly Anyone Can Make This IMSI-Catcher in 30 Minutes*, Vice News (Nov. 16, 2018), https://www.vice.com/en_us/article/gy7qm9/how-i-made-imsi-catcher-cheap-amazon-github.

[30] Nasser, *supra* note 22.

[31] *Id*.

tell the difference.[32] Once an attacker has established an intermediary connection between the user device and a cell tower, it can then perform invasive communication interception such as reading text messages or listening to phone calls. All of this can be done without the user knowing it is happening.

Presidential Alerts. The Wireless Emergency Alert System (WEA) is a service mandated on commercialized cellular networks by the United States government.[33] The WEA system sends alerts via the commercial mobile alert standard (CMAS) and is used to transmit Presidential Alerts, Imminent Threat Alerts, and AMBER alerts.[34] While the service has undoubtedly been useful in many contexts, researchers have found a way to exploit its vulnerabilities.

Messages are sent from cell towers independently from the mutual authentication that occurs on LTE and 5G networks.[35] Essentially, because the emergency alerts must be sent all at once across many different devices and cell carriers, the system is designed to utilize a unique channel that bypasses some of the cell network's security architecture. As a result, all messages sent using this system are inherently vulnerable to spoofing from malicious base stations.[36] While the transmission of the alert is secure from the government to the cell tower, the broadcasted SIB message sent from the cell tower to the user device is susceptible to malicious interference and manipulation on the unique channel.

Unlike a man-in-the-middle attack, which requires the rogue base station to intercept the user device before it connects to a legitimate tower, WEA is set up so message alerts can still be sent (and thus spoofed) even if a user device has securely connected to

---

[32] *Id*.
[33] 47 C.F.R. § 10.1.
[34] *Id*.
[35] Gyuhong Lee et al., *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks*, MobiSys '19 (June 2019), https://ericw.us/trow/lte-alerts.pdf.
[36] *Id*.

another tower.[37] Consequently, a malicious actor is able to send an unauthenticated message indiscriminately to essentially every phone in range, which the user device interprets as a genuine Wireless Emergency Alert message.[38] The user device ultimately displays the alert onscreen as if it came from an authorized official, with no way for a user to determine if it's authentic or not.

Researchers have suggested that it is possible to reach 49,300 seats of 50,000 seats in an outdoor stadium using only four 1-watt rogue base stations.[39] The consequences, if carried out by a particularly malicious actor or various actors, could be devastating. Depending on the content of the message, this could cause mass panic to thousands, if not hundreds of thousands of people. In addition to the injuries that may result from a targeted spoofed alert, a general distrust of emergency alerts could follow, resulting in apathetic responses to a genuine emergency.

B. In addition to pre-authentication vulnerabilities, the failure to address Signaling System 7 vulnerabilities allows for even more malicious exploitations.

Signaling System 7 (SS7) is a crucial component of the telecommunication network's backbone. At a basic level, it is a set of protocols implemented in the 1970s that allow phone carriers to connect to each other around the world and customers to roam using other carrier networks while billing the domestic carrier.[40] SS7 was viewed as revolutionary when it was released, as it established separate channels for call signaling, allowing higher data transmissions and improved quality and reliability of phone calls. Despite being introduced decades ago for the purpose of improving landline phone calls, SS7 is still critical for the cellular ecosystem and cell communication's interoperability at an international scale.

---

[37] *Id*.
[38] *Id*.
[39] *Id*.
[40] Bode, *supra* note 13; Mayer, *supra* note 25.

However, security researchers have raised alarms about troubling vulnerabilities in SS7 for many years.[41] In fact, the Third Generation Partnership Project (3GPP) issued a report in 2000 that warned of the distressing vulnerabilities present within SS7.[42] The report argued that "the problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner," 3GPP wrote in a 2000 report.[43]

Malicious actors primarily use SS7 vulnerabilities to track cell phone location, disrupt phone service, intercept text messages, and eavesdrop on calls.[44] Recently, thieves have reportedly even used SS7 to siphon money from bank accounts.[45] To execute these hacks, actors are not directly hacking into a target's phone, but rather gaining access into the SS7 infrastructure, often by the simple act of paying a less scrupulous carrier anywhere in the world.[46]

The SS7 protocol was not developed with modern day technology in mind and has not be kept pace with today's sophisticated hackers.[47] Warning of a "Wild West" where

---

[41] John Leyden & Simon Rockman, *White Hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln*, The Register (Dec. 26, 2014), https://www.theregister.co.uk/2014/12/26/ss7_attacks/.

[42] Daniel Oberhaus, *What is SS7 and is China Using It To Spy on Trump's Cell Phone?*, Vice News (Oct. 25, 2018), https://www.vice.com/en_us/article/598xyb/what-is-ss7-and-is-china-using-it-to-spy-on-trumps-cell-phone.

[43] *Id*.

[44] Cooper Quintin, *Our Cellphones Aren't Safe*, New York Times (Dec. 26, 2018), https://www.nytimes.com/2018/12/26/opinion/cellphones-security-spying.html.

[45] Joseph Cox, *Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts*, Vice News (Jan. 31, 2019), https://www.vice.com/en_us/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank.

[46] Kim Zetter, *The Critical Hole at the Heart of Our Cell Phone Networks*, Wired (Apr. 28, 2016), https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/.

[47] European Union Agency for Network and Information Security, European Union Agency for Network and Information Security, *Signalling Security in Telecom SS7/Diameter/5G* (March 2018), https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g.

large numbers of carrier networks interconnecting on SS7's legacy infrastructure, one 2017 report alerted that carriers and governments alike have not paid enough attention to bolster SS7 security, especially as carriers rely on it to route sensitive information beyond phone calls, such as personal and geolocation data.[48] While the early days of telecommunications operated on trusted relationships between a small handful of carriers, the explosion of carriers that have access to SS7 make it quite easy for a malicious individual or nation-state actor to pay for access to SS7. Security researchers have identified numerous fixes to SS7 vulnerabilities, but there is less agreement among telecommunication carriers over whether to implement them.[49]

II. Solutions to pre-authentication and SS7 vulnerabilities exist in theory but require significant additional development to make them actionable.

Developers have already devised working solutions to pre-authentication and SS7 vulnerabilities. The most recent 5G specifications, for example, include stronger authentication and encryption using Public Key Infrastructure (PKI), which could mitigate the privacy and security issues associated with pre-authentication. PKI is ideal for inherently insecure systems such as cellular networks, which are particularly vulnerable to intercepted communications because of the nature of the radio layer itself.[50] PKI has proven highly effective in other contexts, allowing operating systems to

[48] *Id*.

[49] Zetter, *supra* note 46.

[50] Anyone with radio-transmitting capabilities can mimic the signals transmitted by cell phone users and cell towers, thus exposing devices to a suite of inherent vulnerabilities unless the devices can somehow authenticate the signals they receive. Hassan Mourad, *The Fall of SS7 – How Can the Critical Security Controls Help?*, SANS Institute (2020), https://www.sans.org/reading-room/whitepapers/critical/fall-ss7-critical-security-controls-help-36225; *see* Ron Ih, *Public Key Infrastructure Explained*, Kyrio.com (May 29, 2018), https://www.kyrio.com/blog/internet-of-things-security/public-key-infrastructure-explained.

verify that downloaded software is safe to install, and enabling web browsers to ensure that trusted websites can be accessed without exposing users to malware.[51]

However, this solution is optional in the 5G specification and its use depends entirely on carriers choosing to implement it. And even if 5G carriers do opt into using this solution and related features, it will do nothing to protect current 4G LTE networks. Regardless, it is important for the Commission to weigh the costs and benefits of allowing mobile carriers to be sole decisionmakers when it comes to implementing available security features. Finally, the FCC should also revisit potential solutions to diminish SS7 vulnerabilities.

A. Solving pre-authentication attacks using Public Key Infrastructure likely will be ineffectual in practice.

In theory, one way of preventing pre-authentication vulnerabilities has already been devised in forthcoming 5G specifications, using public key infrastructure (PKI).[52] But it may not be effective in practice because carriers will not be required to implement it. Moreover, this next-generation solution will do nothing to protect current 4G LTE networks, which will likely remain vulnerable to pre-authentication attacks indefinitely.

Public key infrastructure works by obfuscating both a mobile user's and a cellular tower's[53] identifying information through advanced asymmetric cryptography.[54] Use of this technology improves upon existing security schemes in LTE by authenticating the

---

[51] *What is PKI (Public Key Infrastructure) and why do I need it?*, Fedidcard.gov, https://www.fedidcard.gov/faq/what-pki-public-key-infrastructure-and-why-do-i-need-it (last visited Feb. 17, 2020).

[52] Karl Norrman & Prajwol Kumar Nakarmi, *Protecting 5G against IMSI catchers*, Ericsson.com (Jun. 29, 2017), https://www.ericsson.com/en/blog/2017/6/protecting-5g-against-imsi-catchers.

[53] The term "cell tower" in 5G refers to the small cell cites used to operate the high-frequency bands of the wireless spectrum. *5G Cell Towers – Are They Safe & Who Decides Where They Go?*, Vertical Consultants, https://www.celltowerleaseexperts.com/cell-tower-lease-news/5g-cell-towers-are-they-safe-who-decides-where-they-go (last visited Feb. 17, 2020).

[54] Fedidcard.gov, *supra* note 51.

"pre-authentication" messages sent between the user and tower during the handshake process. In other words, PKI reduces the amount of implicit trust between the communicating devices and forces each device to prove its identity before sending back *any* confidential information, such as a user's IMSI number. This effectively provides stronger IMSI protection during the pre-authentication stage, while also making it more difficult to track the locations of specific users.[55] Compare this process to current protocol where it is still possible to extract the identity and locations of users during the handshake process.[56]

However, PKI-enhanced features are optional in 5G specifications and may not be implemented by default in cellular network equipment.[57] Thus, such security features are not effective—or are effectively nonexistent—simply because their implementation depends entirely on how cellular operators deploy and manage their networks. For example, the latest 5G specification references these extra features with language that reads, "Confidentiality protection of user data between the [mobile device] and the [network equipment] is optional to use."[58] While the idea of more vigorous security and privacy over the radio layer is promising,[59] it will have no avail if carriers choose not to use them.

Even if 5G carriers do opt into using these next-generation features, it will do nothing to protect current 4G LTE networks in the interim. This is especially problematic

---

[55] Norrman & Nakarmi, *supra* note 52.

[56] Roger Piqueras Jover, *LTE security, protocol exploits and location tracking experimentation with low-cost software radio*, arXiv.org (Jul. 18, 2016), https://arxiv.org/pdf/1607.05171.pdf.

[57] *Security architecture and procedures for 5G system* (Release 16), 3GPP (Dec. 31, 2019), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g10.zip.

[58] *Id*.

[59] Some researchers predict that even the PKI architecture in 5G will not be effective in preventing pre-authentication attacks because certain components are missing, are deliberately left out of the specifications in order to reduce the burden on carriers, or would be more effective if employed by all carriers in order to eliminate the problem of implicit trust in pre-authentication messages. Jover, *supra* note 56.

because LTE will still be widely used for many years after 5G is deployed.[60] The 3GPP does revise older specifications when it updates its newer ones,[61] but PKI may only be feasible in 5G. Given the classification of PKI technology as a mere option in 5G, it is unlikely that the organization would contemplate specifying such features in older protocols because it would add significant latency.

From a mobile carriers' perspective, the benefits of implementing PKI-type encryption at the pre-authentication stage in current wireless networks might not outweigh the practical costs.[62] This is primarily because the extra data necessary to encrypt frequent handshake messages would likely slow down each user's ability to connect to the network.[63] The added latency would then be repeated any time a user moves from one location to another.[64] Public key encryption works well and is extremely secure but is based on complicated mathematics, and requires the exchange of much more data than simple encryption.[65] As a result, devices and towers would have to work much harder to both encrypt and decrypt data over a system that often requires users to

---

[60] Shara Tibken, *No, 5G isn't going to make your 4G LTE phone obsolete*, Cnet.com (Jul. 12, 2019, 3:45 PM), https://www.cnet.com/news/no-5g-isnt-going-to-make-your-4g-lte-phone-obsolete.

[61] *3GPP Specification Release Numbers*, Electronics Notes, https://www.electronics-notes.com/articles/connectivity/3gpp/standards-releases.php (last visited Feb. 17, 2020); *see also* Roger Piqueras Jover, *5G protocol vulnerabilities and exploits*, http://rogerpiquerasjover.net/5G_ShmooCon_FINAL.pdf (last visited Feb. 17, 2020) ("The structure of the PKI used for the certificate is out of scope of the present document.").

[62] "Ideally, all broadcast messages should be authenticated; however, such an approach can be impractical due to its substantial communication and computational overhead requirement. We thus only provide authentication guarantees for a limited number of bootstrapping messages." Hussain, *supra* note 21.

[63] Steve Lander, *Disadvantages of Public Key Encryption*, Chron.com, https://smallbusiness.chron.com/disadvantages-public-key-encryption-68149.html (last visited Feb. 17, 2020).

[64] *Id*.

[65] *Id*.

connect and reconnect several times, due to the portable nature of mobile telephony.[66] This computational overhead ultimately means that public key systems can sometimes be very slow, and might not be ideal for resolving pre-authentication issues on older radio-layer designs. The problem then becomes one of competing interests: network speed versus security.

In the Commission's pursuit of moderating threats posed by flaws in 5G infrastructure, it is important for the Commission to consider its universe of options and weigh the pros and cons of allowing mobile carriers to be the sole decisionmakers when it comes to mobile security. The Commission may have an interest in influencing carriers to implement stronger security protocols in 5G, even if the 3GPP's specifications deem the additional features optional to use. Additionally, because carriers will continue using less secure 4G LTE protocols for many years to come, the Commission might also have an interest in determining whether similar solutions are feasible or desirable on current networks.

B. Solutions to SS7 vulnerabilities exist, but more research is necessary.

In a March 2017 report titled "Legacy Systems Risk Reduction," the Communications Security, Reliability and Interoperability Council (CSRIC) outlined several ways SS7 vulnerabilities can potentially be mitigated.[67] Similar to mobile handshake vulnerabilities, a major problem with SS7 is that there is no mutual authentication between networks when they connect to one another. Thus, one solution outlined in its report involves adding mutual authentication protocols that filter data between networks, acting as a firewall to interrupt any malicious attempts to gather sensitive data or eavesdrop on phone calls and text messages.[68]

---

[66] *Id*.
[67] Working Group 10, *Legacy Systems Risk Reductions Final Report* (2017), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.
[68] *Id*.

A second proposed solution would involve sunsetting SS7 altogether and transitioning over to the newer "Diameter" protocol, which supports all of SS7's functionality and more. However, researchers have warned that although Diameter will solve many of SS7's security issues, it will create an entire suite of new vulnerabilities. CSRIC concluded that "[f]urther study needs to be considered for both Diameter and 5G security as these systems and networks are deployed."

Accordingly, the FCC should revisit these potential solutions in its assessment of 5G architecture. Otherwise, SS7 could remain a vulnerable necessity on which networks will continue rely to communicate with one another. Because the Commission possesses broad authority to encourage or require implementation of feasible solutions to SS7, it should weigh the costs and benefits of doing nothing.

III. The Commission has broad and flexible authority to lead a whole-of-government effort to address the national and individual security threats posed by the vulnerabilities plaguing the cellular network.

For years, security researchers have outlined many of the network problems and solutions described above. It is crucial for the Commission to build on this work and embark on a wide-ranging and rigorous exploration of network vulnerabilities and their workable solutions.

Several industry commenters argue that the Commission lacks legal authority to exert more expansive influence in securing the networks.[69] Likewise, many industry commenters note there are other government bodies working to improve network security.[70]

---

[69] *TIA Comments* at 5; *NCTA Comments* at 2.

[70] Several comments point to the work being done to address cell network vulnerabilities by the Department of Homeland Security (DHS), Department of Commerce, the National Institute for Standards and Technology (NIST), and Congress, among others. *CTIA Comments* at 1-3, 6-8. *TIA Comments* at 6-8; *USTelecom Comments* at 6; *NCTA Comments* at 4-5.

The Commission not only has the power to spearhead such an important and wide-ranging inquiry in coordination with other agencies, but also has the legal authority to implement its findings. The Commission has the expertise and rulemaking authority to lead the commenters' proposed "whole-of-government" approach and subsequently implement effective solutions.

The Commission possesses multiple regulatory avenues through which it can exercise the authority necessary to expand its network security focus and launch an inquiry into addressing a much broader suite of cybersecurity concerns. To secure greater security information from relevant industry actors, explore feasible solutions, and encourage or require better security awareness and practices, the Commission can leverage its authority under the Communications Act, including Title II authority to ensure telecommunications services advance the public interest, Title III authority to ensure radio spectrum allocation, over which cellular communications are transmitted, promotes national security and public safety, and Commission authority to prevent and penalize transmitting or divulging communications without the sender's consent under Section 605.

A. Mobile telephony's unique position expands rather than contracts the Commission's regulatory arsenal to act.

Some industry commenters argue that the Commission lacks the necessary legal authority to enact equipment sanctions beyond those carriers receiving funding from the Universal Service Fund.[71] For the most part, however, commenters advance these arguments without offering any statutory or interpretive support.[72] A basic review of the Communications Act and recent Commission precedent reveals a contrary proposition: the Commission holds expansive authority to ensure cell network security.

[71] *NCTA Comments* at 2; *USTelecom Comments* at 6.
[72] *See id.*

The Commission's authority over wire and radio communication and its mandate to ensure widespread access, advance national security, and promote public safety are the Communications Act's foundational pillars. In addition to Title I's broad grant of authority and its related affordance for the Commission to exercise ancillary jurisdiction,[73] Congress gave the Commission specific responsibilities and power over telecommunications providers under Title II and radio transmissions under Title III.

Mobile telephony inhabits Title III, but is subject to many Title II regulatory requirements. While mobile telephony is delivered by means of radio transmissions that are regulated under Title III, the voice telephony services it provides likewise implicate Title II. Under Section 332(c)(1)(A), the Commission regulates commercial mobile telephony providers as Title II common carriers.[74] Therefore, the Commission has a suite of diverse regulatory powers from both Title II and III to not only conduct a wide-ranging inquiry better grasping network security threats and challenges, but to also implement effective and meaningful solutions.[75]

B. The Commission has Title II authority to examine persistent security challenges and implement feasible solutions.

The Commission's authority to apply Title II provisions to the cellular network empowers the Commission to require security information from carriers necessary to

---

[73] 47 U.S.C. § 154(i); *United States v. Southwestern Cable Co.*, 392 U.S. 157, 178 (1968).
[74] 47 U.S.C. § 332(c)(1)(A).
[75] *Cellular Security Order*, 34 FCC Rcd. at 11,436, ¶ 34. On February 28, 2020, the Commission proposed cumulative fines of over $200 million against the four largest cellular carriers for improperly selling third-party access to their customers' location information without taking reasonable measures to protect against unauthorized access to that information. Notices of Apparent Liability for Forfeiture and Admonishment, EB-TCD-18-00027702 (T-Mobile), https://docs.fcc.gov/public/attachments/FCC-20-27A1.pdf; EB-TCD-18-00027704 (AT&T), https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf; EB-TCD-18-00027700 (Sprint), https://docs.fcc.gov/public/attachments/FCC-20-24A1.pdf; EB-TCD-18-00027698 (Verizon), https://docs.fcc.gov/public/attachments/FCC-20-25A1.pdf (collectively, *Location Data Fine Notices*).

better grasp the nature of persistent vulnerabilities as well as avenues through which to encourage or mandate the implementation of feasible solutions. The recent proposed fines against wireless carriers for failing to properly protect customer location data exemplify the Commission's ability to exercise its Title II authority to encourage improved carrier security practices.[76]

As the Order notes, "it is well-established that the promotion of national security is consistent with the public interest and part of the purpose for which the Commission was created."[77] The protection of life and property directly follows national security in the Commission's organic statute, which outlined that the Commission was created in part "for the purpose of national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications. . . ."[78]As the Order explains, "ensuring the safety, reliability, and security of the nation's communications networks is vital not only to fulfilling the purpose of the Act but to furthering the public interest and the provision of quality services nationwide."[79]

The Commission is expressly authorized to secure the information necessary to fulfill one of its primary duties, which is to ensure the communications network's do not threaten national security or public safety. The Commission has direct authority under Section 218 to obtain from telecommunication providers "full and complete information necessary to enable the Commission to perform the duties and carry out the objects for which it was created."[80] The Commission can use Section 218 to ensure industry stakeholders work with the Commission in better understanding the universe of threats plaguing the cellular network, a critical first step toward identifying workable solutions.

---

[76] *Id*.
[77] *Cellular Security Order*, 34 FCC Rcd. at 11,436, ¶ 34.
[78] 47 U.S.C. § 151.
[79] *Cellular Security Order*, 34 FCC Rcd. at 11,471, ¶ 124.
[80] 47 U.S.C. § 218.

The Commission is empowered to ensure that wireless carrier policies and practices are in the public's interest. Section 201(b) of the Communications Act obligates telecommunications carriers to ensure that "all charges, practices, classifications, and regulations" are just and reasonable.[81] This provision empowers the Commission to "prescribe such rules and regulations as may be necessary in the public interest."[82] The obligation under Section 201(b) to ensure that telecommunications carriers serve the public interest empowers the Commission to ensure that the nation's phone networks are secure.

The Commission has the authority to not only investigate current practices, but also implement stricter rules around protecting consumer's wireless security and privacy. Section 222(a) requires the Commission to ensure that telecommunications carriers fulfill their "duty to protect the confidentiality of proprietary information of, and relating to . . . customers."[83] In proposing fines of over $200 million against the four largest carriers for data protection misconduct, the Commission relied on privacy regulations underpinned by Section 222, which requires carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[84]

The vulnerabilities identified in Part I greatly threaten the confidentiality of customers' proprietary information. Importantly, the Commission itself articulated in 2014 that 'proprietary information' [PI] should be understood to include "personal data that customers expect their carriers to keep private."[85] Given the number of

---

[81] 47 U.S.C. § 201(b).
[82] *Id*.
[83] 47 U.S.C. § 222(a) (imposing a "duty to protect the confidentiality of proprietary information of, and relating to . . . customers.").
[84] *Location Data Fine Notices* at ¶ 8 (T-Mobile), ¶ 7 (AT&T, Sprint, Verizon) (citing 47 C.F.R. § 64.2010(a)).
[85] *TerraCom and YourTel America*, Notice of Apparent Liability, 29 FCC Rcd. 13,325, 13,331, ¶ 16 (2014).

vulnerabilities that have been directly brought to the carriers' attention, it is clear carriers are not meeting their duty to protect customers' proprietary information.

C. The Commission has Title III authority to ensure an improved response to threats.

The Commission's duties to protect national security and public safety under its mandate to serve the public interest[86] likewise extend to its authority over radio transmissions under Title III. A primary function of the Commission's Title III duties is to oversee spectrum use as well as the provision and renewal of spectrum licenses. At base, the Commission has interpreted the Communications Act as requiring the Commission "to ensure that spectrum is assigned in a manner that serves the public interest, convenience, and necessity."[87] The Supreme Court recognized in *NBC v. United States* that Title III gave the Commission "expansive powers" and a "comprehensive mandate to 'encourage the larger and more effective use of radio in the public interest.'"[88]

To fulfill this mandate, the Commission has several regulatory tools under Title III that it could consider using to address the security of the network. For one, the Commission could condition the award and renewal of spectrum licenses, upon which mobile carriers rely for operation, on meeting stricter network security standards:

- Under Section 303(b), the Commission has the authority to "prescribe the nature of the service to be rendered by each class of licensed stations and each station within any class."[89]
- Additionally, the Commission has expansive authority under Section 303(f) to "make such regulations not inconsistent with law as it may deem necessary to

---

[86] *Cellular Security Order*, 34 FCC Rcd. at 11,436, ¶ 34.
[87] *Policies Regarding Mobile Spectrum Holdings Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, 29 FCC Rcd. 6133, 6136-37, ¶ 6, https://www.fcc.gov/document/mobile-spectrum-holdings-report-and-order.
[88] *NBC v. United States*, 319 U.S. 190, 219 (1943).
[89] 47 U.S.C. § 303(b).

prevent interference between stations . . . [so long as] . . . the Commission shall determine that such changes will promote public convenience or interest or will serve public necessity, or the provisions of this chapter will be more fully complied with."[90]

- The Commission likewise possesses the authority under Section 316 to modify spectrum licenses "if in the judgment of the Commission such action will promote the public interest, convenience, and necessity."[91]
- Section 309(j)(3), which empowers the Commission to establish a competitive bidding process for mutually exclusive license applications, instructs the Commission to "include safeguards to protect the public interest in the use of the spectrum and shall seek to promote the purposes specified in [Section] 151 of this title."[92]

The Commission could take different approaches to leveraging security policy goals through the conditioning of licenses: either (1) requiring specific security protocols be implemented before receiving or renewing a license or (2) mandating that certain security standard-setting processes, such as security-by-design practices, are followed during specification development.

First, the Commission could condition spectrum licenses on an operator's ability to meet stricter network security requirements. The 3GPP's Working Procedures allow Organizational Partners to adopt optional specifications or amend the approved specifications to conform to their region's needs.[93] If the Commission conditioned their spectrum licenses on meeting security thresholds that are more stringent than 3GPP's,

[90] 47 U.S.C. § 303(f).
[91] 47 U.S.C. § 316(a)(1).
[92] 47 U.S.C. § 309(j)(3). Section 151 instructs the Commission to regulate communication by wire and radio "for the purpose promoting safety of life and property." 47 U.S.C. § 151.
[93] Third Generation P'ship Project, Working Procedures, at Article 6, Article 47 (Aug. 23, 2019) https://www.3gpp.org/ftp/Information/Working_Procedures/3GPP_WP.pdf.

the ATSI would be forced into adopting additional security standards that would allow their members to receive Commission licenses.

Second, the Commission could mandate that certain security standard-setting processes are followed by U.S. companies during specification development. This result could also be achieved through conditional licensing.

D. The Commission has authority to mandate improved cell network security under Section 605.

The Commission's authority to prevent and penalize the transmission and divulgence of communications without the sender's consent directly implicates network security. Section 605 grants the Commission authority to penalize persons who receive, assist in receiving, transmit, or assist in transmitting communications by wire or radio and divulge or publish that content without the sender's knowledge or consent.[94]

Cyberattacks are facilitated by vulnerabilities within a carrier's network and involve carriers transmitting and divulging communications without the sender's consent. Section 605's legislative history confirms that it was "designed to regulate the conduct of communication's personnel."[95] This provision imposes a duty on network operators to secure their network, and the Commission therefore has the authority under Section 605 to penalize carriers that fail to implement the security measures necessary to prevent cyberattacks and other exploits.

E. The Commission can lead a "whole-of-government" approach to the threats facing the cellular network.

The security challenges facing cell networks undoubtedly require extensive and diverse government attention. This sentiment was echoed by some industry comments championing a "whole-of-government" approach, in which the Commission is just one of

[94] 47 U.S.C. § 605(a), (e).

[95] *See* Department of Justice, Criminal Resource Manual 1001-1099, https://www.justice.gov/archives/jm/criminal-resource-manual-1066-interception-radio-communications-47-usc-605.

many governmental agencies working to improve network security.[96] We agree that the Department of Homeland Security (DHS), the Department of Commerce, the National Institute for Standards and Technology (NIST), and other agencies are all engaged in important work on network security issues.

However, the fact that other agencies are working on network security does not negate the Commission's critical role in addressing the security of the cell network, and the Commission must not abdicate its responsibilities under the Communications Act to simply play a "supporting role" to the other agencies.[97]

While it is true that other agencies such as DHS have unique technical expertise and capabilities, the Commission remains the only agency able to enact rulemaking directed at commercial carriers.[98] It is critical for the Commission created specifically to establish rules and regulations for telecommunications carriers to not only be involved, but to be a leader in this effort. A "whole-of-government" approach should not morph into an approach that disarms the one agency with actual authority to meaningfully regulate network security.

---

[96] *CTIA Comments* at 1-3, 6-8; *TIA Comments* at 6-8; *USTelecom Comments* at 6; *NCTA Comments* at 4-5.

[97] Letter to Senator Ron Wyden, Chairman Ajit Pai, Federal Communications Commission, Nov. 13, 2018, https://www.documentcloud.org/documents/5796465-Chairman-Ajit-Pai-Response-to-Senator-Ron-Wyden.html.

[98] Tom Wheeler, *Cybersecurity is not something, it is everything, Brookings Institute*, (Feb. 15, 2018), https://www.brookings.edu/blog/techtank/2018/02/15/cybersecurity-is-not-something-it-is-everything/.

* * *

The cellular network is plagued with vulnerabilities deeply rooted within the network's architecture. As a result, the networks are built on an infrastructure that is susceptible to an array of malicious attacks. It is important to acknowledge that certain bad-actor equipment and service providers focused on in this Order do not pose the sole or even most material threat to our national and individual security over the network.

While the Order is a step in the right direction, it is critical for the Commission to embark on a more holistic inquiry of cell network vulnerabilities and the technical and policy strategies that can provide the most feasible and effective solutions. The Commission not only has the power to spearhead such an important and wide-ranging inquiry, it has the legal authority to implement its findings.