Report on the Regulatory Treatment of International Cellular Roaming Traffic

NANC Call Authentication Trust Anchor Working Group

Table of Contents

Report on the Regulatory Treatment of International Cellular Roaming Traffic

1. Introduction

Fighting illegal robocalls is a top consumer protection priority for the Federal Communications Commission (FCC) and call authentication is an important part of solving this critical challenge. With the passage of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Congress expressed its support for a robust call authentication system.[1]

The FCC's Wireline Competition Bureau has called upon the North American Numbering Council's (NANC) Call Authentication Trust Anchor (CATA) Working Group (WG) to report on the regulatory treatment of international cellular roaming traffic. Specifically, they directed the NANC to address the following:

- Identify whether and to what extent international cellular roaming traffic is less likely to carry illegal robocalls than other traffic.
- Identify whether it is technically feasible for providers to segregate or otherwise clearly identify legitimate international cellular roaming traffic for compliance purposes and, if so, by what means. As part of this inquiry, analyze:
    - Whether such segregation or identification is already occurring and, if so, how widespread the practice is and under what circumstances it typically occurs; and
    - Any burdens or barriers to providers identifying or segregating such traffic, including whether those burdens or barriers vary based upon the size of the domestic provider receiving traffic or other factors.
- The extent to which other countries have anti-robocall or other regulatory regimes in place that require or rely on the segregation or identification of international cellular roaming traffic or that regulate such traffic differently, and the benefits and burdens associated with these foreign regulatory approaches.
- Provide recommendations as to whether and, if so, how the Commission should modify its call authentication and/or robocall mitigation rules to account for international cellular roaming traffic. As part of this inquiry:
    - Evaluate the likely benefits and costs associated with any recommended approaches;
    - Analyze whether it would be technically feasible for illegal robocallers to disguise traffic as cellular roaming traffic to take advantage of any "lighter touch" regulatory regime for such traffic adopted by the Commission; and

[1] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. 151, 116th Cong., § 4(b)(l) (2019) (TRACED Act).

    - Provide recommendations regarding any steps that the Commission and industry could take to prevent illegal robocallers from exploiting any such modifications to the Commission's robocalling rules.
- Provide an analysis of whether, and if so, how, the segregation or identification of international cellular roaming traffic would affect the ability of gateway providers to authenticate such traffic using STIR/SHAKEN.

1.1. Assumptions

The following set of assumptions are considered for the analysis and recommendations contained in this report:

1. In a 2G/3G network, call delivery is controlled by the Visited Network.
2. In a 4G/5G network, call delivery is controlled by the Home Network (according to 3GPP TR 23.749 "Study on S8 Home Routing Architecture for VoLTE").
3. Local Break Out (LBO) for roaming is an alternative 4G/5G routing architecture but has been deprecated. LBO is only supported for roaming on 4G/5G networks for emergency services calls. Delivery of non-emergency roaming calls in 4G/5G is controlled by the Home Network.
4. US North American Numbering Plan (NANP) does not have cellular-only number ranges.
5. Networks using national numbering plans which have dedicated cellular-only number ranges potentially create a risk of facilitating illegal robocalls if calls using those numbers are protected from proposed blocking.
6. For the Visited Network to grant access to network resources by a roaming device, the Home Network provides authentication confirmation to the Visited Network outside the US.

2. Background

2.1. International Cellular Roaming Defined

International cellular roaming allows subscribers to continue using their mobile phone or other mobile device to make and receive voice calls and text messages, browse the internet, and send and receive emails, while visiting another country. Roaming extends the coverage of the home operator's retail voice and text messaging services, allowing the mobile subscriber to continue using their home operator phone number and data services when traveling outside of the US. The seamless extension of coverage is enabled by a wholesale roaming agreement between a mobile subscriber's home operator

and the visited mobile operator network. The roaming agreement addresses the technical and commercial components required to enable the services.[2]

2.2. How Cellular Roaming Works

The concept of "home" and "visited" networks is used in roaming. The Home Network refers to the network the subscriber is registered with and is their day-to-day cellular provider. The Visited Network is the network a subscriber roams onto temporarily and is outside the serving area of the Home Network.

When the subscriber travels to a network other than their Home Network, the device attempts to communicate with the Visited Network. The handset may be preconfigured to select a specific Visited Network, or the subscriber may be able to choose which Visited Network is preferred.

The Visited Network picks up the signal from the mobile device, notes that it is a visitor and attempts to identify the Home Network based on the IMSI. The IMSI contains the MCC (Mobile Country Code), MNC (Mobile Network Code) and MSIN (Mobile Subscriber Identification Number). If there is a roaming agreement between the Visited Network and the Home Network, the Visited Network authenticates the mobile device based on network attachment information received from the Home Network. If there is not a roaming agreement, then the Visited Network is unable to authenticate the device with the Home Network. The Visited Network may use alternate methods to provide service, e.g., provide a mechanism to contact customer care, or deny access. But in the case where a roaming agreement does exist, once authenticated, the device is able to originate and receive services. Services can include voice, text messaging, broadband data, and other services.

How services are delivered to international roamers differs depending on whether the attachment to the Visited Network is over a 4G/5G or 2G/3G access network. When access is 4G/5G, services are delivered using the S8 Home Routing model (GSMA IR.65 specification), where the Visited Network establishes IP connectivity between the roaming mobile device and its Home Network. The mobile device then obtains services directly from the Home Network, just as it does when the device is not roaming. When access is 2G/3G, services are delivered and calls are routed by the Visited Network without involvement of the Home Network.

[2] GSMA International Roaming Explained. https://www.gsma.com/latinamerica/wp-content/uploads/2012/08/GSMA-Mobile-roaming-web-English.pdf

Figure 1 shows the case where a roaming mobile device attached to the Visited Network over 4G/5G originates a call to a US NANP number. Per the S8 Home Routing model, call setup signaling is exchanged directly between the device and its Home Network. After applying any originating services, the Home Network routes the call, possibly via one or more Transit Networks, to the Terminating Network serving the called US NANP number. Since the mobile device has been authenticated and the call is home-routed, the Home Network knows that this is a call originated by one of its mobile subscribers who is roaming.

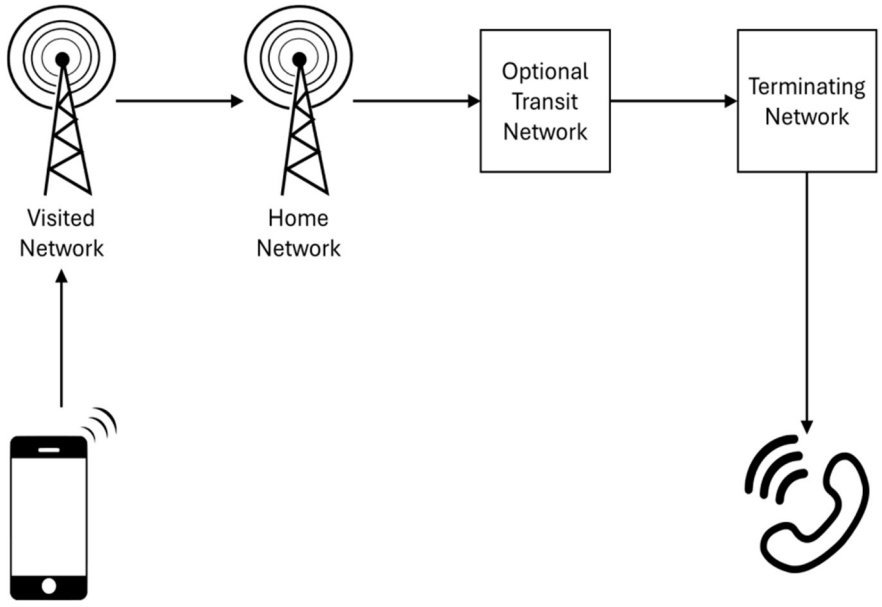

Figure 1: 4G/5G International Cellular Roaming Call Flow

Figure 2 shows the case where a mobile device attached to the Visited Network over 2G/3G roaming using LBO originates a call to a US NANP number. Call setup signaling is exchanged directly between the device and the Visited Network. The call is not home-routed; rather, the Visited Network routes the call like any other call originated by an international entity to a US NANP number. Specifically, the call is routed (typically via Signaling System 7 (SS7) and/or Session Initiation Protocol (SIP) trunks) to an International Gateway Network. The International Gateway Network then routes the call to the Terminating Network serving the called US NANP number, possibly via one or more Transit Networks. Calls arriving at the International Gateway Network can include a mix of legitimate calls from US mobile subscribers roaming internationally, and non-roaming calls from international entities spoofing US NANP numbers. The International Gateway Network currently has no ability to distinguish between these two call types.

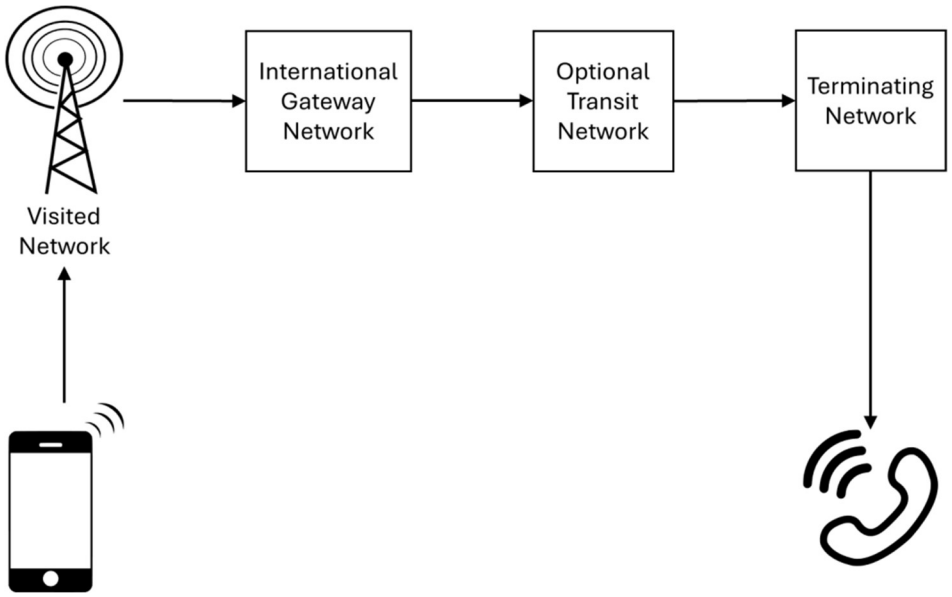

Figure 2: 2G/3G International Cellular Roaming Call Flow

3. Report

This section evaluates the likelihood of using roaming to generate illegal robocalls, identifies different options, and recommends steps the FCC and industry could take to prevent abuses.

3.1. Feasibility of Identifying Legitimate Cellular Roaming Traffic and Whether That Traffic is Less Likely to Carry Illegal Robocalls

3.1.1 Feasibility to Disguise Cellular Roaming Traffic as Illegal Robocalls

One of the questions directed to the CATA WG is "whether it would be technically feasible for illegal robocallers to disguise traffic as cellular roaming traffic to take advantage of any "lighter touch" regulatory regime for such traffic adopted by the Commission." When roaming is implemented using LBO, fraudulent assignment of the CLI ("caller ID spoofing") is possible. But when roaming is implemented using S8 Home Routing (S8HR), it is not. Since S8HR is the preferred implementation for 4G/5G networks, the use of LBO is expected to decline as networks are upgraded to 4G/5G worldwide.

LBO

Only the device's Home Network knows whether an internationally-originated call using a calling number assigned from the US NANP is originated by a device roaming using LBO. Fraudulent usage is detectable when the illegal robocaller calls another number served by the Home Network of the spoofed number.

Determining whether an internationally-originated call using a US NANP number in the Calling Line Identifier (CLI) is from a legitimate international cellular roamer requires determining if the number in the CLI of the internationally-originated call is associated with an active international cellular roamer. Determining whether the roamer is actively making a call attempt would provide greater certainty.

Determining if the number in the CLI of the internationally-originated call is associated with an active international cellular roamer is simple for the network to which the number signaled as CLI in the call request is subscribed. This information is available in that Home Network's Home Location Register and can be used to help the Home Network identify potential spoofing. For other networks to answer that question would require some means to share that information.

Determining whether the roamer is actively making a call attempt is not a trivial undertaking. The Home Network, which would commonly be responsible for determining whether a CLI is that of an active international cellular roamer, may not have the means to determine if the international roaming subscriber is also simultaneously making a call attempt.

S8HR

When roaming is implemented using S8HR, call control signaling is transparently forwarded from the packet core of the Visited Network to the packet core of the calling device's Home Network; and thereafter to the Home Network's IP Multimedia Subsystem (IMS). It is subject to the same

authentication and security mechanisms as calls originated by the Home Network's non-roaming devices. There is no increased risk of or exposure to fraudulent use of CLI due to roaming implemented using S8HR. The Home Network (not the device) populates the CLI in calls originated by both non-roaming subscribers and by subscribers roaming via S8HR; hence the opportunity for spoofing of CLI is greatly reduced. Assuming the Home Network implements STIR /SHAKEN, it will indicate the validity of the CLI to downstream networks by appending an appropriately populated SHAKEN PASSporT to the outgoing call control signaling.

3.1.2 Likelihood of International Cellular Roaming Traffic Carrying Illegal Robocalls

Another question directed to the CATA WG is to "identify whether and to what extent international cellular roaming traffic is less likely to carry illegal robocalls than other traffic."

In the experience of USTelecom's Industry Traceback Group (ITG), the official traceback consortium designated by the FCC under the TRACED Act, tracebacks of illegal robocalls have not identified international cellular roaming traffic as a notable source of illegal robocalls. Of the eighty-one non-US providers identified in ITG tracebacks in 2023 as originating suspected unlawful robocalls, only eight appear to provide mobile service. These providers, however, generally also provide other services including Voice over IP (VoIP), wholesale, and international long distance, and the ITG has no reason to believe that these calls were from roaming subscribers. These providers were responsible for less than ten percent of the tracebacks of suspected unlawful robocalls that identified a foreign service provider.

3.2. Practices of Other Countries Related to Segregating Traffic

Various countries are actively working to treat international cellular roaming traffic as a protected class of traffic.

Regulators in Finland, France, Germany, Lithuania, and Turkey have all implemented rules to block calls or suppress display of CLI for calls that originate internationally using numbers in the CLI from the country's numbering plan[3]. The blocking rules make an exception for calls that originate with international roamers who are either callers from abroad roaming in-country or callers from the country roaming abroad. Note that France created their rule in 2021 but repealed the rule in July 2023.

Regulators in Ireland, Portugal, Malta, and Austria are engaged in consultative processes to develop similar blocking rules and exceptions for international roaming traffic.

Regulators in Finland and Ireland proposed using "proxy servers" capable of determining whether the number in the CLI is from an international cellular roamer to identify and protect (i.e., not block) calls from legitimate international roamers.

[3] Ofcom, "International approaches to tackling scam calls", a summary report of responses to Ofcom's March 2023 questionnaire on international approaches to tackle scams.

Finally, regulators in Norway and Lithuania assert service providers in their countries are technically capable of identifying calls from international cellular roamers using existing roaming databases.

3.3. Recommendations

The desired outcome is to protect calls which are likely legitimate and to block or label those calls which are likely illegal. Currently, calls that originate outside of the US using NANP numbers either route to the US service provider's network and are treated like all other calls originating on the service provider's network or they are handed to a US International Gateway Network and the gateway provider meets its FCC obligations including certification of its Robocall Mitigation Plan in the Robocall Mitigation Database which further includes "Know Your Customer" (KYC) measures.

The CATA WG recommends that the FCC continue to apply existing rules to roaming traffic. The costs of developing processes to segregate roaming from non-roaming traffic are believed to outweigh any benefit. Additionally, any benefit would be temporary since providers are moving to Voice over Long Term Evolution (VoLTE) which authenticates and routes calls over the Home Network of the originating subscriber.

3.3.1. Steps the Industry Could Take to Prevent Abuses

1. Mobile network operators should continue the transition of international cellular roaming to VoLTE networks. To the extent roaming occurs on 2G or 3G networks, service providers are required to implement FCC requirements at the US International Gateway Network.
2. Industry should continue to review and monitor traffic for illegal robocall trends and propose actions, best practices, or FCC rules if new developments materialize.
3. Mobile network operators should leverage information about the roaming status of their subscribers to protect legitimate calls.

3.3.2. Steps the FCC Could Take to Prevent Abuses

1. Encourage partner regulators to transition to VoLTE networks for roaming.
2. Review process for removing international providers from the Robocall Mitigation Database on a timely basis. The FCC could possibly ask for comment on other ways to identify international bad actors to remove them from this database.
3. Continue to enforce existing rules.

The CATA WG believes it is rare for mobile subscribers to originate illegal robocalls because originating traffic from a mobile network is typically more expensive than other technologies, and international cellular roaming is even more expensive and therefore may be cost prohibitive. However, if changes to technology, regulation, or other input factors alter the cost/benefit analysis for scammers, this assertion could change. The segregation or identification of international cellular roaming traffic would not affect the ability of US International Gateway Network providers to authenticate such traffic under current FCC STIR/SHAKEN requirements.

4. Glossary

For the purposes of this document, the following definitions apply:

Cellular traffic – voice calls that originate on a mobile network.

Cellular roaming traffic – voice calls that originate on a cellular network other than the subscriber's Home Network.

FCC – Federal Communications Commission. The FCC may also be referred to in this document as "the Commission."

IMS – IP Multimedia Subsystem. A standardized architectural framework for delivering IP multimedia services.

International cellular roaming traffic – voice calls that originate on a cellular network in a different country than the country of the subscriber's Home Network.

International Gateway Network provider - intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its facilities before transmitting the call downstream to another provider.

LBO – Local Break Out. A roaming architecture in which originating services and onward routing to the terminating network are provided to the roaming device by the visited network.

S8HR – S8 Home Routed. A roaming architecture in which originating services and onward routing to the terminating network are provided to the roaming device by its home network.

SIP – Session Initiation Protocol. The foundational signaling protocol for creating, modifying, and terminating voice calls on internet protocol (IP) networks. [RFC3261]

Subscriber – the user consuming cellular service and may include the device used for placing the call.

Traffic – voice calls.

US International Gateway Network provider - US-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its US-based facilities before transmitting the call downstream to another US-based provider or terminating on its own network.

5. Annex

5.1. Roaming IMS subscriber attached over 4G/5G Packet Switched access network

Mobile roaming of subscribers over 4G/5G access uses VoLTE call signaling based on the GSMA IR.65 "IMS Roaming, Interconnection and Interworking Guidelines" technical specification. The GSMA IR.65 specification outlines two main mechanisms:

- Local Break Out (LBO)
- S8 Home Routed (S8HR)

LBO was deployed by carriers to support civilian emergency calls (e.g., 911 in the US, or when a US subscriber dials 112 while roaming in Europe).

The S8HR architecture is shown in Figure 3. The terms used in the diagram have the following meanings:

- RAN – Radio Access Network
- E-UTRAN – Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Network (also referred to as LTE RAN)
- EPC – Evolved Packet Core
- The visited EPC contains:
    - MME – Mobility Management Function
    - SGW – Serving Gateway
- IPX – IP eXchange
- The home EPC contains:
    - HSS – Home Subscriber Server
    - PGW – Packet Gateway
- PDN – Packet Data Network
- All other entities in Home Network are part of the IMS PDN

The core network function in this architecture is the EPC which creates IP connectivity between the mobile User Equipment (UE) and a PDN (in this case the home IMS PDN). The box on the left shows the mobile UE connected to the visited EPC via the E-UTRAN. The box on the right shows the home EPC and IMS PDN. The IPX acts as an interconnect/routing hub between the Visited and Home Networks.

The roles played by the EPC network functions in Figure 3 are as follows:

- MME – Interworks with the home HSS via the S6a interface to obtain authentication and authorization information about a newly attached roaming subscriber. It authenticates the mobile UE, and interworks with the SGW via the S11 interface to establish a bearer channel for SIP signaling between the mobile UE and the home IMS. Note that the MME interface to establish the leg of the bearer channel between the SGW and UE is not shown in this diagram.
- SGW – based on control messages received from the MME via the S11 interface, and establishes the bearer channel with the home PGW via the S8 interface.
- HSS – contains the authentication and authorization/subscription information for each subscriber served by the home IMS.
- PGW – terminates the bearer channel from the Visited Network in the Home Network.

Once the bearer channel is established, the UE can exchange SIP signaling messages with the home IMS.

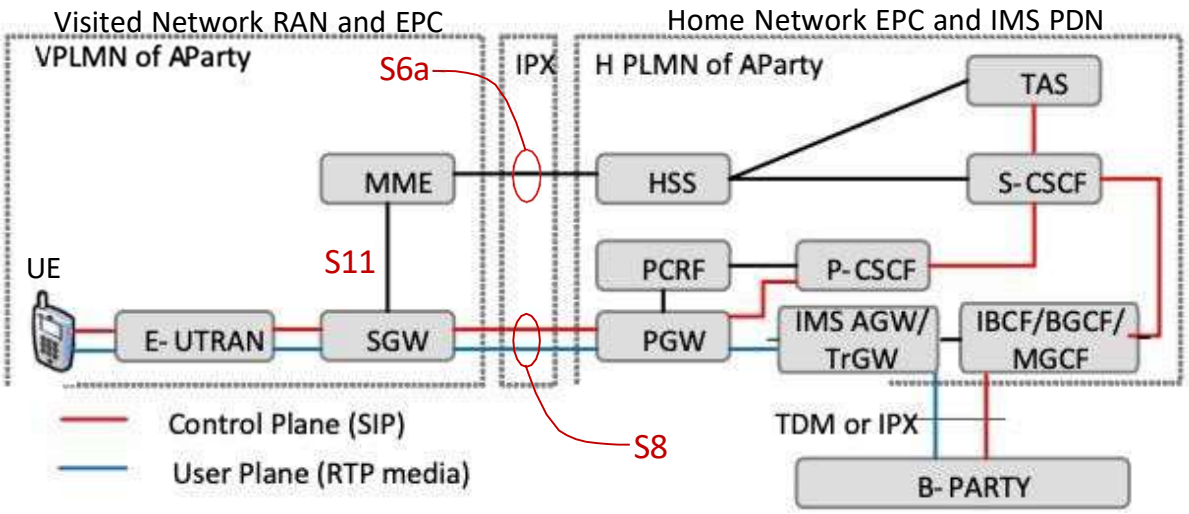

Figure 3. – S8HR IMS Roaming Architecture (VoIMS service shown)

Figure 3 provides an overview of the procedures that enable a subscriber roaming over 4G access to obtain call originating services, including STIR/SHAKEN authentication, from the subscriber's home IMS network.

5G uses a different set of Network Function (NF) components and does not use a 4G Mobility Management Entity (MME) and Serving Gateway (SGW) to establish the mobile IP VPN via the S8 interface back to the Home Network PGW but the operational result is the same, i.e., a mobile IP VPN is established between the Visited and Home Network and the mobile device uses SIP over IP to register and originate/terminate calls from/to the Home Network so all calls originate/terminate domestically.

5.2. Roaming IMS subscriber attached over 2G/3G Circuit Switched Access

The support of mobile roaming of IMS subscribers over 2G/3G access tends to be more complex than the S8HR roaming model described in Section 5.1 since it requires interworking between the Circuit Switched and Packet Switched domains. Also, providers have multiple roaming options to choose from. For all options, the UE attaches to the visited Mobile Switching Center (MSC) using 2G/3G attachment procedures. The visited MSC then queries the HSS in the home EPC to obtain authentication and authorization information for the roaming UE and authenticates the UE's Universal Subscriber Identity Module (USIM). International gateway providers are typically used to route these calls.

5.3. SS7 and Diameter Security Risks

Signaling System 7 (SS7) Mobile Application Part (MAP) and Diameter protocols are the principal standards that support global roaming authentication between carriers. This authentication occurs

before a call is placed. Once the device is outside its Home Network and authenticated, call delivery is further authenticated and then routed as any other call, although routing is separate from the authentication that occurs prior to the call being placed.

The FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group on Legacy Systems Risk Reduction, composed of wireless industry stakeholders, technology experts, and federal government participants, studied the risks associated with SS7[5]. They developed nine recommendations to reduce the security risks of SS7 and Diameter[6], an interconnect protocol that replaces SS7, and used largely in 4G LTE networks, as well as in the transition to 5G.

[5] See CSRIC V: Working Group 10, Legacy Risk Reductions (2017), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf ("CSRIC Report").

[6] See CSRIC VI, Final Report – Recommendations to Mitigate Security Risks for Diameter Networks, Version 1.1, at 8 (March 14, 2018), https://www.fcc.gov/file/13925/download ("CSRIC VI Diameter Report").