NENA Telephony Denial of Service (TDoS) Information Document

Abstract: This document describes Telephony Denial of Service (TDoS) in 9-1-1 networks, including methods for detection and mitigation.

NENA Telephony Denial of Service (TDoS) Information Document

NENA-INF-045.1-2025
DSC Approval: 12/14/2021
PRC Approval: 01/28/2021
NENA Board of Directors Approval: 03/04/2022
Reaffirmed: 07/01/2025
Next Scheduled Review Date: 07/01/2030

Prepared by:
National Emergency Number Association (NENA), Systems Security & Resiliency Committee, Telephony Denial of Service (TDoS) Working Group

1 Executive Overview

9-1-1 is vulnerable to security issues, including call flood-based attacks such Telephony Denial of Service (TDoS), which saturate the network and prevent individuals from receiving timely service. 9-1-1 is vulnerable to TDoS, as a function being well known, having limited resources (especially call takers), older technology (in E9-1-1), and the need to answer every call.

There have been TDoS attacks against 9-1-1 in the past. A notable event was the mobile botnet in late 2016, where an attacker compromised over 1000 mobile phones and caused them to all dial 9-1-1 until restarted. There have been recent attacks to 9-1-1 directly and through connected administrative access in law enforcement and municipal offices. Attackers are using Voice Over IP (VoIP), compromised PBXs, and other techniques to generate the calls. Some attacks also include conferencing of multiple call takers, in an attempt to create confusion and waste call taker time.

The E9-1-1 network is slowly migrating from legacy technology and localized equipment to Next Generation 9-1-1 (NG9-1-1), where shared infrastructure is used for local, regional, or even national 9-1-1 access. NG9-1-1 consolidates the access from service providers and other features into an Emergency Services IP Network (ESInet). There are few TDoS mitigation options for E9-1-1. NG9-1-1 has the ability to mitigate most TDoS attacks by routing traffic between PSAPs, using features such as the "Bad Actor" mechanism and deploying external bulk DDoS mitigation services.

TDoS can be categorized by attack volume:

- Low volume is defined as the number of attack calls is fewer than the number of call takers. This can be considered a nuisance, but it ties up call taker resources.
- Medium attack volume is defined here as calls greater than available call takers but less than the capacity of the local network and systems to handle it. This requires some kind of mitigation to avoid overwhelming the PSAP.
- Large volume is call volume greater than the size the local network and systems can handle.

E9-1-1 has no effective mechanism to mitigate TDoS. NG9-1-1 standards define several mitigation mechanisms including methods that reroute traffic to other PSAPs and call takers, the ability to mark a traffic source as part of an attack ("Bad Actor"), and external mitigation services capable of mitigating terabits of attack traffic.

Detection & mitigation of TDoS is complicated by spoofing of phone numbers, especially when the numbers used in the attack changes rapidly. The industry is working on the

STIR/SHAKEN[1] standard, designed to authenticate the calling number and thereby reduce the impact of spoofing, TDoS, and robocalls. STIR/SHAKEN has implementation mandates in June of 2021 and is expected to be implemented over time. However, until all networks become compliant with STIR/SHAKEN, not all calls will be authenticated. So, while it is helpful, it's not a silver bullet. There are also proprietary solutions for TDoS, but they are not widely implemented.

Mitigation of TDoS is a challenge. Even when it is completely clear that a call is malicious and part of a TDoS attack, some ESInet providers and PSAP managers are unwilling to drop a call. This is even more unlikely, when it is not completely clear that a call is part of a TDoS attack. This may mean that other call treatment options, such as routing to PSAPs with available resources is used or sending calls to specially trained call takers. There are TDoS mitigation mechanisms specified in NG9-1-1 standards, but they are not widely deployed. This means many NG9-1-1 systems are still vulnerable to TDoS attacks.

[1] STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards.

Table of Contents

NENA
INFORMATION DOCUMENT
NOTICE

This Information Document (INF) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

NENA reserves the right to revise this Information Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at nena.org.

Intellectual Property Rights (IPR) Policy

NOTE – The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement any standards referenced by this document or to implement or follow any recommended best practices, procedures or architectures contained herein.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA-INF-045.1-2022	03/04/2022	Initial Document
NENA-INF-045.1-2025	07/01/2025	Reaffirmation

2 Understanding TDoS

2.1 TDoS versus DDoS Explained

While a Distributed Denial of Service (DDoS) attack is out of scope for this revision, this section explains the difference between DDoS and a Telephony Denial of Service (TDoS) attack for clarification purposes.

DDoS is an attempt to bring down a network connected system by overwhelming it with so much traffic that legitimate users are unable to connect to the service. TDoS is a flood of malicious inbound calls that target public-safety response systems such as 911

In a legacy E9-1-1 system, a TDoS attack would be leveraged against the E9-1-1 trunks coming in to the PSAP, in contrast to a DDoS attack, which would typically be leveraged against an IP connection to the PSAP.

In NG9-1-1, the incoming IP connection could be a Session Initiation Protocol (SIP) call interface or an HTTP data interface. In this document we define an NG9-1-1 TDoS as an attack against the SIP interface, since it is the SIP interface that supports emergency call signaling.

Strictly speaking, some occurrences of overload do not necessarily relate directly to a TDoS attack, since there is the possibility of legitimately initiated 9-1-1 calls overloading system resources and having the same result (blocked calls) as a true TDoS attack. This similarity of symptoms is referred to as "valid" calls in the next section.

Note: In both E9-1-1 and NG9-1-1 configurations, administrative calls (e.g., admin line calls in E9-1-1) still exist.

2.2 TDoS Taxonomy

There are several different TDoS attack signatures that can affect 9-1-1. However, the signature and detection can be divided into groups based upon whether the calls are "real" or "synthetically" generated. The key difference between these types of calls is that it is not likely that the calling number will be forged or "spoofed" for real calls. Conversely, the calling number for synthetic calls is always spoofed, since the calls are not real. These two cases are covered below.

2.2.1 Real Calls

Real calls are those originating from actual devices, including mobile phones, legitimate Voice over IP (VoIP) phones, consumer landlines, and business phones serviced by an organizations Private Branch Exchange (PBX). There are various methods where these devices can be used to generate a TDoS attack, including mobile botnets, Non-Service Initiated (NSI) phones, compromised PBXs, and others. However, in most cases, the ANI in

E9-1-1 or the P-Asserted-Identity (P-A-I) in NG9-1-1 will NOT be spoofed but will be the actual number associated with the phone. This has a significant impact on the attack signature and detection of the attack. For example, it is relatively straight-forward to determine that a device is participating in a TDoS attack, based on how frequently calls are received with the same calling number. The interval between calls may also be a constant and can also be used as an indicator of a possible TDoS attack. So, after a certain number of calls is received from the same calling number, especially if they can be grouped in some way (all coming from one area, PBX, mobile device type, service provider, etc.), it should be safe to start treating future calls from that calling number as an attack.

2.2.2 Synthetic Calls

Synthetic calls typically originate through VoIP. A common method of perpetrating this type of attack is to use an open-source PBX such as a variant of Asterisk and a SIP service to generate and deliver the TDoS calls to the target. This takes some expertise to perform and route the calls to the desired 9-1-1 Public Safety Answering Point (PSAP). It is also possible (although to our knowledge this has not yet occurred in the wild) to compromise some Internet of Things (IOT) devices that have SIP call generation capability, or mobile devices, causing them to generate a TDoS attack. It may or may not be possible to change the calling number used from such devices. The key for these types of attacks is that the calling number will be spoofed. If the attacker is at all sophisticated, then they can change the calling number every time and/or make it appear that the number is coming from the correct area serviced by the PSAP.

2.2.3 Detection of Spoofing

Detection of spoofing may be difficult.

Spoofing of the calling number makes detection of a TDoS attack more difficult to detect and mitigate. Spoofing of the calling number is most easily performed with calls originated with VoIP but is also possible with a compromised PBX. Aside from STIR/SHAKEN in the future, there is virtually nothing in SIP that can be used to reliably detect spoofing. While there are no standard capabilities in NG9-1-1 for detecting calling number spoofing, some techniques exist including detection of malformed numbers, numbers outside of the PSAP area, and unallocated numbers. Some service providers also offer APIs which can be used in real-time to help determine if the calling number for a call is authentic.

Filtering mechanisms based on STIR/SHAKEN are likely to assist in detection of these attacks, and "Bad Actor"[2] can be used to help mitigate spoofing attacks.

[2] For "Bad Actor" description see NENA-STA-010.3 [8], in the "Border Control Function, Interface Description"

2.3 Categorizing TDoS

We can differentiate TDoS into 3 categories:

1. Low-volume attacks, which are described as when the number of attack calls is approximately less than the number of calltakers
2. Medium-volume attacks, which are described as when the number of attack *and* valid calls is approximately greater than the number of calltakers, but the signal volume of all calls does not exceed the size of the access network pipes.
3. High-volume attacks, which are described as when the signal volume of attack and valid calls exceed the size of the access network pipes.

3 Spoofing Identity In Emergency Calls

One essential component to address the threat of TDoS is Source Identity Authentication. This is a mechanism to cryptographically sign key elements in the "SIP" signaling messages that setup the 9-1-1 call. The digital signature on each call allows the recipient to identify a service provider near the caller, the origin telephone number, and the time the call was placed. Recipients can be confident that information that has been signed has not be tampered with in transit. The secured timestamp ensures that the signaling messages are fresh; recipients can easily detect any attempt to store and replay messages later. The technology to sign the signaling message and interpret the results is the "STIR" work in the IETF, and in the US, the mechanism to distribute the keys used for signing is the "shaken" work in ATIS [2]. STIR defines the "Identity" header in a SIP transaction to contain the signed data. If a 9-1-1 call is received and has a validated signed Identity header, the likelihood of the caller's telephone number being spoofed is small, but the SHAKEN mechanism relies on trust that the Originating Service Provider is careful to sign only calls for which it knows the sender and the sender is using a telephone number it is authorized to place calls from that number. Over time, the reputation of each OSP can be used as an additional input to decide which calls might be spoofed even when a validated Identity header is received. Dramatically limiting spoofing of telephone numbers reduces the ability of an attacker to remain anonymous. Attackers could still infiltrate/take over legitimate call sources and place attack calls from those sources, which would have validated Identity headers.

By eliminating, or at least dramatically reducing the probability of spoofing, the caller telephone number becomes a reliable indicator that calls came from the same caller. Therefore, if one bad call is received, that telephone number can be marked as compromised and further calls from that number can be suppressed until the attack subsides. The ability to reliably filter on telephone number dramatically increases the reliability of separating bad calls from good calls.

Despite its utility to reduce unwanted calls, STIR/SHAKEN is not a panacea. At the time this document was released, only calls with a SIP signaling path end-to-end can be digitally signed. This means that calls through a legacy E9-1-1 network and 9-1-1 calls that traverse a Legacy Network Gateway (LNG) or Legacy Selective Router Gateway (LSRG) as part of an NG9-1-1 system cannot be signed. Though the digital signature is typically affixed by the origination carrier, a sophisticated attacker may be able to circumvent the security mechanisms within a carrier network that were designed to prevent spoofing. In addition, a carrier could itself be compromised. Some carriers may not apply as much care to controlling signatures as others might. The STIR/SHAKEN mechanism is not yet widely deployed. Current regulations may not require signatures on 9-1-1 calls. However, receipt of a call with a valid signature is much more likely to contain the actual phone number assigned to the caller than a call without a valid signature.

It is not expected for STIR/SHAKEN to be able to provide any authentication capability in E9-1-1 systems. NG9-1-1 systems should be able to make use of signed identity if they adhere to STA-010.3 standards [8]. Although current standards require the path from originating network to the terminating network to be 100% IP, further work in the standards is expected to allow such a capability to be extended to legacy systems (funding and regulatory actions permitting).

STIR/SHAKEN is considered a very important component of an effective TDoS mitigation effort. Therefore, NGCS operators should place a high priority on getting valid signed Identity headers on calls from all OSPs.

Although Time Division Multiplex (TDM) networks are not capable of signing the signaling of 9-1-1 calls, it is also the case that it is very difficult to spoof calls from older systems. Since TDM systems are connected directly to the Selective Router (SR) or an LNG, without any untrusted[3] intermediaries, spoofing from these systems is unlikely. VoIP and wireless networks also don’t use any untrusted intermediaries, and in particular, there is never an untrusted TDM network between the original network and the SR/LNG. Therefore, when STIR/SHAKEN is implemented on the origination network, it will be very effective at preventing spoofing for 9-1-1 calls.

4 Mitigation of TDoS Attacks in E9-1-1

There is very limited capability to mitigate any kind of TDoS attack in an E9-1-1 system. The fact that not only is there no capability to perform any kind of filtering on the front end of a Selective Router, but also that the size of the trunk groups coming out of the back end

[3] In this context “untrusted” refers to a network that could change signaling fraudulently.

of the Selective Router are so small relative to the number of call takers (to get P.01 GoS)[4], results in the capacity to handle bad calls being constrained. Even if one could separate good calls from bad calls, the rate of calls that can be handled is severely limited by the signaling protocols (CAMA outpulse). Given the anticipated migration to NG9-1-1, there is industry reluctance to invest in short term fixes to existing legacy E9-1-1 systems to address this challenge.

If there are more incoming calls (both bad and good) than call takers, and if calls are originating from more than one service provider, the Selective Router will effectively act to block good calls from all sources. There is nothing that can be done to mitigate this situation because there isn't a way for the Selective Router to filter out any specific calls. The PSAP could filter on Telephone Number, if calls weren't being spoofed noting that STIR/SHAKEN is not effective with a TDM system e.g., using a Selective Router, but it can't send more calls to the PSAP in than there are call takers available. Therefore, the effectiveness is limited and eliminating this problem would take implementing external systems between the SR and the PSAP or changes to the CPE. This means there is no effective mitigation for any large or even medium scale attack for legacy systems.

If the attack is from one service provider, where the size of the attack is smaller than the size of the trunk group to the SR and telephone numbers are fixed for the attack, then filtering based on TN via some kind of middle box between the SR and a PSAP or within CPE might help reduce call volumes. However, because the CAMA out-pulsing must be completed, calls cannot be filtered before the TN arrives at that middle box. Doing this type of filtering may reduce the introduction of calls from the offending TN(s).

If the SR has IP options (like RFAI) and it can effectively send more calls out than a TDM SR, it's still limited by the input trunk group sizes. Filtering on TN, if that were supported, could stop some more calls than in a pure TDM environment.

5 Analysis and Mitigation of Low/Medium-Volume TDoS Attacks in NG9-1-1

Note: Volume related terms are in relation to the PSAP's call taking capabilities. Larger PSAPs may have higher tolerance than smaller PSAPs.

[4] The probability (P) expressed as a decimal fraction of a telephone call being blocked. P.01 is the grade of service reflecting the probability that one call out of one hundred during the average busy hour will be blocked. P.01 is the minimum recommended Grade of Service for 9-1-1 trunk groups.

NG9-1-1 systems, when built to NENA standards (v2 of STA-010 [9] and subsequent versions), have two mechanisms that are available to help mitigate small and medium scale TDoS attacks:

1. The Session Border Controller (SBC) component of the Border Control Function (BCF) should contain logic that is capable of recognizing commonly encountered TDoS attacks and blocking calls that meet known patterns.
2. The "Bad Actor" mechanism[5] allows a PSAP to mark the identity (typically, the telephone number) of an attacker and temporarily block subsequent calls from that identity.

SBCs are the primary defense mechanism to guard against attack toward enterprise and carrier SIP systems, and thus are generally considered to be the first line of defense for attacks that are smaller in number than the pipe size reaching the SBCs. For attacks that are distinguished by an attempt to exploit SIP signaling weaknesses that have been seen multiple times in past attacks, they are typically very effective. These types of mechanisms are less effective when new attack vectors are used, because they do not have any kind of adaptive component that can be modified on the fly to respond to a new type of attack.

SBCs have limits on how many attack calls they can concurrently mitigate, and it can be less than the size of the pipe the SBC is connected to. As noted in the large-scale mitigation section below, 3rd party mitigation services could be engaged for those attacks greater than the SBC can mitigate, or if the SBC is not capable of recognizing the particular attack that is underway.

For attacks where the same identity is used repeatedly in an attack, the "Bad Actor" mechanism can be very effective. Once a PSAP identifies a bad actor identity, the i3 standards provide a way for the PSAP to send a message to the BCF that handles the identity in question, telling the BCF to block subsequent calls from that identity. That means when you get one bad call from each unique identity, it gets marked as a Bad Actor in the BCF, and no subsequent calls from that identity are allowed until the attack subsides.

Disabling Bad Actor filtering for a specific source is based on time and is implementation dependent. Frequency of calls from the source, types of calls, and prior history may determine how long the filtering is maintained.

[5] Note: Bad Actor may not be implemented in transitional NG9-1-1 systems. When implemented, even when the call is coming from a legacy network, the Legacy Network Gateway supplies the actual identity (Call Back number) of the caller, and not the ESQK/ESRK used in the call. Thus, in ESInets with full i3 PSAPs, Bad Actor will work for all callers where the identity is consistent.

Even if a large number of identities are involved in an attack, the Bad Actor mechanism can quickly slow, and then stop the attack calls. If the Bad Actor mechanism is coupled with the i3 mechanisms that allow overflow calls to be handled by any available call taker anywhere on any ESInet, a very large attack from a *finite* number of attack identities can be mitigated. The Bad Actor mechanism is not effective if spoofing is used with random identities for each attack call. STIR/SHAKEN may be effective against the use of random identities as long as the call source has not been compromised. It should be noted that the Bad Actor mechanism is required to be implemented in both the NGCS Border Control Function and PSAP Call Handling System.

Call Diversion is an important mechanism in NG9-1-1 that allows calls to be distributed to any available call taker, anywhere in the country. In the early stages of a TDoS attack, before mitigations come online, Call Diversion may be used to separate good calls from bad calls using the Bad Actor mechanism to label sources of bad calls. While the standards define how this works, deploying it depends on prior arrangements and provisioning.

6 Analysis and Mitigation of High-Volume TDoS Attacks in NG9-1-1

High Volume TDoS is defined in this document as TDoS exceeding the size of the pipes in the ingress network connecting originating service providers to the ESInet. Once the pipe fills, good calls may be blocked from coming into the ESInet and no mechanism between the originating service provider and the ESInet can fix that.

For several years, high volume DDoS attacks on popular Internet properties have been unsuccessful because we have developed effective strategies to mitigate such attacks, even when they reach multiple terabits. Even less popular sites are able to mitigate huge attacks successfully. As with our high volume TDoS attacks, these attacks are larger than the size of the pipe connecting the attacked systems to the Internet.

The mitigation method involves dedicated appliances that:

- are connected to extremely large bandwidth connections,
- are pre-programmed to recognize and filter attack traffic from all traffic when the attack uses a common mechanism,
- and have programmable filtering mechanisms that can be tuned by trained staff to separate good traffic from bad traffic when novel attacks are mounted.

When an attack occurs, the network routing Border Gateway Protocol (BGP) is modified so that instead of routing to the attacked property, it is redirected to so called "scrubbing centers" that have the appliances and staff to perform scrubbing. After filtering, the good traffic from attack traffic is fed to back to the original site via a private connection between the scrubbing center and the site. Several vendors offer services that work like this.

It turns out that the most popular appliances can mitigate SIP, and some of the services have staff trained to mitigate multi-terabit SIP attacks. Thus, the same techniques and services that mitigate multi-terabit DDoS can mitigate multi-terabit TDoS directed at NG9-1-1.

To be able to use these services, which usually have a modest per month fixed cost, the ESInet ingress networks and the OSPs that supply NG9-1-1 calls must be capable of having all NG9-1-1 traffic BGP-routed to the scrubbing centers. This is not how most current ingress networks are constructed. Therefore, changes in both the ESInet and the OSP networks are required.

STA-010 has, for some time, required that the NG9-1-1 system be able to mitigate the largest feasible attack, which at present, as noted, is a few terabits. Mitigation at this scale is very feasible economically and practically, but it does require a change in mindset and network design.

We note that once a large scale TDoS mitigation service is enabled, it can be deployed on attacks smaller than the access network pipe size. This means that special purpose mitigation for mid-size attacks may not be as attractive because the NG9-1-1 system can use the large-scale mitigation mechanisms for smaller scale attacks. It is probably unreasonable to do a BGP-reroute on small attacks, but it is likely the Border Control Function (BCF) mechanisms including "Bad Actor" can handle those.

7 Abbreviations, Terms, and Definitions

See the NENA Knowledge Base for a Glossary of terms and abbreviations used in NENA documents. Abbreviations and terms used in this document are listed below with their definitions.

Term or Abbreviation (Expansion)	**Definition / Description**
BGP (Border Gateway Protocol)	A protocol designed to exchange routing and reachability information among autonomous systems.
DoS (Denial of Service)	DoS (Denial of Service) A type of cyber-attack intended to overwhelm the resources of the target PSAP and deny the ability of legitimate users of the target to use the normal service the target provides. *DDoS (Distributed Denial of Service Attack)* A form of DoS in which the attack source is more than one, often thousands of unique IP addresses. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. *TDoS (Telephony Denial of Service)* A form of DoS directed at a telephony interface which generates numerous phone calls, tying up the network and preventing the destination from receiving legitimate calls. Occasionally the "T" in TDoS may be shown as Telephone or Telecommunications.

SHAKEN (Signature-based Handling of Asserted Information Using toKENs)	An industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network. (ATIS-1000074)
STIR (Secure Telephone Identity Revisited)	SIP header-based mechanism for verification that the originator of a SIP session is authorized to use the claimed source telephone number, where session is established with SIP end to end.

8 Recommended Reading and References

[1] National Emergency Number Association. *NENA Master Glossary of 9-1-1 Terminology*. NENA-ADM-000.24-2021. Arlington, VA: NENA, approved June 22, 2021.

[2] Alliance for Telecommunications Industry Solutions and the SIP Forum. *Errata to ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, Joint Alliance for Telecommunications Industry Solutions.* ATIS-1000080-E. Washington, DC: ATIS, approved February 27, 2019.

[3] Internet Engineering Task Force. *PASSporT: Personal Assertion Token*. C. Wendt and J. Peterson. RFC 8225, February 2018.

[4] Internet Engineering Task Force. *Authenticated Identity Management in the Session Initiation Protocol.* J. Peterson, C. Jennings, E. Rescorla, and C. Wendt. RFC 8224, February 2018.

[5] National Highway Traffic Safety Administration, 911 Program Office. "Cybersecurity". https://www.911.gov/documents_tools/Cybersecurity.html

[6] Federal Communications Commission, Communications Security, Reliability, and Interoperability Council VII. "Report on Session Initiation Protocol Security Challenges and Mitigation." March 10, 2021. https://www.fcc.gov/file/20609/download

[7] Federal Communications Commission, Communications Security, Reliability, and Interoperability Council VII. "Final Report CSRIC Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks." March 10, 2021. https://www.fcc.gov/file/20607/download

[8] National Emergency Number Association. *NENA i3 Standard for Next Generation 9-1-1.* NENA-STA-010.3-2021. Arlington, VA: NENA, approved July 12,2021.

[9] National Emergency Number Association. *NENA Detailed Functional and Interface Standards for the NENA i3 Solution.* NENA-STA-010.2-2016. Arlington, VA: NENA, approved September 10, 2016.

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Systems Security & Resiliency Committee, Telephony Denial of Service (TDoS) Working Group developed this document.

NENA Board of Directors Approval Date: 03/04/2022

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Dan Mongrain, Systems Security & Resiliency Committee Co-Chair	Motorola Solutions, Inc.
Raymond Paddock, Systems Security & Resiliency Committee Co-Chair	Inteliquent, Inc.
Mark Collier, Working Group Co-Chair	SecureLogix
Sarah Rollins, Working Group Co-Chair	Consultant
Tom Breen, ENP, Technical Editor	SecuLore Solutions, LLC
Robert Little, ENP	City of Columbus, OH
Brian Rosen	Brian Rosen Technologies, LLC
Rakhee Duneja	Toronto Police Service, ON CA
Roger Marshall	Comtech Telecommunications Corporation
Tim Lorello	SecuLore Solutions, LLC
Mark Lindsey	ECG, Inc.
Brad Flanagan, ENP	Pitkin County, CO
Terry Purvis, ENP	Williamson County, TX
Bernard Brabant	Consultant

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The Telephony Denial of Service (TDoS) Working Group is part of the NENA Development Group that is led by:

- Jim Shepard, ENP and Wendi Rooney, ENP, Development Steering Council Co-Chairs
- Brandon Abley, ENP, Technical Issues Director
- April Heinze, ENP, 9-1-1 and PSAP Operations Director