

NENA

Impact of IoT Devices and Emergency Calling Applications Information Document

Abstract: This Information document describes the impact of Internet of Things (IoT) devices and emergency calling applications (Apps) on 9-1-1 and provides crucial instruction to developers of IoT devices and systems so that their implementations are effective in their intended interaction with 9-1-1 services.



NENA Impact of IoT Devices and Emergency Calling Applications Information Document

NENA-INF-030.1-2020

DSC Approval: 06/09/2020

PRC Approval: 07/31/2020

NENA Board of Directors Approval: 08/19/2020

Next Scheduled Review Date: 08/19/2021

Prepared by:

National Emergency Number Association (NENA) Systems Security & Resiliency Committee,
IOT/APPS Working Group

Published by NENA

Printed in USA



© Copyright 2020 National Emergency Number Association, Inc.

1 Executive Overview

This Information document describes the impact of Internet of Things (IoT) devices and emergency calling applications (Apps) on 9-1-1. Developers of IoT devices, and developers and managers of systems that employ these devices, should consider this document in the early phases of design and development, to address the potential impact on 9-1-1 operations, and to assure that their implementation(s) are effective in their intended emergency notification to 9-1-1 services.

This document discusses impacts to the operations of 9-1-1 system operators and Public Safety Answering Points (PSAPs) caused by emergency calls and data received from IoT devices and Apps.

Table of Contents

1	EXECUTIVE OVERVIEW	2
	INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY	6
	REASON FOR ISSUE/REISSUE.....	6
2	9-1-1 IMPACTS OF IOT DEVICES AND APPS.....	7
2.1	INTRODUCTION	7
2.2	FLEXIBILITY AND OPERATIONAL CONTROL	8
2.2.1	Call Routing.....	8
2.3	LOCATION ACCURACY	9
2.4	IOT/APP IMPACTS	10
2.4.1	Impacts of Incident Data	10
2.4.2	Impacts of Call and Data Volume	11
2.5	STATIC VERSUS DYNAMIC DATA.....	12
2.6	NON-INTERACTIVE STREAMING MEDIA	12
2.7	DATA RETENTION AND DISCLOSURE	12
2.8	COMPATIBILITY WITH NENA STANDARDS AND PROTOCOLS.....	12
2.8.1	IoT Device/Apps Gateway	13
2.8.2	Connection Models for IoT Device Initiated Calls	13
2.9	INTERACTIVE VERSUS NON-INTERACTIVE (DATA ONLY) CALLS	17
2.10	INFORMATION ABOUT RELATED DATA OR CALLS	17
2.11	AUTONOMOUS VERSUS HUMAN INITIATED/MEDIATED IOT/APPS CALLS	18
2.12	SECURITY.....	19
2.12.1	Security of the Device	20
2.12.2	Data Privacy.....	21
2.13	ADDITIONAL WORKLOAD CONSIDERATIONS	22
2.13.1	PSAP Workload	22
2.13.2	Backroom Workload	22
2.13.3	Administrative Effort.....	23
2.14	ADDITIONAL IMPACTS.....	23
2.14.1	External Impacts.....	23
2.14.2	IoT/App Call Origination.....	24
2.14.3	Liability Considerations	24
3	IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS.....	25
3.1	OPERATIONS IMPACTS SUMMARY.....	25
3.2	TECHNICAL IMPACTS SUMMARY.....	25
3.3	SECURITY IMPACTS SUMMARY	26
3.4	RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK	26
3.4.1	Assistance to implementers.....	26
3.4.2	Industry Liaison.....	26
3.4.3	PSAP IoT/App Forum.....	26
3.4.4	Data Definitions	27
3.4.5	Information Criticality and Call Autonomy.....	27
3.4.6	Internal Information Sharing.....	27
3.4.7	Regulatory and Legislative Concerns.....	28
3.5	ANTICIPATED TIMELINE.....	28

3.6	COST FACTORS	28
3.6.1	<i>IoT Resource Demands</i>	28
3.7	COST RECOVERY CONSIDERATIONS	29
3.7.1	<i>Funding Models</i>	29
3.8	ADDITIONAL IMPACTS (NON-COST RELATED)	30
3.9	ABBREVIATIONS, TERMS, AND DEFINITIONS.....	30
4	RECOMMENDED READING AND REFERENCES.....	33
5	EXHIBIT X.....	33
6	APPENDIX X	33
	ACKNOWLEDGEMENTS	34

**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.

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 this document.

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-030.1-2020	08/19/2020	Initial Document

2 9-1-1 Impacts of IoT devices and Apps

2.1 Introduction

This document focuses on the following areas:

IoT: The Internet of Things (IoT) is the description given to the general category of devices that utilize Internet Protocols for the transmission of data and multimedia communications that typically fall outside of the classifications of traditional mobile and landline telephone devices. IoT devices are inclusive of devices that operate with or without human interaction.

Devices: The devices that utilize IoT protocols are/will be extremely varied with a wide variety of potential interactions ranging from the obvious, such as lights being turned on when an alarm system senses activity, to coordinated operations between complex systems. (Devices that direct a cellphone to initiate a 9-1-1 call are out of scope, as the call will be a cellphone-initiated 9-1-1 call.)

9-1-1 Impacts: Many of the devices are part of or perform functions related to alarms for potential emergency conditions. Examples of such devices include:

- baby monitors,
- intrusion detection,
- potential overheating situations due to malfunctions in HVAC systems,
- smoke and carbon monoxide detectors (typically stationary or in an RV),
- HAZMAT detectors,
- burglar alarms,
- flood sensors,
- personal emergency response systems (PERS) and mobile personal emergency response systems (mPERS),
- smart speakers (such as Amazon Echo, Google Home, etc.),
- connected automobiles (see discussion on Next Generation-Advanced Automatic Crash Notification [NG-AACN] here and in NENA STA-010.3 [3]),
- smart doorbell connected cameras or other fixed/installed smart home devices.

9-1-1 Notification: The primary question will be if it is appropriate to notify 9-1-1 (by the generation of an interactive 9-1-1 call, or a non-interactive [data-only] 9-1-1 alert call), for the event.

In many cases notification to a responsible party (e.g., a partly-automated aggregator, a human monitor, etc.) other than 9-1-1 should be the first action; the notified party may

direct the system to notify 9-1-1, and there could be provisions for the system to direct the call to 9-1-1 should the responsible party not respond within a predetermined parameter, or based on similar events within an area.

In some instances, information detected by sensors in a device might indicate a critical event, or a potentially critical event, while in other cases the information might indicate a situation that could become critical if not resolved. In many cases, events generated by Apps under the direction of a user might be presumed critical.

2.2 Flexibility and Operational Control

Accommodating IoT device/system/App calls to 9-1-1 requires adherence to i3 (NENA STA-010.03 [3]), which provides PSAPs considerable control over the calls and data. PSAPs will need to develop policies regarding processing of calls (especially non-interactive calls) and handling of data. PSAP CAD and call handling systems will need to support the implementation of such policies. For example, PSAPs will need policies regarding the level of trust or suspicion for incoming calls from IoT devices and Apps. Crucially, PSAPs will need policies regarding new Additional Data blocks, establishing which data elements in which blocks to access and which to ignore (which remain available to other entities such as responders), and for those data elements/blocks that are accessed, which data elements to present to call takers, which to make available to call takers (such as in a drill-down), etc. Section 2.4.1 contains more discussion on policies regarding data items and data blocks. For example, a PSAP may have a policy that information such as supplemental (non-interactive) video will not routinely be displayed to call takers (while remaining available to dispatched units or incident command).

Agencies should report to the appropriate supplying or delivering company or organization any discrepancies or inadequate information. This could be the developers, vendors, aggregators, an entity operating a campus, a VoIP carrier, or a cellular carrier.

Upon introduction of new data blocks, PSAPs should review their information retention and release policies (see Section 2.6 for discussion on data retention).

PSAPs should distinguish between incoming information from public/commercial (citizen) IoT devices/Apps, and those used by emergency personnel (e.g., firefighters wearing monitoring devices, responders reporting a separate event they observe). Note that citizen devices convey data as Additional Data blocks referenced in Call-Info SIP header fields, while data blocks from responder devices are in Emergency Incident Data Objects (EIDOs) [2] .

2.2.1 Call Routing

The i3 Policy-Based Routing capability allows for IoT device/App calls, or interactive versus non-interactive IoT device/App calls, to be routed differently (e.g., based on the presence

or content of Additional Data blocks and/or Session Description Protocol [SDP]). Please refer to NENA-INF-011, NG9-1-1 Policy Routing Rules Operations Guide [4] .

2.3 Location Accuracy

The advent of 9-1-1 calls being initiated by IoT devices/Apps exacerbates the criticality of having accurate location information delivered with the call. This is particularly important where there may be no ability to verbally confirm location information through human interaction with a person on the call, and where the 9-1-1 call may be generated by a system of linked IoT devices that are generating the call due to a series of detected events that the system deems as critical.

All incoming 9-1-1 calls from IoT devices or Apps are required to have location data (in accordance with i3 [NENA STA-010] [3]). Calls without location information and without a live person on the call are out of scope of this document, as it is unreasonable to expect such calls to be routed. Calls that lack location information but do have a live person on the call who can provide location information are considered non-IoT calls and hence also out of scope of this document (e.g., legacy alarm system calls).

In many cases, a device or App is located at the scene of an incident being reported. This is not always the case; some devices may detect and report incidents that could be a significant distance from the location of the device. An example where a device reports an incident at a different location than itself is a camera covering a wide area that may be capable of extrapolating a location based on angle and distance; another example is a gunshot detector that may extrapolate a location based on the parameters of the sound. There may be cases where a device is at the location of an incident but a person authorizing a 9-1-1 call is at a different location. An example of this is a smart doorbell or smart security system installed at a property in Texas that alerts the property owner of a person at the door or a break-in. The property owner is in Delaware and uses the monitor App to instruct the device to initiate a 9-1-1 call. The Geolocation header field of the call is used to route the call and may also be used for dispatch, and so references the incident location. When the location of the device or App user is known to differ from the incident location, it should be conveyed in an Additional Data block for supplemental purposes. An Owner/Subscriber Information block should be used to convey this information. (An Owner/Subscriber Information block is able to contain civic and geospatial location information.) In addition, a Comment block should be added with text indicating that the Owner/Subscriber Information block is provided for supplemental purposes to convey the device/device user location. This Comment block should contain the Content-ID of the Owner/Subscriber Information block.

As is true generally for NG9-1-1 calls, but may especially be relevant for calls originated by IoT devices, the accuracy of the location information that arrives with a call may or may not have been verified. The entity performing any verification may employ various mechanisms that can influence the degree of reliance by public safety on the integrity of

the location. The source of location information carried by value, or the identity of a location server indicated in location by reference, may influence the degree of trust in the location information. Calls may be originated with participation from a known origination network or may be originated independently, using an access network that does not participate in the SIP signaling or location information provisioning. As examples, location information may be provided by an untrusted source (e.g., an originating device) and not have been sanity-checked by a trusted carrier; location information may be provided by an untrusted source but be congruent with (e.g., sanity-checked against) information from a trusted source such as access points of a trusted origination carrier; location information may be provided by or mediated by a trusted source (e.g., location by reference from a trusted carrier).

It may be helpful for PSAP call takers to be aware of information about a location or environment, for example, a building or site in which an IoT device generating a 9-1-1 call is deployed. Such information may include building plans, hazardous materials, as well as classifications such as residential (which could further indicate single- versus multi-unit, number of floors, etc.), retail, commercial, public, government, critical infrastructure, and/or educational (which could further indicate pre-school, elementary, middle, high, collegiate, etc.). NENA i3 provides a mechanism for this: Additional Data associated with a location. This mechanism permits Additional Data blocks to be accessed by location. These data blocks are accessed via a URI obtained by querying an Emergency Call Routing Function (ECRF) rather than being carried with a call. See NENA STA-010.3 for more detail. While processing an emergency call, PSAP equipment may perform a query to obtain Additional Data URIs for the call's location. If such Additional Data URIs are returned, the PSAP equipment may then resolve those to obtain the Additional Data blocks. Note that as of the date of this document, these Additional Data blocks have not yet been specified.

2.4 IoT/App Impacts

The ability of IoT devices and Apps to generate interactive and non-interactive calls creates a set of impacts on the 9-1-1 system.

2.4.1 Impacts of Incident Data

IoT device and App generated calls (both interactive and non-interactive) can contain a rich set of data (including incident-specific data) that can be helpful for telecommunicators to assess situations and determine appropriate responses. In many cases, such data were previously unavailable or only available through proprietary systems. The NENA i3 architecture, through the Additional Data mechanism, allows these data items to be standardized, labeled, registered, shared, recognized, and processed per PSAP policy, as well as used in post-incident analysis.

IoT devices and Apps may have the ability to be updated dynamically, and new devices and Apps are continually created, often with increased functionality (e.g., additional

sensors, enhanced sensor data processing). There is a natural tension between speed and innovation on the one side, and interoperability and PSAP processes on the other. At one extreme, new types of data sent to a PSAP may be informative and helpful while also being outside the set of standardized formats, unable to be automatically recognized or processed by PSAP equipment, and potentially confusing to call takers, administrators, reviewers, etc. When transferring calls between PSAPs or between PSAPs and responders, novel data sets can cause non-trivial problems. At the other extreme, waiting for various standards documents to be updated can excessively and needlessly delay the ability of call takers to get the most accurate and useful information about a situation.

Properly handling new data sets that may be carried in calls (either interactive or non-interactive) typically requires that the data set be standardized, registered, and labeled, so that it can be recognized and treated per policy, processed by various equipment, and shared among PSAPs and responders. PSAP equipment needs to recognize the data sets and data elements for proper logging and execution of PSAP policy. PSAP policy may specify which data sets or data elements are displayed to call takers with call presentation, available to call takers on request (e.g., using a drill-down), available only for post-call analysis, or not accessed by a PSAP at all. As an example, a PSAP might determine that certain medical data is not to be accessed within the PSAP (e.g., for privacy and confidentiality reasons). The Additional Data mechanism allows each PSAP or responder handling a call to access data blocks or not.

All data blocks must conform to i3 standards. (This may require that IoT developers work with other developers in order to standardize new data blocks for similar applications.) Data blocks that do not conform to i3 standards are incompatible with the 9-1-1 system and will result in messaging failures.

2.4.2 Impacts of Call and Data Volume

IoT devices may generate a high volume of alerts in a short period of time, and any device may be capable of generating a high volume of updated data. In some cases, IoT devices may use non-i3-compliant protocols and hence must communicate with 9-1-1 systems via a gateway that performs protocol and data conversion between the non-i3-compliant protocol and i3 (see section 2.8). Depending on design, a device or App could potentially initiate multiple calls in rapid succession, or a set of devices could initiate multiple simultaneous calls, and devices or Apps could rapidly update sensor or other data. Such a flood of calls or data updates has the potential to overwhelm 9-1-1 systems and call takers or be interpreted by 9-1-1 systems as a Distributed Denial of Service (DDoS) attempt (causing calls from the IoT system to be blocked). The developers or vendors of IoT devices and Apps may choose to use an intermediate system to analyze and aggregate calls or data updates. In some cases, intermediary or gateway systems mediate calls using algorithms and/or analytics to help improve the validity of alerts along with the accuracy of data supplied in calls.

See Sections 2.8.1 and 2.8.2 for more discussion on gateways and deployment models.

2.5 Static Versus Dynamic Data

Non-location data sent with a call (i.e., App data) may be static or dynamic. Static data is not updated during the call. Dynamic data may be updated during the call. There are different mechanisms available for providing data updates: updates may be triggered by the call originator (referred to as the "push" model), such as the SUBSCRIBE/NOTIFY mechanism defined by the IETF and in NENA i3 (STA-010) [3] ; updates may be requested by the receiver (referred to as a "pull" model), e.g., a URI for updates sent in a Call-Info header or within an Additional Data block (e.g., using the request/response mechanism defined by the IETF and in NENA i3 (STA-010) for vehicle-initiated emergency calls); or a continuous data stream (e.g., sent in a non-interactive media stream).

2.6 Non-Interactive Streaming Media

An interactive 9-1-1 call may in some cases negotiate or offer streaming media intended for PSAP information rather than interactive communications. For example, a smart doorbell or smart security system may initiate an interactive 9-1-1 call where the property owner (perhaps off-site) is available to talk with the call taker via an interactive two-way audio stream while also offering/negotiating one-way video and audio streams of the premises that show the situation, which can assist in determining if dispatch is needed. Another example is NG-AACN calls, where an interactive call is established by the vehicle, allowing the call taker and the vehicle occupants to communicate; the AACN metadata/control mechanism allows the vehicle to identify cameras available for the call taker to monitor. Non-interactive (data-only) calls may also make available one-way non-interactive streaming media. Since non-interactive calls do not establish a SIP session, the streams will typically be offered as URIs located in Call-Info header fields or in Additional Data blocks referenced by Call-Info header fields.

2.7 Data Retention and Disclosure

PSAPs will need to determine how to appropriately retain data received from IoT devices, systems, and Apps in accordance with applicable requirements (e.g., retention of evidence). Similar determinations will need to be made related to requirements mandating or prohibiting public disclosure of information transmitted. For example, health or medical information might be excluded from applicable open records policies.

Prior to receiving new data blocks, PSAPs should review their policies on information retention and disclosure as these policies may need to be expanded or updated.

2.8 Compatibility with NENA Standards and Protocols

It is expected that all IoT devices, systems, and Apps that interface to 9-1-1 will fully comply with all applicable NENA standards and protocols (for example, the interfaces,

methods, data, and other requirements specified in NENA STA-010, known as i3). In situations where a device or App is not compliant with i3 (as discussed in Section 2.4.2 and in this section below), a gateway is needed to interface with 9-1-1. See Section 2.8.1 for further information.

2.8.1 IoT Device/Apps Gateway

Due to the potential complexity of the interface between IoT devices or Apps and the NG9-1-1 system, some IoT device/App developers may choose to utilize a gateway (possibly developed by a third party) to handle this interface. This decision could potentially free the developer from the need to fully understand and implement the NENA-approved standards and protocols, but it could also potentially limit the developer to the types of interactions with 9-1-1 that are implemented by the gateway.

2.8.2 Connection Models for IoT Device Initiated Calls

There are two connection models envisioned for IoT devices to report an emergency incident. These are a direct connection model and an aggregated connection model. Either model might deploy a gateway as discussed above.

2.8.2.1 Direct Connection

IoT devices in this model initiate an NG9-1-1 call (interactive or non-interactive) directly toward an ESInet without traversing an aggregation intermediary function. This approach requires IoT device interface conformance with i3 (NENA STA-010.3) [3] . Advantages of a Direct Connection include:

- No delay in information sent since there is no aggregator
- Direct message conveyance requiring no middlebox potentially charging for service access
- Direct support of NENA i3 in the IoT device may reduce risk of incorrect signaling or data conversion/interworking

2.8.2.2 Aggregated Connection

An intermediary may be deployed in between the IoT device and the NG9-1-1 network to perform the following features and capabilities. Advantages of an Aggregated Connection include:

- Context determination: A middlebox that aggregates messages received from IoT devices can potentially detect some IoT false positives and determine single vs. multiple incidents and severity of impacts
- Security and Scalability: A middlebox can assist with security checks and reduce the scaling impact on an ESInet (e.g., by aggregating potentially many thousands of emergency incident calls into one)

- Reporting: System usage, history, and health monitoring can be enabled through the use of an aggregator for the IoT devices that it serves
- Test/Verification: Periodic testing of IoT devices to verify operational viability could be facilitated by a middlebox
- Association: Retrieval of additional data, including specific IoT device data or external data from other sources may be merged/blended and made available to the PSAP

2.8.2.3 Gateways/Protocol Converters

IoT devices or aggregators that do not support NENA i3 must use a protocol converter or gateway. When a gateway is used:

- There is no restriction on the number of IoT gateways deployed
- It is assumed that gateway operators will have some kind of interconnection agreement with ESInet operators that they are connected to
- IoT gateways will need to conform to ESInet input requirements on the egress side of the gateway, but can support any input protocol
- An IoT gateway, sometimes referred to as a protocol converter, is considered an orthogonal function and therefore may be deployed with either the direct or aggregated models. For example, an IoT gateway can allow IoT devices and/or aggregators to support HTTP but not SIP as their primary protocol

Examples

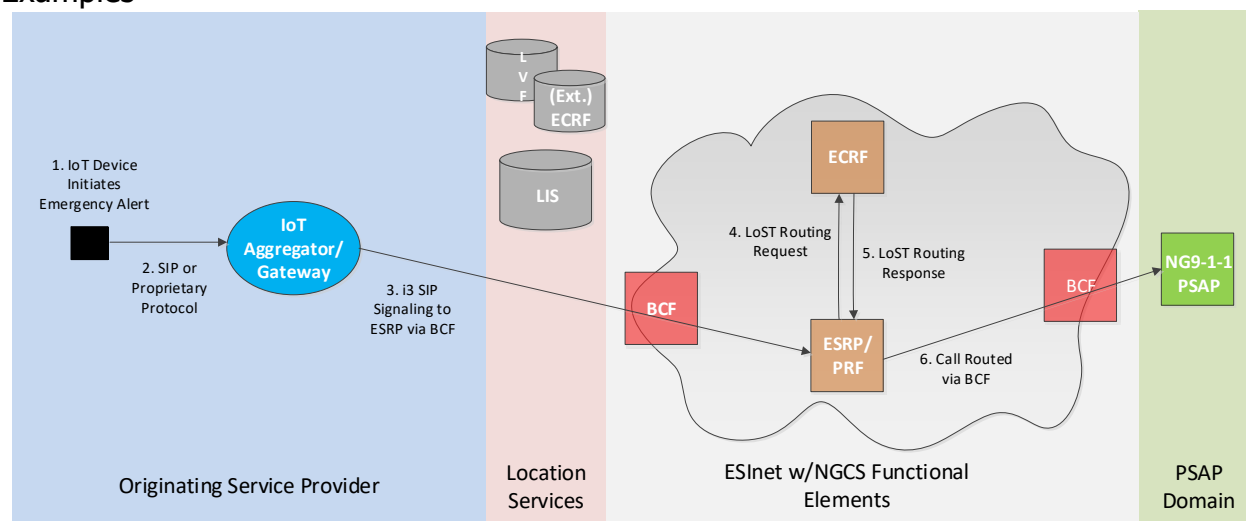


Figure 1. Aggregated IoT Call to ESInet/NGCS and NG9-1-1 PSAP

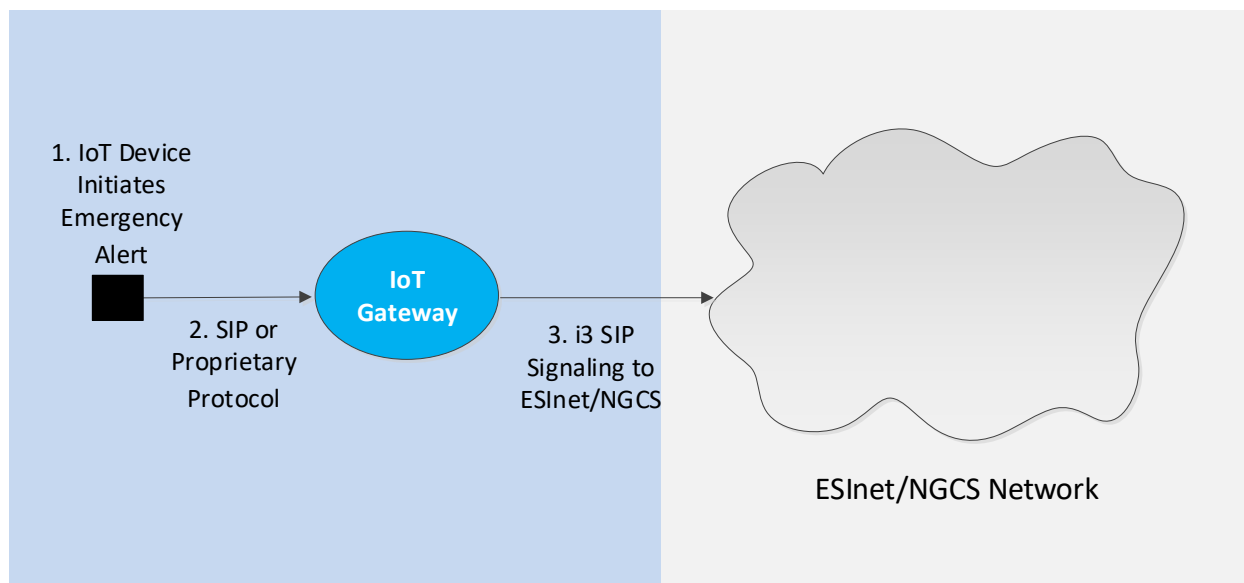


Figure 2. IoT Direct (Via Gateway) to ESInet/NGCS

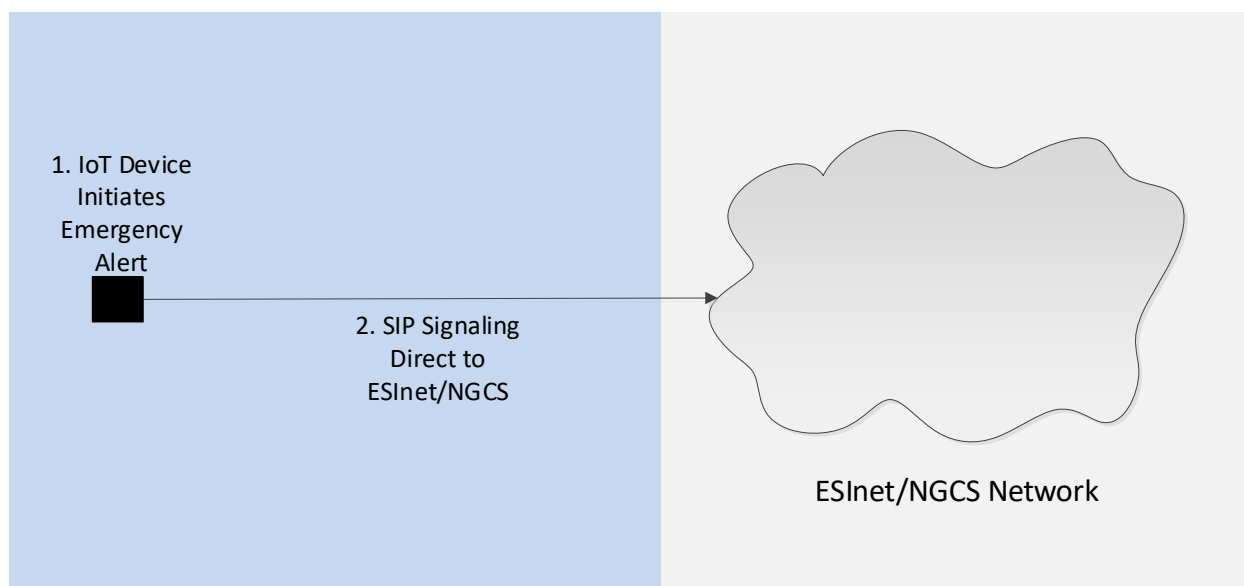


Figure 3. IoT Direct (no Gateway) to ESInet/NGCS

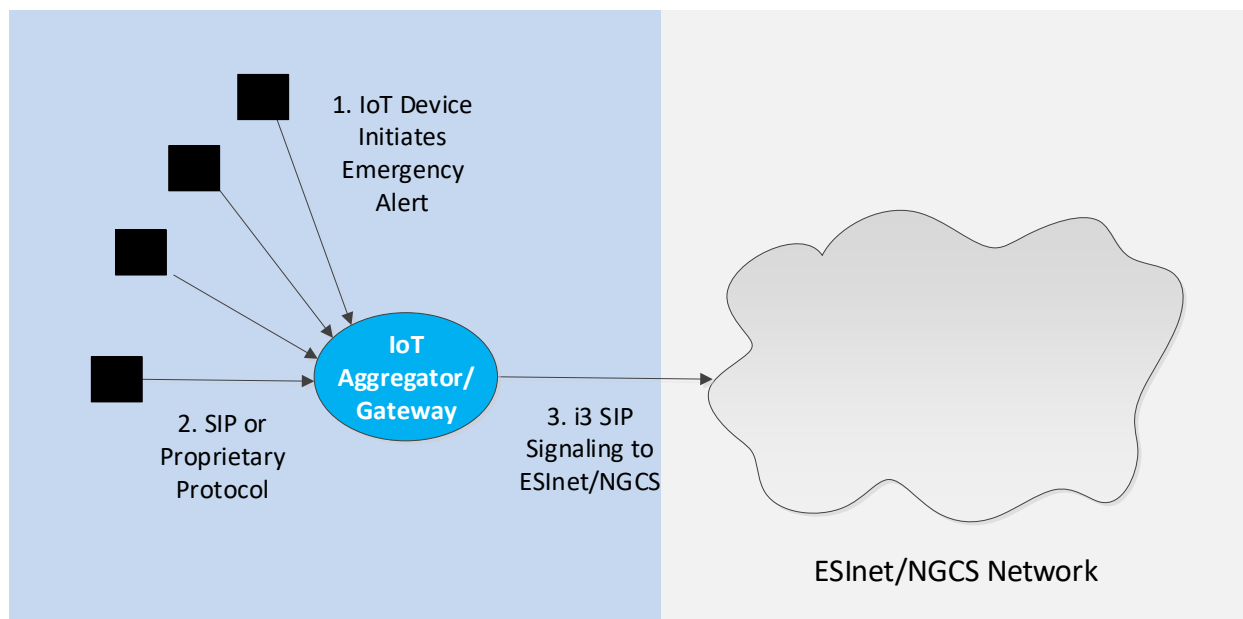


Figure 4. IoT Aggregator (no Gateway) to ESInet/NGCS

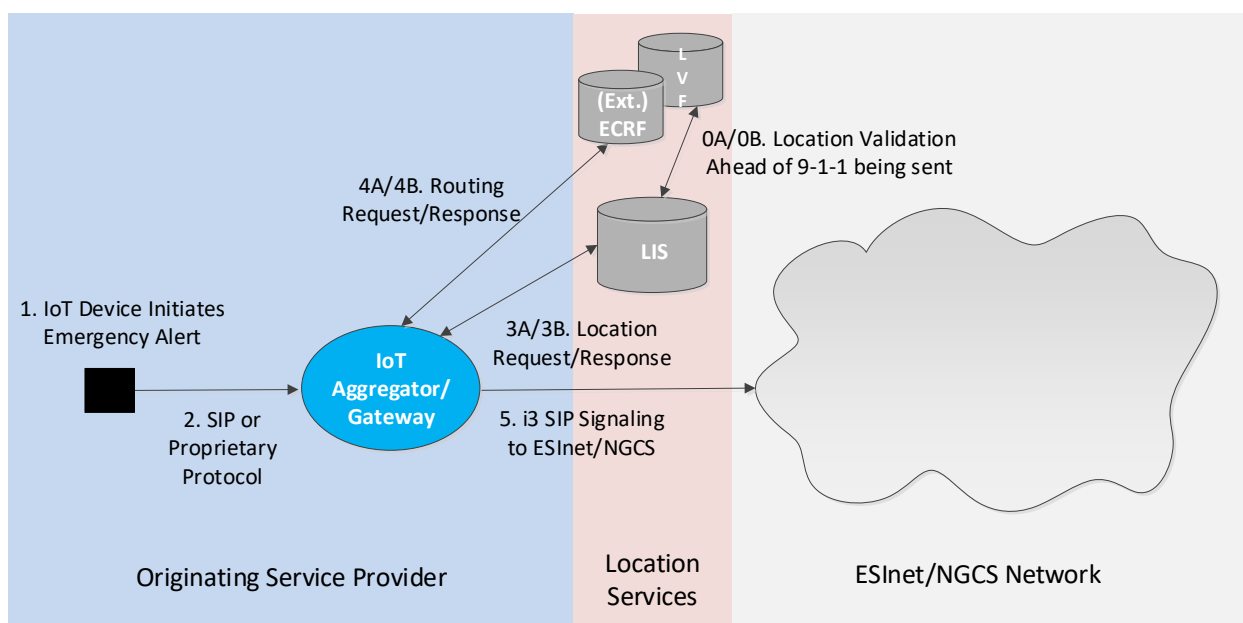


Figure 5. IoT Gateway with Network (OBO) Location to ESInet/NGCS

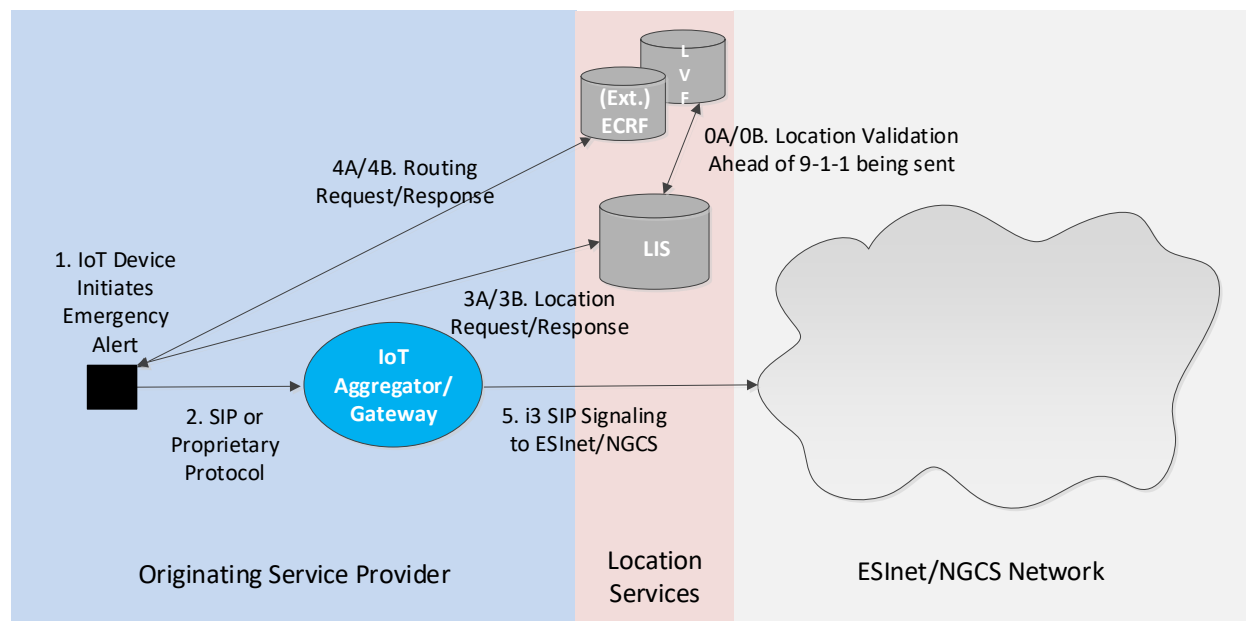


Figure 6. IoT Gateway with End Device Location to ESInet/NGCS

2.9 Interactive versus Non-Interactive (Data Only) Calls

Calls initiated or facilitated by IoT devices and Apps are either interactive or non-interactive. Non-interactive calls are also referred to as data-only calls. If there is an expectation that a call taker can interact with a human, an interactive call is established using SIP INVITE and typically negotiating one or more interactive media streams. If there is no expectation of such interaction (e.g., a call established by a device lacking a microphone or speaker), a non-interactive (data only) call is established using SIP MESSAGE and containing a CAP body. The i3 (NENA STA-010.3) [3] specification provides details and descriptions for both types of calls.

Potentially, some IoT devices might initiate calls where a human may not necessarily be immediately available (e.g., a baby monitor in autonomous mode that detects an urgent situation and initiates a 9-1-1 call while simultaneously paging nearby humans). Such calls are established as interactive calls because the device supports interactive media and a human is expected to be available at some point during the call, even if not immediately. There is currently no standardized mechanism for such calls to be differentiated or identified to the PSAP, and hence it may be difficult for a call taker to differentiate this situation from one where a human is present but is unconscious or otherwise unable to respond.

2.10 Information about Related Data or Calls

When a 9-1-1 call originates via an aggregator, a system deploying sensors, a campus, or similar entity, the entity may be aware of related alerts or sensor, camera, or other data.

Part of the data sent with a 9-1-1 call might be information about similar calls generated by the system or sensors, video, or other data sources near the location that are available to provide data to the call taker. As an example, a field in an Additional Data block could be a URI to a map showing nearby sensors or cameras, or nearby anomalous readings, or could comprise multiple Presence Information Data Format-Location Object (PIDF-LO) sets, each providing location for a related sensor or camera. Separately, PSAP equipment might detect when multiple IoT/App calls originate near each other and could provide cross-linkage to tie them together.

2.11 Autonomous Versus Human Initiated/Mediated IoT/Apps Calls

Other than calls generated from vehicle-based telematics systems (Advanced Automatic Crash Notification or AACN) there are few examples deployed of autonomously-initiated 9-1-1 calls. Because of the prevalence of false alerts in early autonomous systems such as burglar alarms, there has been a strong bias that autonomous alerts be screened by call centers so that calls are forwarded to a PSAP only if necessary and appropriate. AACN deployment has demonstrated that well-designed sensor-based systems can have low false-positive rates. AACN calls carry a flag in the call set-up signaling¹ that differentiates autonomously-initiated from manually-initiated calls².

As sensor and artificial intelligence capabilities increase while costs decrease, both IoT devices and Apps are likely to become more capable of distinguishing genuine emergencies, although there will remain large differences from device to device, App to App, with some devices or Apps proving more reliable than others. It is expected that IoT devices and Apps will increasingly place 9-1-1 calls without human intervention.

The degree of autonomy in 9-1-1 call initiation can be viewed as a range, with completely manual calls on one end and fully autonomous calls on the other. In between are calls suggested by a device or App but triggered by a human, and calls initiated by a device or App with the ability of a human to cancel. As an example, consider calls by IoT devices or Apps that are screened by a call center. Perhaps initially, all such calls may be manually screened, with a human operator determining which should be directed to a PSAP. A machine-learning system may analyze the human decisions along with the call parameters, and start suggesting a determination to the human, perhaps progressing to autonomously handling calls in which it has high confidence while allowing a human to handle the rest, and later may autonomously handle all or almost all calls.

¹ For NG-AACN, a different sub-URN in the Request-URI is used.

² Experience with AACN calls is that manually initiated ones may have a higher false positive rate. It has also been suggested that autonomous AACN calls may be more likely to require a medical and in some cases trauma dispatch, while manual AACN calls may be more likely to be reports of impaired drivers or road hazards that require police.

The level of autonomy or human involvement in call initiation is separate from whether there is an expectation that a PSAP call taker can communicate with a human during the call. For example, a medical monitor device may be equipped with a microphone and speaker allowing a call taker to communicate with the wearer, and AACN vehicles likewise allow interactive communication during emergency calls. Both may provide for both manual and autonomous 9-1-1 call initiation. Burglar, fire, flood, chemical spill, and other such alarm systems may have no capacity or expectation of interactive communication (although they may provide for streaming video and/or audio), yet they might have the ability for a human to approve or cancel an emergency call as well as to manually initiate a 9-1-1 call (e.g., via a panic button). It may be helpful to PSAP call takers to know if a call was manually or autonomously initiated (interactive calls have an expectation of human interaction while non-interactive calls do not). For example, an autonomously initiated interactive call where there is no response to a call taker's questions may indicate an unconscious or absent victim.

There are numerous examples where an IoT device or App might determine that an emergency call is warranted. Aside from the examples above, other such IoT devices include gunshot detectors and surveillance cameras that use facial recognition or license plate reading to identify fugitives. These devices may be deployed by public safety agencies and may identify situations warranting immediate dispatch³.

It may be desirable for IoT/App 9-1-1 calls to distinguish manual from autonomous initiation (as is the case for AACN calls), and potentially the degree of autonomy. While this information may not affect the call taking and dispatching process, it could prove helpful to responding personnel. For example, arriving personnel would be able to explain why they have responded if they are met with surprise by people who are unaware that a call was placed. The information may also have value when analyzing the performance of the system or following up on a malfunction.

2.12 Security

Autonomous Internet of Things devices present a distinct set of security challenges. The fact that the devices being described in this document can send alerts directly into the ESInet (and downstream to PSAPs), and the fact that users will rely on these devices for the protection of life and property, means the impact of these devices being hijacked, attacked or otherwise compromised can be severe.

IoT devices and the systems they are integrated into will be of variable designs making consistency of security protection difficult. In addition, the sensors and other elements

³ Note that, if the device is inside an ESInet (directly or via a VPN) and the appropriate dispatch URI is known, the device creates an incident by sending an Emergency Incident Data Object (EIDO) [2] (e.g., in a MESSAGE routed to a pre-determined dispatch) per Incident Data Exchange (IDX), while devices outside an ESInet or where the appropriate dispatch URI is not known in advance generate calls carrying citizen Additional Data blocks and location information, per i3.

including software of the IoT devices themselves are likely to be purchased as commodity products with unknown and potentially widespread attack vulnerabilities. Even when vulnerabilities are discovered it may be difficult to identify the placement of the impacted units. Deployed IoT devices may have widely varying capabilities for remote software updates, and such software updates (as discussed elsewhere) themselves raise the potential for compromise. If IoT software, firmware or hardware are compromised, this could lead to a capability for a DDoS attack on the 9-1-1 system by activating widespread critical event notifications from the systems where the sensors or elements have been installed. Systems with incorporated IoT devices may be operated by entities known to emergency authorities, and therefore such systems might be subject to a lower inherent level of suspicion when calls and alerts enter the 9-1-1 system which could enhance the apparent legitimacy of malicious calls. This lower level of suspicion plus the likely widespread locations for the calls may make this type of nefarious activity difficult to recognize other than by volume of similar calls.

For devices capable of calling 9-1-1, several aspects of security need to be addressed:

- A. Security of the Device
- B. Data Privacy
- C. Transport Layer Security
- D. Application Layer Security
- E. Security Considerations at the PSAP

2.12.1 Security of the Device

Potential scenarios arising from malicious access to an IoT device include:

- sending incorrect information to the ESInet/PSAP in a valid emergency
- sending an invalid location to the ESInet/PSAP (e.g., swatting attack or denial of service)
- not responding to a valid emergency situation (device disabled or altered location)
- triggering emergency notifications in non-emergency situations
- attacking the ESInet/PSAP with continuous notifications when no emergency exists
- theft of private or protected information contained within the device
- using the device to attack other parts of the network (e.g., denial of service attack)

Device manufacturers, vendors and installers need to incorporate security awareness and risk assessment into their standard processes. Network operators will need to increase their security awareness as IoT devices that interface with the ESInet become available to the public.

Devices need to be hardened to prevent unauthorized usage; the device should require that any default password be changed the first time the device is configured, and best-practice password-strength enforcement needs to be applied. The device needs to provide appropriate root-level security to prevent malicious software/firmware modification.

Validation of configuration parameters and other inputs to the device needs to be robust in order to protect against possible code injection and buffer overflow attacks. Performance and boundary testing of the device should be performed to ensure a level of confidence against buffer overflow and fuzzing attacks.

Any inbound ports that are not required for the normal operation of the device should not have active listeners.

Device manufacturers need to provide an appropriately secure mechanism for updating the software/firmware contained within the device. Software updates need to be code-signed, so that the device can ensure that the code has not been altered. Device manufacturers should also provide an incident reporting and tracking mechanism.

Any device initiating an emergency call to the ESInet should uniquely identify itself with information that includes a device serial number and/or MAC address and a software revision level using the Additional Data block for Device Information. This enhances the ability to apply call suspicion processing, such as increasing the suspicion level of calls from devices believed to be defective/untrustworthy (i.e., bad actors). As part of call suspicion processing, calls from devices that do not include this information should be marked with a high level of suspicion and might be rejected or treated with low priority by the ESInet and PSAP per policy.

2.12.2 Data Privacy

Manufacturers of devices that are configured to contain private information (e.g., medical data, etc.) need to perform a privacy impact analysis as part of their security process and be aware of all regulations that apply (e.g., Health Insurance Portability and Accountability Act [HIPAA], General Data Protection Regulation [GDPR]). Any private information stored within the device should be encrypted.

2.12.2.1 Transport Layer Security

All devices need to adhere to the i3-specified security requirements regulating the transport of signaling and media.

2.12.2.2 Application Layer Security

Standard SIP authentication measures are recommended where feasible to verify the identity of the device and/or user account requesting service from the network. Such authentication requires the IoT device to have a relationship with a SIP node in the network that can perform the authentication. This node may be maintained by an ESInet operator, or it could be operated by a vendor or other authority (that has a trusted relationship with the ESInet). Note that the ESInet and/or PSAPs may take authentication or lack thereof into account when prioritizing incoming calls and making decisions regarding bad actors.

2.12.2.3 Security Considerations at the PSAP

Any firewall or protective software analyzing IoT data streams associated with IoT calls to 9-1-1 should be fully capable of examining multiple data types for potentially nefarious elements and blocking those data streams while transmitting clean elements to permit receipt of the call and its associated data.

Consideration will need to be given to assuring that transmitted information such as links to web pages and additional data documents do not compromise security.

As technology evolves, so will the complexity of cyber security threats, and the industry needs to continuously upgrade its approach to dealing with these threats, especially from IoT devices. A number of organizations are working toward defining security standards for the Internet of Things, including:

- National Institute of Standards and Technology (NIST)
- Internet Engineering Task Force (IETF)
- U.S. Department of Homeland Security
- Internet of Things Security Foundation
- GSM Association

Manufacturers of IoT devices capable of initiating or participating in emergency requests, and the associated vendors and service providers, need to keep their security practices up to date with current industry standards and recommendations.

2.13 Additional Workload Considerations

The additional workload potentially created by 9-1-1-capable IoT devices needs to be considered by the PSAPs when planning staffing levels and making personnel decisions.

2.13.1 PSAP Workload

IoT device/system and App input to the PSAP will likely increase the 9-1-1 call traffic and the handling time for calls. This increase may be significant for some types of information such as video. Additionally, IoT devices and Apps will likely necessitate alterations to the call handling workflow and may require specialized training and/or personnel. Some types of information conveyed by IoT devices and Apps may have great value after a dispatch is made but may not need to be considered prior to a dispatch. PSAPs may decide that some information such as supplemental video will not be made available by default to call takers. For example, some types of data may be more useful to responders than for dispatch, while other types of data may be more helpful for post-incident investigation/analysis. See Section 2.4.1 Impacts of Incident Data for more information.

2.13.2 Backroom Workload

The additional data received from IoT devices and Apps is likely to impact the work associated with the operation and maintenance of information systems, e.g., facilitating the

management of diverse inputs. Additional storage capacity may be needed to store received data, which may be required for evidentiary purposes and/or post-incident investigation/analysis. It is particularly important to ensure consistency of record management while considering the impact on the duties of PSAP personnel. It should be noted that, while IoT devices/systems and Apps may be capable of delivering a vast amount of data to the PSAPs, those responsible for managing that data flow into the PSAPs should prioritize data critical to an emergency response. Section 2.4.1 addresses PSAP policies with regard to additional data.

2.13.3 Administrative Effort

IoT device/system and App deployment situations are likely to vary widely, from consumer-targeted nationwide (or global) rollouts, to regional or localized site-specific deployments. To properly handle IoT devices, systems, and Apps deployed in commercial or public sector environments, coordination between the entities responsible for such deployments and local PSAPs may be necessary, which may include, for example, loading relevant site information into PSAP data systems and ensuring the accuracy thereof. Calls to 9-1-1 from IoT-based systems and Apps may require follow-up work by PSAP administrative personnel to work with IoT system and App owners/managers to correct information sent by the systems such as location, device, or other data.

2.14 Additional Impacts

IoT devices that can generate 9-1-1 calls present a 9-1-1 access capability that is not clearly addressed in current regulations, especially with regard to the requirements placed on communication protocols and system providers. In addition, the 9-1-1 community has little experience receiving and processing calls initiated from IoT devices. Discussions need to be initiated to clarify these requirements to accommodate IoT devices, including requirements for critical elements such as accurate location information and data importance assessments.

2.14.1 External Impacts

The information received from IoT devices is likely to be included in the processes that follow an emergency event. Systems processing IoT-initiated calls will need to support access to data by prosecutors, defense attorneys, investigators, and others who have a need to review events. The considerable variety of IoT and App information and the potential complexity of inputs from multiple devices may complicate, or simplify, the work of these individuals.

To aid this work, the incident data for the call, including sensor and location data, calling timestamps, identification of data sources and entities initiating the call, and other pertinent data from an IoT device must be recorded. Once recorded, the incident data

must be maintained for review, perhaps for a significant amount of time. Note that privacy requirements apply to incident data.

2.14.2 IoT/App Call Origination

It may be expedient for IoT developers to utilize the expertise of third-party emergency call centers to process calls to 9-1-1 and to take advantage of their existing interfaces and capabilities for processing calls to 9-1-1.

IoT developers are responsible for ensuring that any third-party emergency call centers processing their 9-1-1 calls do so correctly; calls must have proper location information conveyed via their SIP header and be sent toward the PSAP using an appropriate ESInet. IoT developers, whether using direct links to 9-1-1 or using third-party emergency call centers, must process calls in compliance with NENA i3 standards. Failure to do so will result in misdirected or undeliverable emergency calls.

IoT devices and third-party emergency call centers must not direct emergency calls to non-emergency lines of PSAPs. Non-emergency lines receive lower-priority call handling and are not capable of carrying the associated information that is crucial for emergency calls. Device or App calls to non-emergency lines have the potential to flood those lines, and could be perceived as part of a malicious attack on the PSAP.

2.14.3 Liability Considerations

As new devices, applications and market participants (e.g., application providers, consumer electronics manufacturers, private and public access networks, Internet Service Providers (ISPs), and third-party IoT cloud service providers, etc.) interact with the 9-1-1 system, the addition of IoT introduces new liability considerations.

Today, liability for 9-1-1 support among legacy telephone carriers, equipment providers, 9-1-1 agencies, 9-1-1 technology and service providers, and security alarm services is well established. For instance, service agreements between these entities and their customers address the responsibilities for each party regarding 9-1-1 use and related liabilities (including the limits of liability) for system failure or misuse. Many local jurisdictions have laws and regulations in place that address the use of monitored security alarm systems, including fees imposed on consumers and/or alarm companies for false alarms that result in unnecessarily dispatching first responders.

In order for market participants to support IoT devices and Apps for 9-1-1 and for consumers to adopt such technologies for this purpose, the following liability considerations should be considered.

2.14.3.1 Responsibilities to End Users

Suppliers of services, applications, and devices may be willing to accept limited liability for complying with specific published NENA i3 and IoT 9-1-1 standards, but might not be

willing to accept responsibility to end-users that guarantees connectivity to 9-1-1 or that 9-1-1 systems will be able to accept the calls from such services, devices, or applications.

2.14.3.2 Responsibilities among Interconnected Service, Application and Device Suppliers

As opposed to providing a passive pass-through pipe for broadband connectivity, facilities-based ISPs may become active participants that transport 9-1-1 calls from IoT applications and devices to 9-1-1 ESInets. Such active participation may include providing location and routing functions, 9-1-1 bandwidth prioritization, Quality of Service (QoS) and secured connectivity through dedicated VPNs from their private networks to ESInets. These ISPs may seek limited liability to other service, device, and application suppliers and to the 9-1-1 agencies to which they are connected. Likewise, application and device suppliers may be required to accept some liability for ensuring that their products do not introduce viruses or other attacks or experience malfunctions that could adversely impact the security or reliability of other devices, applications, or service providers in the network.

2.14.3.3 Responsibilities of End Users

Consumers may need to accept liability for misuse (deliberate or otherwise) of devices and applications, including human-caused false alarms. Such responsibility and liability may be incorporated in the terms and conditions consumers agree to with their ISPs and other service providers, or part of local ordinances.

3 Impacts, Considerations, Abbreviations, Terms, and Definitions

This document provides information and recommendations for the initiation and handling of emergency calls generated by IoT devices and device Apps. This document expands on the protocols, processes, and other aspects specified in NENA i3 (NENA-STA-010.3) [3]. It is intended in part to provide IoT device, system, and App developers and operational managers information and recommendations to ensure their calls are correctly initiated and handled by emergency services. This document also provides information and recommendations to emergency services authorities on calls generated by IoT devices and Apps, including both technical and operational guidance. This document also recommends that NENA as an organization undertake certain activities related to IoT devices and Apps.

3.1 Operations Impacts Summary

Deployment of IoT devices and emergency-related smart device applications carries significant and potentially unrecognized changes to the processes and protocols of PSAP call takers, responders, administrators, and other roles and entities.

3.2 Technical Impacts Summary

This is an informational document. As such, the recommendations made throughout this document may be considered as a guideline for considering and preparing for the impacts

of IoT devices and applications on 9-1-1 overall, and PSAPs in particular. When implemented, some of the recommendations within this document may have significant technical impacts.

3.3 Security Impacts Summary

As noted in Section 2.122, appropriate security measures are needed for IoT devices, Apps, the systems in which they are deployed, and all elements and functions within the emergency services system. It is crucial that 9-1-1 system providers, PSAPs, and authorities take into account the security issues associated with IoT devices and Apps as part of their network provisioning, protocols, and operating procedures.

3.4 Recommendation for Additional Development Work

Several areas, described below, require further work.

3.4.1 Assistance to implementers

It is appropriate for NENA to produce documents and related items that will assist IoT developers and implementers to understand and comply with the appropriate requirements.

3.4.2 Industry Liaison

It is appropriate for NENA to establish a working relationship with the industries developing and deploying IoT connectivity to assist in assuring that the industry as a whole understands the roles, procedures, and technology necessary to interface with 9-1-1 systems.

NENA should consider creating a working group or other structure aimed at encouraging developers to work in a non-competitive environment to share expertise on interfacing IoT devices/systems to 9-1-1 with specific emphasis on uniform data blocks, data definitions, and similar attributes in 9-1-1 data streams. The group objectives should be aimed at assuring that PSAPs can rely on consistency of similar data while permitting developers to implement systems with minimal delay caused by formal standards development. Another objective should be consistency and improvement of triggering thresholds for initiating an emergency call.

3.4.3 PSAP IoT/App Forum

In conjunction with the IoT developer working group or other structure, NENA should implement a process aimed at facilitating the sharing of information concerning IoT devices/systems and Apps with the PSAP community. The primary goals will be assisting developers and PSAPs in avoiding surprises and/or confusion when IoT and App 9-1-1 calls are received, assisting the PSAPs to effectively utilize the data blocks being transmitted, and assisting the PSAPs to understand the nature of the IoT device or App making the call

including the likely parameters that would cause a call to be initiated. In addition to providing consistency of 9-1-1 call management from the particular IoT system, such a process will provide developers an established method of expanding awareness of their IoT device/system without the burden of contacting each PSAP where the device/system or App is implemented, and a potential process for PSAP feedback concerning issues that may impact the effectiveness of the IoT device/system.

Public information efforts by the IoT system vendors, owners/managers, and PSAP administrators should be aimed at ensuring that initial implementations of systems with a 9-1-1 call capability are appropriately configured.

3.4.4 Data Definitions

IoT-generated 9-1-1 call information needs to be organized in standardized data blocks to permit uniform handling and appropriate processing within public safety systems. The utilization of standardized elements may also enhance information security.

As identified in Section 2.33, Additional Data blocks have not yet been specified for Additional Data associated with a Location, that is, the contents of the Additional Data blocks dereferenced via Additional Data URIs returned by an ECRF.

3.4.5 Information Criticality and Call Autonomy

A determination should be made regarding the advisability of implementing a new parameter (e.g., Information Criticality) that could be transmitted with the call that helps define the critical nature of the call or the information being transmitted. Additionally, as discussed in Section 2.11, consideration should be given to the desirability of implementing a new parameter indicating the degree of autonomy of the initiation of the 9-1-1 call.

For example, calls originating from a device without human action/confirmation might not have the same criticality as calls from a device initiated after human action/confirmation.

3.4.6 Internal Information Sharing

The development of IoT devices, systems, and Apps that interface with 9-1-1 may require new mechanisms for sharing information among PSAPs and the organizations that support 9-1-1 systems. It is important that information, experiences, and effective practices be shared among and between PSAPs and emergency authorities both regionally and nationwide regarding emerging Apps and devices. NENA, and others, should establish a method for information sharing specifically aimed at encouraging PSAP information sharing concerning IoT devices, systems, and Apps, and related PSAP operational procedures.

Sharing between PSAPs and emergency authorities, and dissemination of information concerning vendors or devices that may be compromised or pose a threat, such as device models, serial number ranges, software versions, etc. is needed. NENA should develop a

framework for such sharing and dissemination, including data formats and sharing mechanisms.

3.4.7 Regulatory and Legislative Concerns

NENA, APCO, NASNA, the Federal Communications Commission, and State Legislatures should actively pursue provisions that would include any IoT devices, systems, and Apps that have the capability to place a call to 9-1-1 in the fiscal support mechanism of the public 9-1-1 service(s). That support mechanism should include aggregating services such as third-party emergency call centers.

3.5 Anticipated Timeline

The Internet of Things (IoT) has been accelerating in recent years as sensing capabilities and communications systems become more capable at lower cost. Multiple wireless technologies provide explicit support for IoT devices (e.g., that may have lower power and processing capability), including 5G cellular networks. Advanced sensors and artificial intelligence capabilities allow IoT devices, systems, and Apps to analyze conditions and take actions, including initiating calls to 9-1-1 both with and without human intervention. See Section 2.11 for further discussion on human and autonomous initiation of such calls. This document may need revision as IoT devices, systems, and Apps mature and their impacts on 9-1-1 become more widespread and change.

3.6 Cost Factors

3.6.1 IoT Resource Demands

As referenced in sections 2.11 (Autonomous Versus Human Initiated/Mediated IoT/Apps Calls) and 2.13 (Additional Workload Considerations), the proliferation of IoT devices and applications accessing the 9-1-1 systems may considerably impact existing PSAP operations, technical and telecommunication systems. While the public safety benefits are desirable for supporting IoT applications with either direct access to 9-1-1 or through third-party call centers, the incremental costs to support these new technologies will need to be considered for all ecosystem participants. Such ecosystem participants include the 9-1-1 community from the Border Control Function of the ESInet to the PSAP terminal as well as potentially Internet Service Providers that deliver the last-mile broadband networks that provide connections, transport, routing, secure connectivity from their private networks and 9-1-1, quality of service/bandwidth prioritization, and potentially location information that link these various applications to 9-1-1. Potential ways to fund these additional resource demands are covered in section 3.7 (Cost Recovery Considerations).

3.7 Cost Recovery Considerations

3.7.1 Funding Models

The principal funding models for 9-1-1 services today are based on universal 9-1-1 fees collected by mobile and landline telephone carriers from their customers on a per-line basis per month. In some cases, additional funding for using 9-1-1 services is also assessed by local jurisdictions for supporting professionally monitored security systems (with third-party call centers) through one-time, annual and bi-annual alarm permit fees collected directly from consumers of those services or the security companies that provide those services.

In order to recover the incremental costs to support the new IoT devices and applications referenced in Section 3.6.1 (IoT Resource Demands), consideration should be given to legislative direction concerning how IoT devices are treated for purposes of inclusion in 9-1-1-specific fiscal support mechanisms. Such mechanisms would presumably be additive to and integrate with existing 9-1-1 funding models such as fees on regulated service.

3.7.1.1 Broadband Fees

One alternative is to assess a monthly non-discriminatory universal 9-1-1 fee on all consumer broadband service. This model is similar to how 9-1-1 fees are collected on mobile and landline telephone service. Internet Service Providers could bill customers for these fees as most already do in their telephone carrier business and remit those fees to the 9-1-1 authorities that collect 9-1-1 fees from the telephone carriers. Such fees were contemplated as part of The Internet Tax Nondiscrimination Act which includes a specific carve-out that permits states to assess 9-1-1 charges on broadband connections.⁴ A portion of these broadband-based fees could be used to reimburse the ISPs for active participation and compliance cost recovery purposes. This would be consistent with the cost reimbursement model associated with carriers and ISPs for compliance with law enforcement requests pursuant to the Communications Assistance for Law Enforcement Act (CALEA).⁵

3.7.1.2 Device and Application Provider Fees

There is a potential for PSAP management agencies to enter into agreements with service vendors such as security camera operators to collect fees where those IoT devices make calls to 9-1-1. This may be particularly true where complex IoT systems make a determination that a set of events creates a critical situation where public safety intervention is critical.

⁴ Internet Tax Nondiscrimination Act, Pub. L. 108-435 (codified as note to 47 U.S.C. § 151)

⁵ Title 18 U.S. Code § 2706

3.7.1.3 Monitored Alarm Security Systems Usage Model

Similar to the monitored alarm system model, 9-1-1 fees could be charged directly to just those consumers that use these IoT applications or third-party aggregators that provide gateway services between consumer applications and 9-1-1 systems. For example, as referenced in Section 2.14.3 (Liability Considerations), many local jurisdictions have laws and regulations in place that address the use of monitored security alarm systems, including fees imposed on consumers and/or alarm companies for false alarms that result in unnecessarily dispatching first responders. Some of these laws and regulations may potentially be extended to cover the use of IoT applications and devices that directly connect to 9-1-1 instead of through a central station alarm company.

3.7.1.4 Transactional Usage Fee Model

There also could be a usage-based transaction funding model whereby usage fees are collected directly from consumers for each 9-1-1 event triggered by the consumer's use of IoT applications and devices. For instance, during the device or application set-up process, the consumer may follow a step that registers the IoT application with the 9-1-1 services. Along with the technical registration process, the consumer may provide a credit card or third-party payment processing service account (e.g., PayPal) that would be billed a transaction fee each time the application accesses 9-1-1 (although this model may have drawbacks compared with an ongoing model, such as creating a disincentive for legitimate emergency calls, stale payment data, etc.).

3.8 Additional Impacts (non-cost related)

This NENA document identifies impacts of IoT devices and Apps on the emergency services system and discusses impacts on such devices and Apps, as well as the systems in which such devices and Apps are deployed, in order to operate with the emergency services system.

3.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1], for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

Term or Abbreviation (Expansion)	Definition / Description
<i>AACN (Advanced Automatic Crash Notification)</i>	<p>An emergency call placed by a vehicle, initiated either automatically or manually, conveying telematics data. Also called a “telematics call”.</p> <p>“Advanced” indicates that the call carries advanced telematics data such as information about a crash, rollover, fire, or other incident, the vehicle description and location, etc.</p> <p>Related Terms:</p> <p>NG-AACN (Next-Generation AACN) is an AACN call using NG9-1-1 and conveying the data in the call set-up, so the call can be identified as an AACN during routing and call handling, and the data may be available to call handling equipment and a call taker immediately.</p> <p>ACN (Automatic Crash Notification) as noted above lacks the advanced aspects.</p>
<i>App (Application)</i>	An application on a device such as a smartphone.
<i>DDoS (Distributed Denial of Service)</i>	A denial of service is a type of cyber-attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides. A distributed denial of service attack uses multiple devices distributed across different IP addresses to make it more difficult to detect or defend against.
<i>ECRF (Emergency Call Routing Function)</i>	A functional element in an ESInet which is a LoST protocol server in which location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP for the caller’s location or towards a responder agency.

Term or Abbreviation (Expansion)	Definition / Description
<i>EIDO (Emergency Incident Data Object)</i>	A JSON-based object that is used to share emergency incident information between and among authorized entities and systems. NENA has adopted the JSON-based EIDO (Emergency Incident Data Object) for sharing incident information among authorized NG9-1-1 entities and systems.
<i>GDPR (General Data Protection Regulation)</i>	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy.
<i>HIPAA (Health Insurance Portability and Accountability Act)</i>	The Health Insurance Portability and Accountability Act of 1996, regulations adopted pursuant to the Act, and specifically, the Security Rule describing protected information and safeguards for protection of electronic protected health information.
<i>IDX (Incident Data eXchange)</i>	A Functional Element that facilitates the exchange of Emergency Incident Data Objects (EIDOs) among other Functional Elements both within and external to an agency. (Previously called "IDE")
<i>IoT (Internet of Things)</i>	Devices capable of communication using Internet protocols.
<i>ISP (Internet Service Provider)</i>	An entity providing Internet access and service.
<i>LVF (Location Validation Function)</i>	A functional element in an NGCS that is a LoST protocol server where civic location information is validated against the authoritative GIS database information.
<i>PERS (Personal Emergency Response System) mPERS (mobile PERS)</i>	A device capable of initiating or requesting the initiation of a request for assistance such as an emergency call. A mobile PERS can be worn or carried by a person to provide service while mobile.
<i>PIDF-LO (Presence Information Data Format-Location Object)</i>	Provides a flexible and versatile means to represent location information in a SIP header field using an XML schema.
<i>PSAP (Public Safety Answering Point)</i>	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.
<i>Third-party emergency call center</i>	An organization, not operated by emergency authorities, that answers or initially receives 9-1-1 calls and forwards them to or toward the appropriate PSAP

4 Recommended Reading and References

- [1] National Emergency Number Association, *Master Glossary of 9-1-1 Terminology*. [NENA-ADM-000.22-2018](#). Arlington, VA: NENA, approved April 13, 2018.
- [2] National Emergency Number Association. *Emergency Incident Data Object (EIDO)*. NENA-STA-021.1-20xx. Arlington, VA: NENA (forthcoming).
- [3] National Emergency Number Association. *i3 Standard for Next Generation 9-1-1*. [NENA-STA-010.3-20xx](#). Arlington, VA: NENA (forthcoming).
- [4] National Emergency Number Association. *Policy Routing Rules Operations Guide*. [NENA-INF-011.2-2020](#). Arlington, VA: NENA, approved June 18, 2020.

5 Exhibit X

Not Applicable

6 Appendix X

Not Applicable

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Systems Security & Resiliency Committee, Impact of IoT Devices and Emergency Calling Applications Working Group, developed this document.

NENA Board of Directors Approval Date: 08/19/2020

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.
Randall Gellens, Working Group Co-Chair	Core Technology Consulting
Dwight Purtle, ENP Retired, Working Group Co-Chair	
Matt Besser, ENP	GeoComm, Inc.
Bob Connell, ENP	Zetron, Inc.
Jason Crutchlow, ENP	Greenville County, SC
Bob Finney III, ENP	Collier County, FL
Dianne Flanagan, ENP	Collier County, FL
Aaron Harris	Bandwidth
Rick Jezierny	Atos Public Safety
Ameel Kamboh	Atos Public Safety
Phongsak Keeratiwintakorn, ENP, CMCP	King Mongkut's University of Technology North Bangkok
Scott Luallin	Intelligent Systems Inc.
Patrick Malone, ENP	Comtech Telecommunications Corporation
Roger Marshall	Comtech Telecommunications Corporation
Christian Militeau, ENP	INTRADO, Inc.
Bob Oenning, ENP	
Nancy Pollock, ENP	Mission Critical Partners, LLC
Larry Reeder	Bandwidth
Phillip Rohrbough	Tarrant County 9-1-1 District, TX
Robert Sherry, ENP	
Charles Simon	Precision Broadband, LLC
Jay Slater, ENP	Bandwidth
Ihar Voitka	Self
Jeffrey Wheeler	Data Technical Services

Lena Wiggins, ENP, RPL	Alameda County Sheriff's Office, CA
------------------------	-------------------------------------

Special Acknowledgements:

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

The IOT/APPS 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, PSAP Operations Director