NENA
The 9-1-1 Association

4350 North Fairfax Drive | Suite 750 | Arlington, VA 22203-1695

Mr. Travis Hall
National Telecommunications and Information Administration
1401 Constitution Ave. N.W.
Washington, D.C. 20230

June 3rd, 2016

RE: **Late-Filed Comments**
Docket No. 160331306-6303-01
In re The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Dear Ms. Hall:

Please find attached joint comments of the National Emergency Number Association (NENA) and the National Association of State 9-1-1 Administrators (NASNA), submitted in response to the above-captioned *Notice and Request for Public Comment*. I am filing the comments out of time due to an oversight on my own part. I would ask that NTIA nevertheless consider them in full, without prejudice to NENA or NASNA.

Sincerely,

Telford E. Forgety, III, "Trey"
Director of Government Affairs

National Emergency Number Association | 800-332-3911 | 703-812-4600 | FAX 703-812-4675 | www.nena.org

Docket No. 160331306-6302-01

Before the United States Department of Commerce
National Telecommunications & Information Administration

In re
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

on notice and request for public comment

JOINT COMMENTS OF THE NATIONAL EMERGENCY NUMBER ASSOCIATION AND THE NATIONAL ASSOCIATION OF STATE 9-1-1 ADMINISTRATORS

Telford E. Forgety, III
Attorney
Director of Government Affairs

NENA: The 9-1-1 Association
1700 Diagonal Rd., Ste. 500
Alexandria, VA 22314
(202) 618-4392
(For the joint commenters)

CONTENTS

Before the United States Department of Commerce
National Telecommunications & Information Administration

Docket No. 160331306-6302-01

In re
The Benefits, Challenges, and
Potential Roles for the Government in
Fostering the Advancement of the Internet of Things

---

on notice and request for public comment

JOINT COMMENTS OF THE NATIONAL EMERGENCY NUMBER ASSOCIATION AND THE NATIONAL ASSOCIATION OF STATE 9-1-1 ADMINISTRATORS

The National Emergency Number Association ("NENA") and the National Association of State 9-1-1 Administrators ("NASNA") respectfully submit the following comments in response to the *Notice and Request for Public Comment* published by NTIA on April 1st, 2016.

COMMENTS

As the leading organizations representing the 9-1-1 profession in the United States, NASNA and NENA believe passionately in the ability of the Internet of Things ("IoT") to

transform emergency response for the better. However, today's emergency-response infrastructure remains largely unprepared to reap the panoply of benefits that the IoT can bring. To ensure that public safety professionals have the ability to rapidly, accurately, and efficiently respond in an emergency, NENA and NASNA encourage NTIA to look carefully at the infrastructure, standards development and research efforts that could be beneficial to both the public and private sectors as the IoT begins to impact 9-1-1.

I. The IoT will transform how public safety agencies operate.

Without question, the IoT will bring about fundamental changes in how public safety professionals handle emergency responses. Unique among public safety disciplines, 9-1-1 sits at the intersection of consumer, government, and responder communications. Consequently, our organizations believe that Public Safety Answering Points ("PSAPs" or "9-1-1 centers") stand both to reap great benefits – and face great challenges – from the IoT.

Already, the IoT has introduced consumers to powerful new capabilities with fascinating implications for public safety. Smart smoke detectors are now on the market that can make use of multiple sensing technologies to radically improve the accuracy of fire detection. Combined with networked thermostats, these devices can shut down ventilation blowers to limit the spread of fire and reduce the likelihood or severity of smoke inhalation injuries *before* field responders arrive on scene. Combined with networked electrical breakers that can de-energize circuits, these devices could also prevent consumer or firefighter electrocution injuries resulting from the use of conductive fire-fighting media such as water.

Beyond the implications of fixed IoT devices, NENA and NASNA foresee significant operational benefits from the IoT for both communications and field-response disciplines. Already, Orleans Parish, Louisiana is leveraging

the IoT to improve emergency response in the field.[1] Additionally, although unmanned aerial vehicles ("UAVs" or "drones") are not always considered part of the IoT, we expect this attitude to change over time. UAV navigation and collision avoidance technology is advancing at a stunning pace. Indeed, much of the technology required for an integrated "smart" IoT response is already available. With only a few years of further development, it seems likely that the following response scenario is possible:

At 3:27 a.m., a connected smoke detector in an Alexandria, VA apartment senses increased ionization and turbidity of the air. A warning tone sounds. At 3:28, Infrared ("IR") sensors in the apartment's connected lightbulbs register a large heat flare in the kitchen. Automated pattern analysis suggests a stove fire; the home's breaker panel interrupts the stove circuit, removing further heat input from the pot of soup, left on by accident, that has boiled dry and caught fire. Fire alarms begin to sound. By now, however, the kitchen cabinetry and ceiling are on fire.

At 3:29, the building's sensor network reaches its predetermined confidence threshold, and concludes that outside fire suppression assistance will be required. Evacuation alarms sound throughout the building, the involved apartment's sprinklers are activated, and the high-confidence fire indication triggers an automated machine-to-machine 9-1-1 call.

Within seconds, a 9-1-1 telecommunicator approves the AI-generated response plan. In phase 1, a small UAV is launched from the roof of a nearby fire house, selected on the basis of favorable winds that will help carry the drone to the scene more quickly. At 3:37, the drone arrives outside the apartment's window; its infrared sensors confirm the extent of involvement within the structure, and its terahertz camera detects two occupants still in the master bedroom. The UAV begins to orbit the building, looking for signs of spreading fire.

---

[1] Microsoft Corp., *Creating a safer city with IoT* (*available at*: https://goo.gl/V4ipkM).

Based on the drone data, PSAP systems automatically retrieve medical records for the likely victims, and dispatch EMS, copying the ambulance on relevant details. By 3:40, a ladder company has arrived on-scene, thanks to a routing algorithm that directed its driverless truck around a downed powerline, detected by automated switchgear. Within minutes, the fire is out, and both occupants, though alive, are removed from the building with serious smoke inhalation injuries. Once transferred to ambulances, the victims are transported to hospital while smart wristbands begin continuous monitoring of their vitals.

As the active fire scene begins to wind-down, responders receive a summarized report of the sensor data that triggered their response, and a detailed report is filed electronically with fire-science organizations for further analysis. Months later, the apartment's systems receive an over-the-air upgrade that improves the fire detection and response algorithms based on data from fires around the country. Later that year, a soup-pot boils dry again. This time, however, the patterns from the previous fires lead to a faster detection, higher confidence reporting, and a faster response. No injuries occur.

Currently, there are four major barriers to the scenario given above: First, public safety agencies lack the advanced, standards-based infrastructure, software, and hardware required to receive and process machine-to-machine 9-1-1 "calls." Second, data formats and exchange standards don't exist or are incomplete, and the community lacks an understanding of when algorithmic event detections should be considered sufficiently reliable to initiate an automated 9-1-1 call. Third, the nascent nature of the IoT market leaves open significant questions about the availability, confidentiality, and integrity of IoT systems that may soon have major roles in emergency response. Fourth, federal, state, local, territorial, and tribal laws and regulations may currently prohibit the use of desirable IoT capabilities, even where the available evidence suggests that those capabilities are accurate and reliable. The sections below address these barriers in turn.

II. Emergency response infrastructure must be updated to accommodate new sources and types of information.

The Enhanced 9-1-1 systems that exist throughout the majority of the United States today are products of the telephone age, not the computer age. Most 9-1-1 calls are still delivered over analog or Time-Division Multiplexed ("TDM") trunks, rather than IP-based networks. This severely limits the flexibility, reliability, and capabilities of PSAPs. For example, the overwhelming majority of 9-1-1 centers are still unable to accept text messages, a technology that has been in common use for nearly two decades. These limited capabilities will not suffice in the connected-device era.

In order to accept the robust, extensible communications media and data that consumers now use routinely, 9-1-1 systems must upgrade to "Next Generation 9-1-1." This native-IP platform leverages open standards, developed by the internet community, to lower the burdens associated with providing 9-1-1 service to consumers. Instead of limiting 9-1-1 service to integrated Access Network / Originating Service providers, this new approach clears the way for platform-independent applications and devices to become part of a new 9-1-1 ecosystem. Around the country, 9-1-1 system administrators and local governments are at the forefront the NG9-1-1 transition. Yet, in many cases, these emergency service pioneers lack access to critical inputs needed to complete that transition. For example, access to multiple, independent broadband data services – required for resiliency and redundancy in safety-of-life systems – limits the ability of local governments to even begin the NG9-1-1 transition. Even where multiple broadband providers are available, the hardware, software, and security services required to safely operate an NG9-1-1 system may not be available or affordable, since legacy E9-1-1 systems must be maintained until the transition is complete.

As federal departments and agencies, states, tribes, territories and localities work to implement NG9-1-1, a national focus on infrastructure availability will be necessary

to ensure that 9-1-1 centers can leverage the benefits of the IoT. Otherwise, local first response systems could face a destructive fragmentation. Already, some poorly-informed application providers have introduced dangerous software products in the market which falsely purport to enrich or replace 9-1-1 or other public safety services. These applications can give consumers a false sense of security that could be deadly in a time of emergency. Were similar developments to take hold in the IoT hardware community, serious and persistent threats to public safety, public safety communications systems, and information security could arise.

NENA and NASNA believe it is imperative that the NG9-1-1 transition proceed quickly. If it does, IoT developers will have powerful incentives to work *with* public safety to transform emergency services for the better. If not, misguided developers may choose instead to work *around* public safety, leading to headaches for PSAPs and field responders, and life-threatening situations for consumers. Moreover, without the platform efficiencies provided by NG9-1-1 availability, the U.S. economy could miss-out on both increased profits derived from novel products and services, and from the decreased costs associated with improved emergency responses: Lives saved and property preserved are important measures of economic impact from public safety services. Consequently, NASNA and NENA urge the Government to facilitate the deployment of NG9-1-1 infrastructure, so that all of these benefits can be sooner recognized.

III. The United States Government should support research and standards development efforts for public safety applications of IoT data.

In addition to infrastructure, hardware, and software, the integration of IoT devices and applications into the U.S. and international emergency response frameworks will require significant investments in data models and analytics-based research. For example, in the future scenario given above, analysis of sensor data from a structure fire led to improvements in future sense-and-react responses. This

kind of rapid-cycle improvement is enabled by standardized data formats and analytic frameworks. In order to ensure that *all* public safety disciplines are able to make such improvements, NENA and NASNA recommend that the U.S. Government engage with a wide array of stakeholders in the emergency response, data analytics, and sensor communities to begin determining what kinds of data would help to improve responses, and how that data would need to be analyzed. This baseline data needs analysis could then feed into government-backed research projects aimed at establishing automatic analysis and improvement frameworks.

Frameworks, in the IoT context, are particularly important to public safety. Without such enabling "middleware," safety-critical data from individual sensor systems and networks could end up "stove-piped." To be most useful, each system's data should be susceptible to correlation with data from other systems. Frameworks make this possible. In the 9-1-1 community, for example, some early analytics work has been done to correlate call locations with network routing decisions and response types. This has led to improved call delivery times and better pre-positioning of scarce public safety resources such as ambulances. Breaking down stovepipes among PSAP systems to arrive at the insights that made this possible, however, was a difficult and complicated task. In many cases, analytics providers resorted to taking data from old-fashioned printer ports, parsing it, structuring it, and time-correlating it before even storing it in a relational database. That process is cumbersome, error-prone, and expensive. The future need not be.

NTIA, NIST, and the NIST ITS are uniquely positioned to develop (or facilitate the development of) critical public safety frameworks for the police, fire, EMS, and 9-1-1 communities. NASNA and NENA therefore recommend that the Department consider undertaking this crucial work *before* fragmentation in the IoT space threatens its utility to public safety.

IV. NIST should investigate the security implications arising from public safety use of IoT devices and data.

As with any new networked technology, IoT devices and systems expose new vulnerabilities that could be exploited for malice or profit. In the public safety space, particularly, the consequences of a security exploit could be considerable. Returning to our apartment fire scenario, an attacker capable of penetrating the apartment's network could gain access to devices with the potential to complicate emergency response or exacerbate the fire threat. Imagine, for example, an attacker wanted to make a fire worse. She might, for example, disable audible and visual warning devices in smoke detectors, set ventilation blowers to their maximum speed to fan the flames, disable sprinkler pumps to keep a fire alive, and override smart locks to prevent victims from escaping. None of this is far-fetched.

Beyond the safety implications for consumers, security considerations have a material bearing on emergency response agencies. Ensuring the availability, integrity, and confidentiality of machine-to-machine alerts, responder data, and real-time communications must be regarded as a safety-of-life issues. Because our first- and field-response agencies will increasingly rely on IoT systems like UAVs, driverless trucks, Search and Rescue robots, etc., it is imperative that the public safety community have access to the tools, systems, and training that are necessary to ensure the security of those systems. Today, many do not.

NENA recently conducted an on-site survey of the security of one relatively sophisticated PSAP. During the course of a NIST Cybersecurity Framework evaluation, vulnerability scan, and phishing campaign, NENA discovered potentially serious vulnerabilities. For example, we found that no internal network security practices were in place: Virtually all security measures were confined to border filtering and passwords and application-layer passwords. Based on discussions with other PSAPs, we are concerned that this may be the norm. In order to ensure that PSAPs can implement adequate baseline security

measures, NENA and NASNA believe that a concerted campaign of education, training, and awareness building will be required. Additionally, simplified machine and network management tools will need to be developed and made available to public safety agencies to facilitate the adoption of the often complex technologies and practices required to secure modern networks. Moreover, workforce development efforts will be required to ensure that PSAPs and other emergency response agencies have access to knowledgeable, skilled technicians able to implement critical security controls.

V. The joint NTIA/USDoT National 9-1-1 Office should compile data on state and local regulations that may delay or prohibit the incorporation of IoT devices and data into public safety responses.

At the policy level, NASNA and NENA are concerned that existing laws and regulations are not being updated fast enough to keep pace with changes in IoT technology. In the past, for example, most jurisdictions understandably prohibited the automated transmission of most alarms to 9-1-1 centers. This occurred because the majority of alarm systems were (and still are) quite limited in processing capabilities. Without algorithmic logic aimed at separating false alarms from real, or integrating the output of multiple sensors to produce a confidence evaluation, most alarm systems could handle only one bit of data: closed or open. If a circuit that was normally in one state suddenly changed to the other, an alarm was generated. Obviously, this generated many false alarms, leading to the sometimes voluminous regulations facing alarm manufacturers and central station operators. Today, however, those limitations are no more. Alarms and other advanced devices on or nearing the market can fuse sensor data to develop a nuanced, statistical view of whether an alert is warranted, and can provide intelligent means for consumers to "wave off" a proposed alert, if it's deemed insufficient by a human to warrant a 9-1-1 "call."

Similarly, legacy telecommunications regulations often take a narrow view of who can and cannot be a provider of 9-1-1 services to consumers or to PSAPs. Today's competitive, innovation-driven application and device markets look little like the unitary markets those regulations were designed to control. Regulations like these could stand in the way of IoT adoption, both by consumers and public safety.

NENA and NASNA take no position here with respect to what laws and regulations concerning IoT alerts and confidence levels *should be*. Rather, we encourage the National 9-1-1 Office to compile a listing of what current laws and regulations *are*. Having such a compilation available will help the 9-1-1 community to engage with stakeholders from every relevant ecosystem, from sensors and alarms to mechanical and HVAC vendors, to begin a conversation about how we can – quickly – update our laws and regulations for the new capabilities of the IoT age.

CONCLUSION

NASNA and NENA look forward to engaging with NTIA and the broader government to help facilitate the incorporation of the Internet of Things into our nation's emergency response systems and our economy.

TELFORD E. FORGETY, III
NENA

EVELYN BAILEY
NASNA

JUNE 2016