Catholic University Journal of Law and Technology

Volume 27 | Issue 1 Article 6

2018

NG9-1-1, Cybersecurity, and Contributions to the Model Framework for a Secure National Infrastructure

Andrew Jackson Coley

NG9-1-1, CYBERSECURITY, AND CONTRIBUTIONS TO THE MODEL FRAMEWORK FOR A SECURE NATIONAL INFRASTRUCTURE

Andrew Jackson Coley[*]

The critical communications infrastructure in the United States is now outdated and inefficient, and therefore vulnerable to network crashes and cyber-attacks. The failure to allocate resources efficiently arises from 9-1-1, the public's primary connection to emergency services in the United States.[1] This lapse in policy has recently garnered attention, bringing forth a new generation of communications networks, which may be the saving grace of our emergency communications infrastructure.[2] This advancement is Next Generation 9-1-1 (NG9-1-1). NG9-1-1 is a substantial upgrade to today's standard 9-1-1 system's "hardware, software, data and operational policies and procedures," and will improve data and call routing capabilities, integrate call data for use by emergency responders, provide secure call networks, and deliver calls to the appropriate Public Safety Answering Points (PSAPs), among other enhanced capabilities.[3]

However, 9-1-1 networks across the United States will be advanced only

[*] Andrew Jackson Coley is a third-year law student at the Catholic University of America, Columbus School of Law, and completed his undergraduate degree in Political Science at Quinnipiac University. Andrew's primary academic interest is the laws response to rapid advancements in technology, particularly in regard to military affairs and national security. The author offers his thanks to Brian Fontes, his mentor on the topic, who was instrumental in this piece.

1 *9-1-1 Origin & History*, NENA, https://www.nena.org/page/911overviewfacts (last visited Nov. 1, 2018).

2 *See Health of the US 9-1-1 System*, 9-1-1 INDUSTRY ALLIANCE, https://www.theindustrycouncil.org/9IA_Health_of_US_911%20_2_.pdf. (last visited Nov. 1, 2018).

3 *What is NG9-1-1?*, NENA, https://cdn.ymaws.com/www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf (last visited Nov. 1, 2018).

through policy and legislation that focuses on recognizing security as an integral part of a network.[4] If successfully implemented, NG9-1-1 may serve as a template for implementing secure, reliable, and resilient communications networks within both the public and private industry.[5] As the next iteration of advanced public safety communications networks, NG9-1-1 is an ideal representation of advanced IP-enabled infrastructure with security measures naturally integrated into the system.

In November 2017, Congress proposed legislation to advance the rollout of NG9-1-1 systems.[6] The proposed legislation is bringing much needed attention to the underfunded emergency call network. It is also representative of a significant issue facing 9-1-1 call networks throughout the country, which is the inability to update Public Safety Answering Points (PSAP), the local location where your 9-1-1 call is answered, without federal funding and resources.[7]

Across the United States, PSAPs are operating at regional and local levels, and the results are significantly varied.[8] Although there have been improvements in PSAP's throughout the country with many states and localities pushing hard to update their systems to next generation technology, as former FCC Chairman Wheeler stated in his testimony before Congress, "these islands of progress are the exception, not the rule."[9] Many PSAPs face significant funding and operational challenges, resulting in out-of-date capabilities equivalent to the functionality of over thirty years ago.[10] 9-1-1 networks, by nature, are state run or local programs.[11] The NG9-1-1 proposed legislation presents an opportunity

---

4 Next Generation 9-1-1 Act of 2017, S. 2061, 115th Cong. (2017); Jane Edwards, *GAO: NHTSA Needs to Establish National 911 Program Performance Goals to Back NG911 Implementation*, EXEC. GOV. (Feb. 26, 2018), https://www.executivegov.com/2018/02/gao-nhtsa-needs-to-establish-national-911-program-performance-goals-to-back-ng911-implementation/; Christine Kenneally, *How to Fix 911*, TIME (Apr. 17, 2011), http://content.time.com/time/magazine/article/0,9171,2062452,00.html.

5 *See Next Generation 9-1-1 Transition Policy Implementation Handbook*, NENA (June 2011), https://www.911.gov/pdf/NENA_NG911_Transition_Policy_Handbook_2010.pdf.

6 *Id.; Staff Discussion Draft- Next Generation 91-1- Act of 2017*, NENA, https://c.ymcdn.com/sites/www.nena.org/resource/resmgr/govaffairs/Overview_—_Draft_Next_Gener.pdf (last visited Nov. 1, 2018).

7 *See* David Raths, *The NG911 Funding Gap*, GOV'T TECH. (Aug. 2, 2016), http://www.govtech.com/em/next-gen-911/The-NG911-Funding-Gap.html.

8 *Health of the US 9-1-1 System*, *supra* note 2.

9 *Oversight of the Federal Communications Commission: Hearing Before the S. Comm. On Commc'n and Tech.*, 114th Cong. 2 (2016) (statement of Tom Wheeler, Chairman, Fed. Commc'n Comm.) [hereinafter *Hearings*].

10 Raths, *supra* note 7.

11 Andrew Hartsig, *Calling 911: Funding and Technological Challenges of County 911 Centers*, NACO, https://www.naco.org/resources/calling-911-funding-and-technological-challenges-county-911-call-centers. (last visited Nov. 1, 2018).

for Congress to create legislation providing federal support to PSAPs while still maintaining the localized nature of 9-1-1 operating systems.[12] While the operation of the current 9-1-1 model is effective at a local level, a lack of federal support enables the continued use of outdated technology in many PSAPs across the country.[13] Further, without federal support, PSAPs will implement next generation technology in vastly different proportions dependent upon locally available funding.[14] The scale of cyber vulnerabilities that IP-enabled call networks present, and the discrepancies and disproportionate capabilities between PSAPs create an imminent security threat to 9-1-1 call networks.[15] Moreover, the NG9-1-1 initiative shows migration to more efficient and sophisticated IP-enabled tech systems. As 9-1-1 networks transition to more security-centric systems, it will be beneficial to enact legislation and create policies that ensure nationwide infrastructure is duly updated and improved.

This Comment will evaluate prevalent security concerns that the transition from current 9-1-1 network technologies to the next generation of IP enabled 9-1-1 call networks will highlight. This Comment will also analyze both local and federal risk mitigation options, as well as applicability to the broader critical infrastructure security within the United States. First, this Comment will look to the history of 9-1-1 call networks, why they require an upgrade, and the advantages of NG9-1-1 and advanced IP-based emergency call networks. Second, while there are advantages to IP-based call networks, there are also risks and vulnerabilities. This Comment will explore these risks by examining commercial and private sector cyber breaches that exposed the vulnerabilities of big data and IP-based networks, and the similar vulnerabilities present in NG9-1-1. Third, with an understanding of the risks and benefits of IP networks, we apply those risks to 9-1-1 networks, and explore the advantages and mitigation options brought by these networks. Due to the local nature of PSAPs and 9-1-1 call networks and the national scale of the problem, we look to other federal programs operating on similar scales, as well as fundamental cybersecurity hygiene practices that may aid in reducing risk to NG9-1-1 networks. Lastly, this Comment will examine how increased federal involvement in 9-1-1, but not necessarily a federalization of the system, can create a more secure emergency call network. A look at proposed federal legislation and ongoing grant programs

---

12 Chris Nussman, *NENA Applauds Introduction of NG9-1-1 Legislation*, NENA (Nov. 3, 2017), https://www.nena.org/news/372953/NENA-Applauds-Introduction-of-NG9-1-1-Legislation.htm.

13 *See* Raths, *supra* note 7; *see also* Collin Wood, *Next-gen 911 Matching Grant Rules Open for Comment*, ST. SCOOP (Sept. 22, 2017), https://statescoop.com/rules-to-issue-next-gen-911-matching-grants-open-for-comment.

14 *See* 911.GOV, *911 Grant Program*, NAT'L 911 PROGRAM ADMINISTERED GRANTS, https://www.911.gov/project_911grantprogram.html (last visited Nov. 26, 2018).

15 Raths, *supra* note 7.

reveals an acknowledgement by legislators and the executive branch alike of the need for increased support for NG9-1-1.

As society increasingly relies upon IP-based networks for incredible advancements in technology, new threats and vulnerabilities emerge that must be recognized and swiftly resolved.[16] NG9-1-1 presents an opportunity to plan for some of the greatest threats to society in the 21st century with a security first perspective.[17] Although experts within the public safety communications industry have provided research and recommendations to increase the security of PSAPs and NG9-1-1 networks, it is vital that enhanced cyber security of PSAPs are implemented in a manner that is practicable.[18] The nature of PSAPs, and their varying capabilities and resources, makes the challenge of securing seamlessly integrated PSAPs in the future all the more difficult. However, the 9-1-1 PSAP rollout reflects global advancements to IP-based systems with seamless integration, and the best way to approach this migration of technology is with a focus on security.

I. THE CURRENT STATE OF 9-1-1

The one phone number that nearly every American can recognize is 9-1-1.[19] According to the National Emergency Number Association, approximately "96% of the U.S. is covered by some type of 9-1-1 service."[20] The number of 9-1-1 calls per year is approximately 240 million, and over 80 percent of those calls are placed wirelessly.[21] The advanced capabilities of "smartphones" permits virtual interactions that are significantly more advanced than the basic 9-1-1 networks are capable of supporting.[22] The Minnesota Department of Public Safety states that: "a new generation of access devices presents a technology challenge to systems originally designed to provide only fixed

---

16 *Cyber Risks to Next Generation 9-1-1*, NAT'L 911 PROGRAM ADMINISTERED GRANTS, https://www.911.gov/pdf/OEC_NG911_Cybersecurity_Primer_May_2018.pdf (last visited Nov. 26, 2018).

17 *See Future of 9-1-1 Issue Brief*, CENTURYLINK, http://www.centurylink.com/asset/business/enterprise/issue-brief/gbc-centurylink-n911-issue-brief-cm160716.pdf (last visited Nov. 26, 2018).

18 Mike Beagles, *BUILD A SMART PSAP CYBER SECURITY STRATEGY: 8 CRITICAL "MUST-HAVES,"* MISSIONCRITICALPARTNERS (Sept. 5, 2017, 4:00 PM), http://blog.mcp911.com/insights/psapcybersecuritymusthaves.

19 *See 9-1-1 Origin and History*, *supra* note 1.

20 *Id*.

21 *9-1-1 Statistics*, NENA (Dec. 2017), https://www.nena.org/page/911Statistics.

22 *See 9-1-1 Origin and History*, *supra* note 1; *Next Generation 9-1-1 Transition Policy Implementation Handbook*, *supra* note 5.

landline 911 calls."[23] Basic 9-1-1 systems experience difficulty in supporting "text messages for emergencies, images and video (including support for American Sign Language users), and easy access to additional data such as telematics data, building plans and medical information over a common data network."[24] The National Emergency Number Association (NENA), has pointed out that increased "inter-communications across states, between states, and across international boundaries requires that we create a more flexible 9-1-1 system design with much greater data handling capabilities."[25] As such, 9-1-1 systems throughout the country are due for an upgrade to prevailing technical standards.[26] Responders should reap the benefits of the litany of advancements in wireless technology, such as the useful integration of data and standardized interface surfaces for calls and messaging, because it will be standard in NG9-1-1 systems.[27]

II. WHAT IS NEXT GENERATION 9-1-1?

The transition from basic 9-1-1 networks to NG9-1-1 networks is, at its core, a transition from analog to digital networks.[28] The New and Emerging Technologies 9-1-1 Act of 2008 summarized NG911 as "a national IP-enabled emergency network capable of receiving and responding to all citizen-activated emergency communications and improving information sharing among all emergency response entities."[29] Accordingly, the Next Generation systems will be able to receive all the data, text, and video capabilities that expand with modern smartphone technology.[30] These upgraded networks, called Emergency Services Internet Protocol Networks (ESINets), provide PSAP's the ability to

---

23 *NEXTGEN 911*, MINN. DEP'T OF PUB. SAFETY, https://dps.mn.gov/divisions/ecn/programs/911/Pages/nextgen-911.aspx (last visited Nov. 1, 2018).

24 *What is NG9-1-1?*, *supra* note 3.

25 *Id.*

26 Senators Nelson & Klobuchar, STAFF DISCUSSION DRAFT—NEXT GENERATION 9-1-1 ACT OF 2017, http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/govaffairs/Overview_—_Draft_Next_Gener.pdf (last visited Nov. 1, 2018).

27 *9-1-1 Origin and History*, *supra* note 1; NAT'L 9-1-1 PROGRAM 2017 NATIONAL 911 PROGRESS REPORT (Nov. 2017), https://www.911.gov/pdf/National-911-Program-Profile-Database-Progress-Report-2017.pdf; *see also What is NG9-1-1?*, *supra* note 3.

28 *Next Generation 911*, *supra* note 5.

29 New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, 122 Stat. 2620 (2008).

30 *See* Fed. Comm. Commc'n, 47 Fed. Reg. 78, 1799 (Jan. 9, 2013) (to be codified at C.F.R. pt. 20) (discussing how Next Generation 9-1-1 technology will support text messaging and other forms of data transmission); *1 NEXT GENERATION 9-1-1: THE ESSENTIAL GUIDE TO GETTING STARTED*, WEST CORP. (2013), http://www.intrado.com/sites/default/files/documents/NextGen%209-11%20The%20Essential%20Guide%20to%20Getting%20Started.pdf; *Next Generation 9-1-1*, *supra* note 5; *What is NG9-1-1*?, *supra* note 3.

transmit larger and more significant amounts of information to police, EMS, firefighters, and other emergency service personnel that PSAPs dispatch.[31] ESINet's are "designed with a high level of redundancy and resiliency to ensure that the network can continue to operate and deliver 911 calls even if some of the circuits or end points are no longer functioning."[32] Notoriously, natural disasters disable the outdated PSAP's basic 9-1-1 system, however, the 9-1-1 systems of the future will function during these dire times.[33] In addition, the consumers, people calling 9-1-1 in an emergency, will have the capability of transmitting more useful information, such as real-time text messages, videos, images, pertinent medical information and more to emergency responders.[34] As a result, data which was previously unusable by most 9-1-1 systems will provide advanced capabilities to first responders in jurisdictions with NG9-1-1 systems.[35] For example, NG9-1-1 networks allow for accurate location information through data transmitted based on the location of the 9-1-1 caller.[36]

One of the significant aspects of NG9-1-1 will be the "seamless interoperability" of the emergency network.[37] "Seamless interoperability," as explained by the Association of Public Safety Communications (APCO), means PSAPs are able to "dynamically share resources and reroute calls, which is particularly valuable during high call volume periods and major disasters affecting PSAP operations." This ability to share resources and reroute calls "should be possible regardless of what call handling equipment, computer aided dispatch, or connecting networks . . . the PSAPs have deployed."[38] The president of APCO states that "seamless interoperability will improve emergency response operations and expand the market so that public safety benefits from the competition and innovation enjoyed in the commercial sector."[39]

---

31 Jeff Lupinacci, *ESInets are a Game Changer for Public Safety and the First Step to Next-Gen 911*, GOV'T TECH. (May 6, 2015), http://www.govtech.com/em/next-gen-911/ESInets-Are-a-Game-Changer-for-Public-Safety.html; *Next Generation 9-1-1*, *supra* note 5.

32 Lupinacci, *supra* note 31.

33 *See* Nussman, *supra* note 12 (discussing a legislative call for next generation 9-1-1 technology during a natural disaster).

34 DEP'T OF PUB. TRANSP., NEXT GENERATION 9-1-1 (2018), https://www.its.dot.gov/factsheets/pdf/JPO_NextGen911_v2.pdf.

35 *NG9-1-1 Project*, NENA, https://www.nena.org/page/NG911_Project (last visited Sept. 21, 2018).

36 FED. COMMC'N COMM'N, INQUIRY CONCERNING 911 ACCESS, ROUTING, AND LOCATION IN ENTERPRISE COMMUNICATIONS SYSTEMS, PS Docket No. 17-239 (Sept. 7, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-346580A1.pdf.

37 Martha Carter, *Achieving Fully Interoperable NG9-1-1*, ASS'N OF PUB. SAFETY COMMC'N (Feb. 1, 2018), https://www.apcointl.org/achieving-fully-interoperable-ng911/.

38 *Id.*

39 *Achieving the True Promise of NG9-1-1*, ASS'N OF PUB. SAFETY COMMC'N (June 12,

Such interoperability will be particularly useful in a 9-1-1 outage, when the public is unable to reach 9-1-1 call centers.[40] In 2017, AT&T experienced a nationwide 9-1-1 call failure, where 9-1-1 callers reported either a busy signal or continuous ringing.[41] This particular failure affected the United States on a massive scale, affecting 18 states and the District of Columbia.[42] The system failure was a result of AT&T's failure to follow "certain best practices outlined by the FCC's [(Federal Communications Commission)] Communications Security, Reliability and Interoperability Council".[43] However, a fully integrated NG9-1-1 network should be able to avoid an operational failure at such a large scale due to the resiliency and interconnectedness of NG9-1-1 networks.[44] Ideally, during a system failure, NG9-1-1 networks may transfer calls from one PSAP to another without the technical difficulty of outdated 9-1-1 systems, which relied upon specialized switches as opposed to IP-based networks.[45] Basic 9-1-1 networks simply do not possess the dynamic technology required to ensure that reliable public safety communications remain available to the public during a third-party network outage.[46] The systems of NG9-1-1, based on IP networks, will possess the ability to transfer calls quickly and efficiently and have calls redirected to operational PSAPs in the event other PSAPs experience failures

---

2017), https://www.apcointl.org/tabletopx/achieving-the-true-promise-of-next-generation-9-1-1.

40 Adrienne Lafrance, *The 9-1-1 Paradox*, THE ATLANTIC (Mar. 10, 2017), https://www.theatlantic.com/technology/archive/2017/03/the-9-1-1-paradox/519192/; Amanda Jackson, *FCC investigating AT&T 911 outage*, CNN (Mar. 8, 2017), https://www.cnn.com/2017/03/08/us/att-911-outages-trnd/index.html; *see also The Network*, FIRSTNET, https://www.firstnet.gov/network (last visited Sept. 22, 2018) (explaining that FirstNet is a nationally designed network created to serve as a public safety communications network with standards matching the commercial minimum standard, where seamless interoperability refers to a PSAP's ability to transfer calls and aid other PSAP's exchange of data between connecting networks (ESInets) across jurisdictions, and the seamless exchange of data between ESInets and public information systems, as well as between NG9-1-1 and FirstNet).

41 Lafrance, *supra* note 40; Jackson, *supra* note 40.

42 *Id*.

43 Colin Gibbs, *AT&T's 911 Outage 'Result of Mistakes Made by AT&T,' FCC's Pai says*, FIERCE WIRELESS (May 18, 2017), https://www.fiercewireless.com/wireless/at-t-s-911-outage-result-mistakes-made-by-at-t-fcc-s-pai-says; FCC's Public Safety and Homeland Security Bureau Reminds Communications Service Providers of Importance of Implementing Network Reliability Best Practices, 17 FED. REG. 672 (Proposed July 12, 2017) (to be codified at 47 CFR §§ 0.191, 0.392), https://docs.fcc.gov/public/attachments/DA-17-672A1.pdf.

44 *Achieving the True Promise of Next Generation 9-1-1*, *supra* note 39; *White Paper: NG9-1-1 Changes Everything: Will you Lead, Follow, or be Left Behind?*, MOTOROLA (2012), https://www.motorolasolutions.com/content/dam/msi/docs/business/global_services_new/_documents/_staticfiles/ng9-1-1_white_paper.pdf.

45 *White Paper: NG9-1-1 Changes Everything*, *supra* note 44.

46 *Id*.

within their systems. [47]

NG9-1-1 will provide a significant number of benefits to public safety.[48] With advanced systems, emergency responders will be capable of responding to emergencies with significantly more information than previously available.[49] With assistance from the federal government in universal implementation of NG9-1-1, the benefits of IP-based communications networks will be more far reaching than any previously operated public safety system.[50] NG9-1-1 will provide vast improvements to the public safety arena, which is in vital need of updates.[51] However, the benefits of NG9-1-1 are dependent upon the successful collection and processing of a significant amount of data.[52] As such, NG9-1-1 will be subject to the same risks as other "big data" collectors, including major data breaches affecting the public at large.[53] Moreover, given the high stakes of emergency preparedness and response, the consequences of a failure to recognize the risks of an IP-based emergency network will likely have greater consequences than the private sector.[54] The first step in preparation is to review the history of major data breaches with a security centric perspective in order to avoid mistakes of the past.[55]

A. Big Data and Privacy Concerns

"Big data" refers to the collection and use of massive amounts of data sets to form relationships.[56] In the context of 9-1-1, collection of 9-1-1 caller data produces a rich amount of information, providing first responders with critical

---

47 *Id*.

48 *White Paper: A Next Generation 911 Cost Study A Basis for Public Funding Essential to Bringing a Nationwide Next Generation 911 Network to America's Communication User and First Responders*, FCC (Sept. 2011), https://docs.fcc.gov/public/attachments/DOC-309744A1.pdf.

49 *White Paper: NG9-1-1 Changes Everything*, *supra* note 44.

50 115th Cong., 1st Session (Nov. 2017); JILL C. GALLAGHER, CONG. RESEARCH SERV., R45253, NEXT GENERATION 911 TECHNOLOGIES: SELECT ISSUES FOR CONGRESS 1 (2018).

51 *Hearing on S. Hrg. 112-576 Before the Subcomm. on the Comm., Tech., and the Internet of the Committee on Commerce, Science, and Transp.*, 113th Cong., 32-33, (June 5, 2014).

52 *Whitepaper: NG9-1-1 Changes Everything*, *supra* note 44.

53 F.C.C. STRATEGIC PLAN FOR STATEWIDE 9-1-1 SERVICE FOR FY 2015-2019 (July 2014), https://transition.fcc.gov/pshs/911/Net%20911/7th-Report/Texas_StrategicPlan_15-19.pdf.

54 JOINT ADVISORY COMMITTEE ON COMM. CAPABILITIES OF EMERGENCY MED. AND PUB. HEALTH CARE FACILITIES: REPORT TO CONG. 11-12 (Feb. 4, 2008), https://www.ems.gov/pdf/FCC-JAC-Report.pdf.

55 *See generally White Paper: NG9-1-1 Changes Everything*, *supra* note 44.

56 *Big Data and the Future of Privacy*, EPIC, https://epic.org/privacy/big-data/ (last visited Nov. 26, 2018).

information in emergency responses.[57] Big data has endless applications. For example, big data collection methods form the basis for the most successful companies of the 21st century.[58] Google and Facebook collect massive quantities of data about their users, and later sell that data for profit.[59] Such uses of big data are beneficial to society and largely contribute to economic growth.[60] However, there are significant privacy and security concerns related to the collection of big data, in particular when network security flaws lead to the hacking and stealing of inconceivable amounts of data.[61]

The most recent notable massive data breach and exposure of significant quantities of data was the Equifax security breach of 2017.[62] The private information of 143 million Americans was accessed and exposed through this credit reporting agency breach.[63] The hackers were able to access credit card numbers and documents containing personal information for over 200,000 people throughout the United States, UK, and Canada.[64]

Such a breach leaves anyone involved vulnerable, exposing the most private

---

57 *See generally id.*; Rebecca Jeschke, *A Privacy Emergency: Consumer Rights at Risk in Next Generation 911*, ELEC. FRONTIER FOUND. (Mar. 14, 2011), https://www.eff.org/deeplinks/2011/03/privacy-emergency-consumer-rights-risk-next; Notice of Request, 79 Fed. Reg 12251 (Mar. 4, 2014).

58 *See, e.g.*, Avantika Monnappa, *How Facebook is Using Big Data - The Good, the Bad, and the Ugly*, SIMPLILEARN (Nov. 3, 2017), https://www.simplilearn.com/how-facebook-is-using-big-data-article.

59 *Id.*; Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/.

60 *FACT SHEET: PCAST Report on Big Data and Privacy: A Technological Perspective*, WHITE HOUSE (May 14, 2014), https://obamawhitehouse.archives.gov/the-press-office/2015/11/16/fact-sheet-pcast-report-big-data-and-privacy-technological-perspective; Josh Green, *Big Data: The Key to Economic Development?*, WIRED, https://www.wired.com/insights/2013/03/big-data-the-key-to-economic-development/ (last visited on Nov. 26, 2018).

61 Jason Parms, *More Info, More Problems: Privacy and Security Issues in the Age of Big Data*, BUS. (Sept. 21, 2018), https://www.business.com/articles/privacy-and-security-issues-in-the-age-of-big-data/; *see also* Stacy Collett, *Five New Threats to Your Mobile Security*, CSO (Sept. 21, 2018), https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html (providing examples of network security flaws that lead to stolen data).

62 *See generally* Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM. (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

63 *Id.*

64 *Id.* (explaining that the Equifax security breach allowed hackers to access information including credit card numbers, and personal identifying information including names, Social Security numbers, birth dates, addresses, and driver's license numbers for thousands of card holders); *see generally* OFFICE OF EMERGENCY COMMUNICATIONS, DEP'T OF HOMELAND SEC., CYBER RISKS TO NEXT GENERATION 9-1-1 2 (2016).

and significant identifying information.[65] Although Equifax's awareness of a bug in their system may be cited as irresponsible for careless cybersecurity standards, data breaches of this scale are far from abnormal.[66] For example, in 2013, Yahoo was hacked and an estimated 3 billion accounts were compromised, reportedly most likely by a state sponsored actor.[67] Other significant data breaches include: eBay, JP Morgan Chase, the U.S. Office of Personnel Management, and Sony's PlayStation Network, among many others.[68] The significance of these breaches is in the characteristics that define them. Each breach is the result of network vulnerabilities being exploited for one reason or another.[69] While the effects of a data breach on a commercial entity can significantly damage an entity's reputation, the effect of a large scale system failure, or exploitation of the advanced systems of NG9-1-1 would place lives directly in danger.[70] An act of cyber breach on an NG9-1-1 system can critically delay emergency services.[71] With the imminent popularity of fully integrated systems, next generation emergency services will become enhanced by the massive quantities of data available through integration with elements of "smart cities," simultaneously creating a more effective emergency network, as well as

---

65 *See* Laurel K. Lackey, *The Mother of All Breaches, How Equifax's Data Hack May Effect You Now…and in the Future*, W. VA. LAW. REV. 1, 37 (2017) (describing how "more personal information was released as a result of this breach than any other breach," and the "effects of the breach will not be known for years, even decades."); McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. NAT'L SECURITY L. & POL'Y 549, 560 (2018).

66 Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Jan. 26, 2018) https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html; Chris Arnold, *After Equifax Hack, Calls For Big Changes In Credit Reporting Industry*, NPR (Oct. 18, 2017), https://www.npr.org/2017/10/18/558570686/after-equifax-hack-calls-for-big-changes-in-credit-reporting-industry.

67 Armerding, *supra* note 66.

68 *Id*.

69 Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES (Oct. 2, 2014), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ ("hackers appeared to have obtained a list of the applications and programs that run on JPMorgan's computers . . . which they could crosscheck with known vulnerabilities in each program and web application, in search of an entry point back into the bank's systems"); Mark Jewell, *Encryption Faulted in TJX Hacking*, WASH. POST (Sept. 25, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/09/25/AR2007092500836.html?noredirect=on; Gordon Kelly, *eBay Suffers Massive Security Breach, All Users Change Their Passwords*, FORBES (May 21, 2014), https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/#5b6d924f7492 ("origin of breach came from hackers compromising a small number of employee log-in credentials").

70 *How Data Breaches Can Affect Brand and Reputation*, VITRIUM (July 23, 2015), http://blog.vitrium.com/document-security-protection-drm-blog/how-data-breaches-can-affect-brand-and-reputation; OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64.

71 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 1.

a goldmine of data available to any hacker capable of exploiting network design flaws if they are not addressed.[72] However, NG9-1-1 is one looming vulnerability in an age soon to be encompassed by integrated big data collection networks.[73]

B. Smart Cities and NG9-1-1

NG9-1-1 is a significant step in the ongoing process of integrating technology into the infrastructure of cities during a time of increasingly significant urbanization.[74] With over 50 percent of the global population living in cities, the efficiency in which people and their environment interact needs improvement.[75] Smart cities are envisioned to be "environmentally sustainable, provide efficient transportation, have efficient use of resources, improved urban planning, and enhanced public safety."[76] Such vastly improved efficiency will be, in part, the product of big data analytics, and there is no doubt that the improved efficiency that smart cities promise to bring are necessary.[77] Among those benefits, there will be an integration of NG9-1-1 within smart cities planning and development.[78]

While definitions vary, generally a smart city is "a municipality that uses information and communication technologies to increase operational efficiency, share information with the public and improve both the quality of government services and citizen welfare."[79] Although the improved operational efficiency of cities is necessary, and even critical to the further development of society, [80] there are a number of significant risks that must be addressed, and continually updated as societal and technological transformations occur.[81] Given the

---

72 Reinhard Ekl et al., *NG9-1-1 Standards and Best Practices Conference, Smart Cities and NG9-1-1*, NENA, http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/sbp/20180118_0800%E2%80%931000_Smart_Cit.pdf (last visited Oct. 20, 2018).

73 *Id.*

74 *Id.*

75 *Id.*

76 *Id.*

77 Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309, 315 (2017).

78 Reinhard Ekl et al., *supra* note 72; *see also* Hiller & Blanke, *supra* note 77 (describing the use of big data in the engineering of smart cities).

79 Margaret Rouse, *What is smart city? – Definition from WhatIs.com*, IOT AGENDA, http://internetofthingsagenda.techtarget.com/definition/smart-city (last visited Oct. 5, 2018).

80 Hiller & Blanke, *supra* note 77, at 311-12, 317 (describing the advantages of data collection in smart cities).

81 *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 107-09 (2018) (discussing smart city movement to data algorithm use as discriminatory, erroneous, or otherwise problematic); Hiller & Blanke, *supra* note 77, at 311-12, 317 (addressing how to define and protect privacy when using big data for smart cities).

significant number of components required to feed massive quantities of data for operational efficiency, it is clear that the transition to smart cities will not occur overnight. In fact, the transition is well underway, as evident by NG9-1-1 system initiatives.[82] For that reason, the implications of an unsecure NG9-1-1 network could have detrimental consequences.

If an NG9-1-1 network were crippled by a cyber-attack, the effects may be significantly amplified within the context of a smart city, and similarly, if a network within a smart city were compromised, NG9-1-1 networks may be placed in a more vulnerable position.[83] This crippling effect is because all of these advanced data systems rely extensively on IP-based network integration, the complexity of which results in the potential for cyber vulnerabilities.[84] For example, in 2017, just days before the inauguration of President Trump, Romanian hackers installed malware on D.C. police computers, requiring the police to disable about 70 percent of D.C. security cameras for several days while the malware was removed.[85] Other attacks around the world include the 2015 cyber-attacks on Ukrainian energy companies by suspected Russian hackers, and a cyber-attack on a terminal of India's "largest container port,"

---

82 Chris Bousquet, *Data-Driven Emergency Response: Learning from Hurricanes Harvey and Irma*, DATA-SMART CITY SOLUTIONS (Oct. 3, 2017), https://datasmart.ash.harvard.edu/news/article/data-driven-emergency-response-learning-from-hurricanes-harvey-and-irma-113 (describing the current and needed development of technology to address citizen needs during hurricanes); Ekl et al., *supra* note 72 (depicting use of IoT data in NG 9-1-1 calls today).

83 Anuradha Shukla, *Are Smart Cities Prepared For Cyber Attacks?*, BUSINESSWORLD (July 11, 2017), http://businessworld.in/article/Are-Smart-Cities-Prepared-For-Cyber-Attacks-/11-07-2017-121886; *see also* Julia Ainsley, *Two Romanians arrested for hacking into 123 D.C. police surveillance cameras before inauguration*, NBC NEWS (Dec. 28, 2017, 7:58 PM), https://www.nbcnews.com/news/investigations/two-romanians-arrested-hacking-123-d-c-police-surveillance-cameras-n833346 (describing cyberattack of police department computers used for camera surveillance); Mary Scott Nabers, *Smart City Security: Atlanta Cyberattack Cripples City*, IOT WORLD TODAY (Apr. 5, 2018), https://www.iotworldtoday.com/2018/04/05/smart-city-security-atlanta-cyberattack-cripples-city/ (describing cyberattack on Atlanta electronic records and need for smart city security).

84 Poul Nielsen, *Smart City Security and Cyber Attacks*, INFO. SEC. BUZZ NEWS (Feb. 25, 2016), https://www.informationsecuritybuzz.com/articles/smart-city-security-and-cyber-attacks (hypothesizing domino effect in which many city operations can be compromised in a cyberattack); NAT'L EMERGENCY NUMBER ASS'N, NENA NEXT GENERATION 9-1-1 SECURITY (NG-SEC) INFORMATION DOCUMENT 15 (2016) (providing guidance on securing IP networks used for NG9-1-1 security).

85 Ainsley, *supra* note 83; Kim Crawley, *Washington DC Surveillance Cameras Infected by Ransomware*, THREAT VECTOR (Jan. 17, 2018), https://threatvector.cylance.com/en_us/home/washington-dc-surveillance-cameras-infected-by-ransomware.html (detailing ransomware used in cyberattack on D.C. police video cameras); Shukla, *supra* note 83.

debilitating one of its essential terminals.[86] Attacks on public safety, critical infrastructure, and commercial sectors, evidence the risk of significant exposure caused by malicious actors intending to do harm.

What makes such vulnerability far more dangerous is the breadth of the attack. If hackers are capable of deleting footage stored on nearly an entire city's security camera footage—what would stop the same hackers from turning all the traffic lights in a city green?[87] On the other hand, what if a worker at a local energy company accidently downloads malware into the fully integrated electric grid, possibly disabling the ability to call a local PSAP? A hacker may as easily reroute calls from one PSAP's jurisdiction to another with the intent of causing mass confusion in the wake of something more sinister, such as a terrorist attack.[88] Therefore, because NG9-1-1 and other IP-based communication technologies will be fully integrated within a futuristic smart city environment, they must be designed by taking security into account throughout development in order to reduce vulnerabilities.

III. UNDERSTANDING THE RISK OF IP-BASED NETWORKS

Your awareness of a medical emergency triggers your call to 9-1-1. You pick up your smartphone and begin instinctively dialing, but unexpectedly, the line is dead. Upon a second attempt from your cell phone with the same result, you may try using a landline to no avail. Panicked, you attempt to drive your critically injured neighbor to the hospital, which also happens to be in disarray. Without access to 9-1-1 dispatchers, a society that has become reliant on virtual communication is rendered lost.[89] Such a scenario may be the result of a large scale cyber-attack on an NG9-1-1 network with lapses in cybersecurity preparedness.[90] Per Murphy's law, if something can go wrong, it will.[91] In the digital age, there is an ever-present risk that malicious actors may exploit

---

86 Shukla, *supra* note 83.

87 Faiz Siddiqui, *Can hackers take over traffic lights?*, WASH. POST (Aug. 8, 2015), https://www.washingtonpost.com/local/could-a-hacker-gain-control-of-dcs-traffic-system/2015/08/08/7cb7cf94-201a-11e5-bf41-c23f5d3face1_story.html?utm_term=.1ea3be697522 (recounting hackers turning traffic lights from red to green).

88 David Raths, *Increased Connectivity Brings Cybersecurity Threats to 911 Call Centers*, EMERGENCY MGMT., Fall 2016, at 30, 31 (discussing ability of PSAPs to reroute calls, but the switch to NG9-1-1 brings more vulnerabilities).

89 Kevin Rector, *Baltimore 911 dispatch system hacked, investigation underway, officials confirm*, BALT. SUN (Mar. 27, 2018, 7:00 PM), http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-911-hacked-20180327-story.html (describing hacking of 911 call center and switch to analog services).

90 Traci Knight, *Improving the Cybersecurity Posture of NG911 Systems*, SAFECOM (Apr. 1, 2016), https://www.dhs.gov/safecom/blog/2016/04/01/improving-cybersecurity-posture-ng911-systems.

91 *Murphy's Law*, WEBSTER'S ENCYCLOPEDIC UNABRIDGED DICTIONARY (1996).

network vulnerabilities.[92] Fortunately, NG9-1-1 presents the opportunity to learn from past cyber threats and create a secure IP-based communications network.[93]

The first step in analyzing risk is to identify possible threats one may encounter.[94] NENA succinctly states:

> IP networks were developed to foster resilient connectivity but not security. IP multimedia services are easy targets because they are based on IP networks that are inherently insecure. IP was also developed to be flexible, so there are many types of services within today's infrastructure that have been built on top of IP over time. Once you transition to NG9-1-1 you rely on these IP networks to deliver Emergency Services.[95]

While NG9-1-1 possesses many capabilities that subvert the risk of operating on vulnerable IP-based networks (such as the ability to transfer calls from a PSAP that is experiencing a loss of operational capability to a functional PSAP in another jurisdiction), the constant and evolving nature of cyber threats and criminal capability ensures an ever-present risk.[96] In an integrated network, an individual system may seem secure.[97] However, vulnerabilities may be present, providing a litany of ways for criminals or state actors to gain access and exploit internet devices and applications.[98] Crypting services used to encrypt malware can be used to hide viruses within systems for significant amounts of time with no clear alert.[99] Hacking technology can be purchased at an affordable cost and is therefore easily accessible.[100] A hacker may gain access to a seemingly secure network by exploiting the network connection using tactics such as "gathering intelligence—often through social engineering, implanting backdoors, strengthening control and access of the target's network, exfiltrating data for as

---

92 PABLO GUTIERREZ ASTILLEROS ET AL., CYBERSECURITY: GUIDELINES AND BEST PRACTICES FOR EMERGENCY SERVICES 3 (2018); Dave Piscatello, *Threats, Vulnerabilities and Exploits - oh my!*, ICANN (Aug. 10, 2015), https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my (explaining the concepts of threats, vulnerabilities in exploitation related to the field of cybersecurity).

93 Knight, *supra* note 90.

94 *Risk Analysis and Risk Management*, MINDTOOLS, https://www.mindtools.com/pages/article/newTMC_07.htm (last visited Nov. 26, 2018).

95 NAT'L EMERGENCY NUMBER ASS'N, *supra* note 84.

96 ASTILLEROS ET AL., *supra* note 92; NAT'L EMERGENCY NUMBER ASS'N, *supra* note 84, at 16; *NG9-1-1 Project*, *supra* note 35.

97 Scott Goolik, *8 Cyber Security Vulnerabilities: Know Your Enemy*, SYMMETRY (May 19, 2016), https://symmetrycorp.com/blog/8-cyber-security-vulnerabilities.

98 *Id.*; *see* ASTILLEROS ET AL., *supra* note 92, at 14.

99 Goolik, *supra* note 97.

100 *Id.* (discussing affordable software such as Remote Administration Tools (RAT), Keyloggers, and Ransomware).

long as they can, [and then] covering their tracks."[101]

Moreover, there is a distinct cyber vulnerability in PSAPs, particularly in the quantity of PSAPs, possessing insufficient resources required to effectively mitigate cyber vulnerabilities.[102] According to Chris Patti, a technical writer for ComTech Telecommunications, "Cybersecurity is—by its very nature—an ongoing, ever-evolving, long-term process. There is no 'magic bullet' that will instantly whip an organization's networks (and its users) into shape."[103] Because PSAPs are critical to the function of NG9-1-1 systems, it is of equal importance that they are secure.[104] According to public safety expert Mike Beagles, PSAPs present a unique cyber vulnerability; "There are more than 6,000 PSAPs located across the country, and 80 percent of them are small, making them unlikely to have adequate cyber security defense programs."[105] Given the nature of NG9-1-1, and the interoperability of ESI-networks and PSAPs, the security that an individual PSAP has will only protect the network to a certain extent.[106] Security policies must be implemented to significantly decrease the risk of losing PSAP operational capabilities. Any PSAP policy that is implemented must focus on developing expertise in the foundational practices and basics of network security.[107] Additionally, because PSAPs throughout the country have significant variances in resources, any implementation must also be realistic.[108] At the heart of any information security policy should be the CIA triad: confidentiality, integrity, and availability.[109]

---

101 *Id*.

102 APCO INT'L, AN INTRODUCTION TO CYBERSECURITY: A GUIDE FOR PSAPS 8 (2016); *see* Beagles, *supra* note 18.

103 Chris Patti, *Top 5 Cybersecurity Practices for PSAPs*, COMTECH (Aug. 8, 2015, 7:00 AM), http://i.telecomsys.com/blog/top-5-cybersecurity-practices-for-psaps.

104 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64; Beagles, *supra* note 18.

105 Beagles, *supra* note 18.

106 NAT'L EMERGENCY NUMBER ASS'N, *What is NG911?*, EMS1 (Apr. 1, 2015), https://www.ems1.com/ems-products/communications/articles/588619-What-is-NG911/ (explaining that ESI-networks carry different types of data using hierarchical design to support emergency management authorities).

107 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 10 (describing recommended actions to improve NG9-1-1 systems).

108 NAT'L EMERGENCY NUMBER ASS'N, *A Policy Maker Blueprint for Transitioning to the Next Generation 9-1-1 System* 6-7 (Sept. 2008), https://cdn.ymaws.com/www.nena.org/resource/collection/B6781C63-012C-4E90-939B-001733976BBC/Policy_Maker_Blueprint_for_Transition_to_NG9-1-1.pdf (discussing planning and coordination by local, state and federal government to fund NG9-1-1 services).

109 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 3; Philip Favro et al., *The New Information Governance Playbook for Addressing Digital Age Threats*, 23 RICH. J.L. & TECH. 1, 33 (2017).

A. Confidentiality, Integrity, Availability

Confidentiality, Integrity, and Availability, also known as the CIA Triad (CIA), are the guiding principles for information and network security policies, which can form the basis of PSAP security.[110] Confidentiality refers to the accessibility of information in a system.[111] First, applying password protections, utilizing encryption services, and ensuring that data is accessed only by those who have clearance is central to confidentiality.[112] Secondly, "Integrity means that attackers cannot change or destroy information in a computer or network without detection and that changed or destroyed information can be restored."[113] Lastly, the availability of data focuses on having the ability to access data instantly.[114] Consistent maintenance of software and hardware will ensure that data will be available.[115] By using the triad as an evaluative tool, PSAPs can focus on the very basics of security with greater efficiency.[116] The Department of Homeland Security elaborates on PSAP cyber security utilizing the CIA triad, stating:

> Loss of confidentiality, integrity, or availability has especially severe impacts in the emergency response domain. For example, loss of confidentiality within NG911 systems could expose information to identity thefts or disrupt ongoing investigations; loss of integrity could disrupt response to 911 calls; and loss of availability could prevent urgent requests from reaching a PSAP.[117]

The cyber security threats to NG9-1-1 networks stems from vulnerabilities present in devices and equipment, network infrastructure and connections, and data, applications, and services.[118] A cybersecurity response must "mitigate[e]

---

110 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 3; Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC be Sticking its Nose Under this Tent*, 2016 U. ILL. J.L. TECH. & POL'Y 35, 65 (2016).

111 44 U.S.C § 3542(b)(1)(B) (defining confidentiality as "preserving authorized restrictions on access and disclosure" of information and information systems).

112 *CIA Triad of Information Security*, TECHOPEDIA, https://www.techopedia.com/definition/25830/cia-triad-of-information-security (last visited Nov. 26, 2018).

113 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 3; Selznick & LaMacchia, *supra* note 110.

114 *See* Philip Robinson, *CIA triad – The Basic Principles of Data Security*, LEPIDE BLOG (Feb. 16, 2017), https://www.lepide.com/blog/cia-triad-the-basic-principals-of-data-security/ (discussing data integrity and its availability).

115 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 8; Favro et al., *supra* note 109, at 36.

116 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 3.

117 *Id.*

118 *Id.* at 5.

risk by lessening vulnerabilities, deter threats, and minimize[e] consequences."[119] PSAPs of the future realistically cannot be entirely secure. Cyber breaches and illegal access to PSAPs will inevitably happen due to a variety of circumstances, including faults in security, mistakes, poor cyber hygiene, and malicious actors.[120] By following basic cybersecurity protocols, PSAPs will be able to mitigate risks, and decrease the fallout from major incidents.[121] PSAPs should follow basic cybersecurity protocols promulgated by the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[122]

B. NIST Framework

NIST points out in its Framework for Improving Critical Infrastructure Cybersecurity, "[t]he Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary."[123] The goal of this framework is to provide a technologically neutral approach to implement best practices for cyber security.[124]

The "Framework Core" is a set of five underlying principles meant to be considered in the implementation of dynamic best practices.[125] The five underlying principles are: Identify, Protect, Detect, Respond, and Recover.[126] Identify is a function focused on developing "an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities."[127] "The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event," with specific focus on cybersecurity awareness and training, data security, information protection processes and procedures, and other protective technologies.[128] "The Detect Function enables

---

119 DEP'T OF HOMELAND SECURITY, *National Infrastructure Protection Plan* 7 (2009) https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

120 *Id.*; OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 4.

121 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 8.

122 *See generally* NAT'L INST. STANDARDS & TECH., *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (explaining that each organization will have individual risks, but that the Framework will help reduce them).

123 *Id.* at 2.

124 *Id.* at 4.

125 *Id.* at 4.

126 *Id.*

127 *Id.* at 8.

128 *Id.*

timely discovery of cybersecurity events."[129] Responding to cybersecurity events requires the implementation of appropriate activities regarding detection thereof.[130] Recovery consists of developing and maintain a systems resiliency and capability to restore "any capabilities or services that were impaired due to a cybersecurity event."[131]

By implementing the NIST cyber-security framework, PSAP's can ensure a high level of security through diligence in updating standards, and recognition of new threats.[132] NG9-1-1 requires consistent security, that also detects ever-evolving cyber threats.[133] While the security of NG9-1-1 has certainly received recognition, and standards are in place to identify and solve technical issues, PSAPs and ESInets, along with all Voice Over Internet Protocol Communications, still remain vulnerable.[134] The policies and administrative agencies that are charged with ensuring the security for NG9-1-1 must ensure security protocols in the evolution of NG9-1-1.

IV. NG9-1-1 LEGISLATION

In November 2017, Congress introduced the Next Generation 9-1-1 Act of 2017 (the Act) to support and aid the deployment of nationwide NG9-1-1 systems.[135] The policy goals of the Act include creating "seamless interoperability between PSAPs;"[136] maintaining State, regional, and local levels of control; the promotion of "increased compatibility"; and the "functional interconnection of the nation's 9-1-1 systems with the wireless nationwide public safety broadband network being deployed by the First Responder Network Authority."[137] Many PSAPs have already commenced transition to the IP-based NG9-1-1 systems.[138] While the Act calls for increased action on critical issues facing the implementation of NG9-1-1, such as cybersecurity, there are practical barriers facing NG9-1-1, namely funding considerations for PSAPs.[139] Increased federal support to PSAPs is necessary if the substance of the Act is to

---

129 *Id*.
130 *Id*. at 11.
131 *Id*. at 9.
132 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 6.
133 *Id.* at 10.
134 *NG9-1-1 Project*, *supra* note 35.
135 S. 2061, 115th Cong. § 1.
136 *Id.* at § 4.
137 *Id.* at § 2.
138 Adam Stone, *PSAPs Move Ahead with Next-Generation 911 as Carriers Lag*, EMERGENCY MGMT. (June 28, 2017), http://www.govtech.com/em/next-gen-911/PSAPs-Move-Ahead-with-Next-Generation-911-as-Carriers-Lag.html.
139 *Id.*; S. 2061, 115th Cong. § 2.

be realized.

A. The Next Generation 9-1-1 Act Implementation

The Act is a necessary piece of proposed legislation to provide guidance and funding, to ensure an effective rollout of NG9-1-1 nationwide.[140] The Act first acknowledges that nationwide framework is "essential to help guide the transition" to NG9-1-1, while still maintaining the need to preserve "[s]tate, regional, and local control over the governance and technology choices of the Nation's 9-1-1 systems."[141] Maintaining localized control is a primary policy point of the Act.[142] This is because 9-1-1 is a state-provided emergency call network and each state has their own model by which they operate emergency response systems.[143] It is a localized system, and many PSAPs have not been significantly updated since the 1970s.[144] The Act addresses the significant vulnerabilities inherent in IP-based networks.[145] However, without a more effective implementation of federal efforts and funding, NG9-1-1 will fall victim to the very same discrepancies of the current 9-1-1 system and lag behind in many areas of the country.[146] The National 9-1-1 program analyzed a survey of states transitioning to NG9-1-1, stating:

> about half of states were transitioning to NG911 in 2015, but that state

---

140 S. 2061, 115th Cong. § 6.

141 *Id.* at § 2.

142 *Id.* at § 6.

143 *See* NAT'L. HIGHWAY AND SAFETY TRAFFIC ADMIN., GUIDELINES FOR STATE NG9-1-1, 10 (2012), https://www.911.gov/pdf/National_911_Program_Model_Guidelines_State_NG911_Legislative_Language_2012.pdf.

144 Mark Fletcher, *The Truth about 911: How Outdated Technology is Putting Your Life at Risk*, AVAYA (July 22, 2016), https://www.avaya.com/blogs/archives/2015/07/the-truth-about-911-how-outdated-technology-is-putting-your-life-at-risk.html.

145 S. 2061, 115th Cong. § 2; David Simpson, *Creating a Culture of Cybersecurity in America's 911 Call Centers*, FCC BLOG (Jan. 28, 2016), https://www.fcc.gov/news-events/blog/2016/01/28/creating-culture-cybersecurity-america's-911-call-centers (explaining IP-based systems "can also introduce new vulnerabilities and expose 911 systems to cyber threats that didn't exist in the legacy 911 environment.").

146 *See* 911.GOV, *Current State of 911 Funding and Oversight*, at 1 (2008), https://www.911.gov/pdf/National_911_Program_Current_State_911_Funding_Oversight_2013.pdf (explaining "current 911 funding is unstable and inadequate to support the migration to NG911."); *Discussion Draft To Provide Funding for the Construction and Maintenance of a Nationwide, Interoperable Public Safety Broadband Network and for Other Purposes and on H.R. 4829, the Next Generation 911 Preservation Act of 2010 Before the H. Subcomm. on Comm., Tech., and the Internet of the Comm. on Energy and Com.*, 111th Cong. 2 (2010) (statement of Rep. Rick Boucher, H.R. Committee on Energy and Commerce) (maintaining "The largest single challenge to creating the first responder network is identifying and obtaining the funding that is needed for the buying, the installation, the operating, and the maintaining of the equipment that will provide broadband communications.").

> and local progress varied. 10 states reported that all 911 authorities in their state processed calls using NG911 systems. 18 states reported having no state or local NG911 transition plans in place, which indicates that these states were in early planning stages or had not yet begun.[147]

Although the National Highway and Traffic Safety Administration (NHSTA) is leading efforts to ensure the implementation of NG9-1-1 is supported at a federal level, the fundamental issue of uneven implementation will persist.[148] The Government Accountability Office (GAO) has called upon NHSTA to "develop performance measures and goals to assess how the initiative meets its mission in supporting the implementation of the Next Generation 911 system."[149] The greatest challenge facing federal agencies working to ensure effective rollout of NG9-1-1 are the various discrepancies between states and regions within states.[150] For example, the National Association of State 9-1-1 Administrators (NASNA) examined the authority that statewide 9-1-1 programs possessed in the implementation, and control over their networks.[151] The study recognizes that state 9-1-1 programs are generally created by state legislatures, and that not all states even have 9-1-1 programs.[152] The study also revealed that 24 states did not possess the level of oversight or enforcement necessary to ensure funds secured via state tax or revenue streams for 9-1-1 are actually allocated to 9-1-1 services.[153] In fact, the allocation of 9-1-1 funds to other state functions is a fraudulent act that has been plaguing state 9-1-1 agencies for over a decade.[154] Although Congress is attempting to ensure proper federal oversight

---

147 Kevin Randolph, *GAO reviews Next Generation 911 implementation nationwide ahead of roadmap development*, HOMELAND PREPAREDNESS NEWS (Feb. 27, 2018), https://homelandprepnews.com/stories/26999-gao-reviews-next-generation-911-implementation-nationwide-ahead-roadmap-development.

148 *Final Report of TFOPA Working Group 3*, TASK FORCE ON OPTIMAL PUB. SAFETY ANSWERING POINT ARCHITECTURE (TFOPA), WASHINGTON UTILS. AND TRANSP. COMM'N, at 5 (Sept. 28, 2018).

149 Edwards, *supra* note 4.

150 NAT'L ASS'N OF ST. 9-1-1 ADMINS, FOUR POTENTIAL SUSTAINABLE FUNDING MODELS FOR NG911, at 13 (2015).

151 *Id*.

152 *Id*. at 11.

153 *Id*. at 13; *see* Elaine Seeman et al, *The First Step in Modernizing our 911 Emergency Call Centers: Revising the Sate Enhanced (E) 911 Legislative Funding Scheme to Efficiently Distribute 911 Funds*, 2012 U. ILL. J.L. TECH. & POL'Y., 289, 298 (2012) (explaining North Carolina's 9-1-1 funding formula was based off the "ill-fated assumption" that "local governments would spend their annual 911 fund distributions" but instead the states accumulated large surpluses for "unspecified purposes").

154 Michael O'Rielly, *States Must Stop Raiding 9-1-1 Fees*, FED. COMM. COMMISSION (Mar. 1, 2017, 4:52 PM), https://www.fcc.gov/news-events/blog/2017/03/01/states-must-stop-raiding-9-1-1-fees#_ftn1 (explaining that some states "divert fees collected for legitimate and needed 9-1-1 communications capabilities to unrelated purposes" and that the FCC has been dealing with the problem for almost fifteen years); *see also* COMM. ON

for the implementation of NG9-1-1, the very localized nature of 9-1-1 is the greatest barrier to overcome in achieving a secure 9-1-1 network.[155] Increased federal oversight is vital to ensure NG9-1-1 is not only implemented, but also secured. 9-1-1 networks did not effectively address the risk of cyber-attacks due to the "closed network function" of their systems. However, with integrated IP-based networks, the level of oversight to ensure maximum operability and security of call networks need to increase.[156]

B. Cybersecurity and the NG9-1-1 Act

Continually, cybersecurity has received a significant amount of national attention. From Facebook's violation of user trust, to President Trump's Executive Order to strengthen the cybersecurity of federal networks and critical infrastructure, all evidences not only a national but international need to secure networks and data.[157] The Act has placed an emphasis on cybersecurity, noting the risk of threats posed to PSAPs and next generation networks.[158] It is critical

---

COMMERCE, SCI., & TRANSP., THE ENHANCED 911 EMERGENCY COMMUNICATIONS ACT OF 2003, S. REP. NO. 108-130, at 3 (2003) ("Recently, State lawmakers and administrators have […] discovered instances in which E–911 funds have been used for purposes other than the provision of E–911 service. Observers claim as many as 11 States have been 'raiding' their collected E–911 funds to satisfy other State obligations.").

155 NAT'L ASS'N OF ST. 9-1-1 ADMINS, *supra* note 150, at 10 (discussing how Congress can use Federal grants to provide for funding and oversight in implementation of NG911); *see* S. 2061, 115th Cong. § 3 (stating that "a nationwide strategy for Next Generation 9-1-1 services has become essential to help guide the transition and create a common framework for implementation of Next Generation 9-1-1 services," and as such Congress is enacting legislation to achieve this goal).

156 *See* Jay English, *Cybersecurity and the PSAP*, APCO INST. (Mar. 2014), https://www.apcointl.org/doc/training-certification-1/481-cde-36485-cybersecurity-and-the-psap/file.html (explaining that "new concerns are emerging about the safety of the 9-1-1 closed-loop system, as we are discovering that the 'loop' may not be quite as 'closed' as we've always thought").

157 WHITE HOUSE, PRESIDENTIAL EXECUTIVE ORDER ON STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE (2017) (explaining that "the President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises" and that "because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise"); Carole Cadwalladr & Emma Graham Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election ("The data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box.").

158 S. 2061, 115th Cong. § 11 ("The Office, in consultation with the Department of

that the security of NG9-1-1 is not overlooked, and that the NG9-1-1 Act places the duty of addressing cybersecurity issues on the Department of Homeland Security, the National Institute for Standards and Technology, and the FCC.[159]

Although specific agencies have been delegated the responsibility in assisting with the implementation of specific standards, the Act designed "nonproprietary, consensus based standards" while still allotting for state, local, and regional control.[160] Because the Act provides consensus-based standards, local governments are given the responsibility to ensure that their call networks and PSAPs are up-to-date and in accordance with those standards.[161] As a result, any nonproprietary security protocols suggested by expert agencies will merely be left to each state and local government to independently implement either as local governments see fit, or as governments are capable.[162] While it is in the interest of each state to consistently maintain a security centric approach regarding its PSAPs, an increase in federal support will play a role in ensuring consistent funding and support. Without consistent funding and continually managed security protocols at a local level, PSAPs may lapse in security updates and be left vulnerable to cyber threats.

While a federal recommendation for cybersecurity will prevent the federal government from overreaching their regulatory authority, and respect the autonomy of state governments, it will not ensure effective and consistent cybersecurity efforts. There are major discrepancies in the status of PSAP technology throughout the United States.[163] The 9-1-1 funding throughout the

---

Homeland Security and the National Institute for Science and Technology, shall provide support to States, localities, vendors, and other entities in addressing cybersecurity issues related to Next Generation 9-1-1 services.").

159 *See* OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64, at 6 (explaining that "the Department of Homeland Security (DHS) strongly recommends adopting the NIST Cybersecurity Framework, which is a flexible, risk based approach to improving the security of critical infrastructure," to address NG9-1-1 cybersecurity issues); Knight, *supra* note 90 (discussing how "NG911 will also introduce new vectors for attack that can disrupt or disable PSAP operations, broadening the concerns of—and complicating the mitigation and management of—cyber risks across all levels of government," and as such, the Department of Homeland Security Office of Emergency Communications and Department of Transportation National 911 Program has produced the NG911 Cybersecurity Primer to address said cybersecurity issues).

160 S. 2061, 115th Cong. § 4.

161 *Id.*

162 *Id.*

163 Raths, *supra* note 7 ("So far, […] the federal grant funding to help PSAPs transition to next-generation 911 has been minuscule."); *see* Donny Jackson, *Public-safety groups seek federal funds to pay for next-gen 911 (NG911) upgrades*, URGENT COMM. (Mar. 21, 2018), http://urgentcomm.com/ng-911/public-safety-groups-seek-federal-funds-pay-next-gen-911-ng911-upgrades **(**discussing how "in 2012, Congress funded the implementation of an advanced, interoperable, wireless broadband network for first responders, known as

country has been subject to frequent misuse.[164] These discrepancies, and PSAP's uneven deployment of standards-based technology nationwide, are likely to persist in the absence of meaningful reform in the manner that PSAPs implement security protocols and network maintenance.[165] PSAP jurisdictions receiving state and federal assistance and grants to effectively implement NG9-1-1 security measures do not present major security risks, however, jurisdictions that lack funding and resources hindering implementation and regulation of proper security protocols are at greater risk of experiencing a cyber breach.[166]

While the initial implementation of NG9-1-1 systems will significantly improve the security of updated PSAPs, the efforts to update these PSAPs will have little long-term effect without a consistent and diligent practice of cyber hygiene and security.[167] Suggested standards provide a flexible way for PSAPs to independently and accurately gauge their own cyber preparedness. However, in the absence of meaningful federal support, suggested standards will only continue the uneven implementation of advanced security protocols.[168] Future

---

FirstNet," and that "the progress of FirstNet highlights the need for Congress to make a similar investment to modernize the complete emergency communications sector of our nation's critical infrastructure by achieving Next Generation 911").

164 *See* COMM. ON COMMERCE, SCI., AND TRANSP., *supra* note 154 ("State lawmakers and administrators have begun investigating the use of E-911 funds, and have discovered instances in which E–911 funds have been used for purposes other than the provision of E–911 service."); *see* O'Rielly, *supra* note 154 ("Some states divert fees collected for legitimate and needed 9-1-1 communications capabilities to unrelated purposes.").

165 *See* GALLAGHER, *supra* note 50 ("NG911 technologies are expected to change the way 911 systems operate and interoperate. Local 911 systems may need to create or revise policies to accommodate the new technology. Similarly, with the ability to interconnect systems, there is potential to create a nationwide 911 system, which may create the need for new policies to ensure PSAPs are interoperable and secure."); Elaine Seeman et al., *Legal, Policy and Ethical Issues of Using Big Data and Predictive Analytics in Next Generation (NG) 911 to Notify and Aid the Dispatch of First Responders*, 25 ALB. L.J. SCI. & TECH. 547, 557 (2015) ("Notwithstanding the benefits of more NG911 data and information, the collection and delivery of these data and information by telecommunication carriers, 911 service providers, PSAPs and first responder agencies [without proper security protocols in place] raise legal, ethical, and public policy issues to provide emergency services.").

166 *See* GALLAGHER, *supra* note 50, at 4 ("Each PSAP uses different technologies, is in different phases of upgrade, and is dependent on different sources of funding. […] As a result, there is variability in 911 levels of services [, such as security services,] across jurisdictions."); James E. Holloway et al., *Federalism in the Financing of 911 Emergency Call Services: Nature of the Federal-State Funding Arrangement to Finance Next Generation (NG) 911 Services*, 5 J. L., TECH. & INTERNET 113, 126 (2014) (discussing how "NG911 funding arrangements must permit states to govern essential […] information management and technology interests and objectives needed to provide NG911 services," including security).

167 GALLAGHER, *supra* note 50, at 10.

168 Next Generation 9-1-1 Act of 2017, H.R. 4672, 115th Cong. §2 (2017); *Realizing Nationwide Next-Generation 911 Before the Subcomm. on Commc'n and Tech. of the Comm. on Energy and Commerce*, 115th Cong. 3-4 (2017) (opening statement of Rep. Marsha Blackburn, Chairman, S. Comm. on Commc'n and Tech.); GALLAGHER, *supra* note

PSAPs must possess the resources to ensure that standards are consistently met and security is "baked in by design."[169] In the event PSAP security protocols lapse significantly, a malevolent cyber actor will undoubtedly possess the capability to inflict great harm upon the PSAP networks. As a recent congressional report pointed out: "[w]hile there is a national interest in promoting consistent cybersecurity policies across all PSAPs, there are no mechanisms in place to require state and local adoption of these best practices, which may present a risk to the NG911 network and the systems to which they interconnect."[170]

The increased resiliency of next generation systems is due to their interoperability, which happens to significantly increase the risk that an attack on one PSAP may have an effect on another interconnected PSAP.[171] PSAP interoperability is a reference to a multitude of next generation capabilities, allowing PSAPs to "seamlessly (1) receive calls and related data from origination networks, (2) share calls and related data among connecting ESInets, including across state boundaries, and (3) hand off calls and related data with each other."[172] Because NG9-1-1 interoperability is expected to be implemented first regionally, and then nationally, it is time "to adopt common technical standards that will enable interoperability," as well as security.[173]

V. NG9-1-1 SYSTEMS IN THE AGGREGATE: A FUNDING CRISIS

Because PSAPs operate on a state, regional, and local level, the challenge is unique in ensuring nationwide PSAP security. According to NENA, "as of December 2017, the United States [had] 5,783 primary and secondary PSAPs."[174] Many PSAPs will not make the transition from current 9-1-1 systems to NG9-1-1 without federal assistance.[175] The NG9-1-1 Act proposes sustainable funding models.[176] However, while current funding helps move PSAPs to next generation technology, it is not sufficient to protect PSAPs nationwide.[177]

50, at 5.

169 ASTILLEROS & MERTKA, *supra* note 92, at 32.

170 GALLAGHER, *supra* note 50, at 10.

171 *Id.* at 8.

172 ASS'N OF PUBLIC-SAFETY COMM. OFFICIALS-INT'L, Comment Letter on Proposed Rule to Revise Regulations for the 911 Grant Program Under the Next Generation 911 Advancement Act of 2012 (Nov. 6, 2017), https://www.regulations.gov/document?D=NTIA-2017-0002-0010.

173 GALLAGHER, *supra* note 50, at 8.

174 *9-1-1 Statistics*, *supra* note 21.

175 911.GOV, *supra* note 14.

176 H.R. 4672, 115th Cong., § 6(a)(2)(C).

177 911.GOV, *supra* note 14.

Diverting fees from underfunded 9-1-1 centers can "lead to understaffed calling centers, longer wait times in an emergency, and sluggish dispatch for public safety personnel. It also will slow the ability of 9-1-1 call centers to update their systems to support digital age technologies."[178] Although federal assistance programs, particularly the current multi-agency NG9-1-1 grant program, will provide essential funding to assist with the implementation of NG9-1-1, the implementation is only the first step in upgrading and enhancing nationwide 9-1-1 networks.[179] Once PSAP's are operating on NG9-1-1 systems, their advanced capabilities and connectivity will create a perpetual cyber risk on a large scale if the necessary funding is not secured and then maintained.[180]

The ultimate goal of the NG9-1-1 legislation is a nationwide deployment of 9-1-1 and PSAPs.[181] Through successful federal support, nearly 6,000 PSAPs in the United States would be upgraded to next generation networks.[182] This means each of the 6,000 PSAPs integrated with IP-based networks will be left vulnerable to the same threats as any other IP-based network.[183] However, each individual PSAP's capabilities will likely vary due to discrepancies in funding.[184] Although some PSAPs will implement secure networks, and conduct routine protocols to safeguard their ESI-networks, many PSAPs will likely receive inadequate funding and resources to maintain secure networks and will not have the capability to detect and prevent cyber threats.[185] Even if a sustainable funding model can be created and executed, the local nature of 9-1-1 guarantees that the actual implementation will vary.[186] 9-1-1 systems in the

---

178 Michael O'Reilly & Jessica Rosenworcel, *States are stealing funds from 9-1-1 emergency services — now they'll be punished*, THE HILL (Feb. 9, 2018), http://thehill.com/opinion/technology/373043-states-are-stealing-funds-from-9-1-1-emergency-services-now-theyll-be; Jean Turgeon, *When is Enough Actually Enough? A Hard Look at the Lagging Face of Public Safety (Part 1)*, AVAYA (Sept. 13, 2016), https://www.avaya.com/blogs/archives/2016/09/a-hard-look-at-the-lagging-face-of-public-safety-part-1.html.

179 911.GOV, *supra* note 14.

180 OFFICE OF EMERGENCY COMMUNICATIONS, *supra* note 64; *see also* Knight, *supra* note 90 (highlighting the range of risks potentially involved with NG911 and suggestions for possible mitigations of mentioned risks).

181 *See* S. 2061, 115th Cong. § 3.

182 *9-1-1 Statistics*, *supra* note 21; *see also* S. 2061, 115th Cong. § 2 (proposing accelerated implementation of NG-911 services to upgrade networks therefore increasing compatibility with emerging technologies).

183 Raths, *supra* note 88, at 2; *see also* GALLAGHER, *supra* note 50, at 8-10 (listing the possible setbacks to nationwide deployment of NG911, and the funding issues states are currently facing trying to decide which version of 911 to fund).

184 Raths, *supra* note 88; *see also* GALLAGHER, *supra* note 50, at 7 (positing the different outcomes various types of funding programs may have on the NG911 roll-out and upkeep efforts).

185 Raths, *supra* note 88.

186 *See* GALLAGHER, *supra* note 50, at 7.

United States need certainty regarding the future security of their networks.

In 2016, former FCC Chairman, Tom Wheeler recognized the need for Congressional action in NG9-1-1 implementation for PSAPs in a statement made before the Subcommittee on Communications and Technology of the United States House of Representatives during a hearing on the "Oversight of the Federal Communications Commission."[187] During this hearing, he presented three points to help with the implementation and operation of NG9-1-1 and PSAPs.[188] First, Chairman Wheeler called for a National 9-1-1 map to "eliminate the seams between commercial communications network infrastructure and emergency response dispatch systems."[189] Although this would provide clarity to the actual operational capability and mapping of PSAPs nationwide, this comment will focus on the latter two points. Second, Chairman Wheeler recognized the inability of PSAPs to keep up with cyber defense and called for bringing PSAPs under the protective wing of DHS's "Einstein Program" to centralize security efforts.[190] Third, Chairman Wheeler called for a national timetable, or target date, for completing the transition to NG9-1-1.[191] By implementing Chairman Wheeler's vision of federal support for PSAP's and their implementation and operation of NG9-1-1, the emergency call network of the future can be a success.

A. Federal Funding of Public Safety Initiatives

The NG9-1-1 grant program is a joint effort between the National Telecommunications Industry Administration (NTIA) and NHSTA.[192] The program, authorized under the NG9-1-1 Advancement Act of 2012,[193] allocated about "$115 million from spectrum auction proceeds" for NTIA and NHSTA to support the PSAP transition to NG9-1-1.[194] States that participate in this program

---

187 *Hearings*, *supra* note 9; *see also* Suresh Gursahaney, *FCC Chairmen Calls for NG911 Funding and Support for PSAPs*, MICROAUTOMATION (Aug. 10, 2016), http://www.microautomation.com/new-blog/fcc-chairman-calls-for-ng9-1-1-funding-and-support-for-psaps (summarizing Chairman Wheeler's comments to Congress).

188 *Hearings*, *supra* note 9.

189 *Id.*

190 *Id.*

191 *Id.*; *see also* Gursahaney, *supra* note 187 (summarizing the requests of Chairman Wheeler while before Congress).

192 NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. & NAT'L TELECOMM. & INFO. ADMIN., MANAGEMENT PLAN FOR THE NEXT GENERATION 9-1-1 GRANT PROGRAM (2017), https://www.ntia.doc.gov/files/ntia/publications/nhtsa_ntia_ng911_grant_program_management_plan.pdf.

193 Next Generation 9-1-1 Advancement Act of 2012, 47 U.S.C. §§ 1471-1473 (2018).

194 911 Grant Program, 82 Fed. Reg. 44131 (proposed Sept. 21, 2017) (to be codified at 47 C.F.R. pt. 400).

are permitted to use funds from the program for the "adoption and operation of NG911 services and applications; and the implementation of IP-enabled emergency services and applications enabled by NG911 services, including the establishment of IP backbone networks and the application layer software infrastructure needed to interconnect the multitude of emergency response organizations."[195] The maximum amount of funds allotted through the program are "$500,000 per state and $250,000 per territory," and although funds were expected to be awarded in early 2018, none have been awarded to date.[196]

Although the 9-1-1 grant program addresses the issue of underfunded PSAPs, commenters on the Notice of Proposed Rulemaking (NPRM) for the 9-1-1 grant program have expressed concern that the amount of funding available will only allow "marginal enhancements in any given area."[197] Other public safety associations have suggested alternative funding initiatives to efficiently use the available money.[198] For example, APCO has gained support for their proposal to focus funding initiatives on specific facilities to create model PSAPs and spur statewide deployment.[199] In their reply comment to the NPRM, APCO states:

> [T]he best way to use these grants is to create model deployments that demonstrate proofs of concept for fully-deployed and interoperable NG911 services in urban, suburban, and rural areas. By focusing on model NG911 deployments for a few areas, the grant program can better serve the entire country by producing blueprints for efficiently modernizing 911 systems nationwide. This should lower costs and speed implementations for systems that follow.[200]

APCO continues to state that interoperability ("meaning PSAPs can seamlessly (1) receive calls and related data from origination networks, (2) share

---

195 Wood, *supra* note 13.

196 *Id.*; *see also 911 Grant Program*, *supra* note 14 (outlining the two-stage application process and various requirements and stating that "NHTSA and NTIA will review all complete application packets and will then make awards").

197 Paul Kirby, *Public Safety, Industry Entities Weigh in on NG-911 Grant Program*, NAT'L PUB. SAFETY TELECOMM. COUNCIL (Nov. 17, 2017), https://blog.npstc.org/2017/11/07/public-safety-industry-entities-weigh-in-on-ng-911-grant-program; ASS'N OF PUBLIC-SAFETY COMM. OFFICIALS-INT'L, *supra* note 172.

198 *See* Kirby, *supra* note 197 (stating that the National Association of State 911 Administrators, The Colorado Public Utilities Commission, and other similar organizations are seeking clarification on the grant process to reduce confusion regarding state funding limits, and to reduce the potential that grant-seekers within the same states submit redundant applications); *see also* ASS'N OF PUBLIC-SAFETY COMM. OFFICIALS-INT'L, *supra* note 172.

199 *See generally* Jackson, *supra* note 163 (quoting FirstNet's Dave Buchanan, stating that the organization received "great feedback . . . [at their suggestion to make] call centers, PSAPs and those employees that work at PSAPs amongst those who have the priority and preemption in the top tier of eligible users").

200 Kirby, *supra* note 197; ASS'N OF PUBLIC-SAFETY COMM. OFFICIALS-INT'L, *supra* note 172.

calls and related data among connecting ESInets, including across state boundaries, and (3) hand off calls and related data with each other") must remain a top priority and proposes to condition the grant of funding on "achieving and maintaining interoperability."[201] If the local government fails to obtain this objective, the conditional funding must be returned back to the grant fund.[202] While ideally, the NG9-1-1 grant program will be capable of sufficiently supporting PSAPs nationwide, without additional funding,[203] APCO's proposal is likely the most efficient way to leverage funding for the full implementation of NG9-1-1.[204]

Although direct federal assistance for the implementation of NG9-1-1 in PSAPs would present an impracticable challenge, there may be alternative ways for the federal government to effectively aid in the implementation of NG9-1-1 on a local level.[205] Another public safety communications program may serve as a model or provide valuable lessons for the provision of federal assistance to local public safety networks.[206] Specifically, the First Responder Emergency Network is an example of a federally sanctioned public safety initiative providing direct support to state and local governments.[207]

While 9-1-1 inherently operates locally, the federal funding of local initiatives is not a foreign concept and FirstNet is the prime example of federal support for local public safety initiatives.[208] FirstNet, authorized under the Middle Class Tax

---

201 ASS'N OF PUBLIC-SAFETY COMM. OFFICIALS-INT'L, *supra* note 172 (defining interoperability to mean that "PSAPs can seamlessly (1) receive calls and related data from origination networks, (2) share calls and related data among connecting ESInets, including across state boundaries, and (3) hand off calls and related data with each other").

202 *Id.*

203 Public Notice and Comments Sought Regarding Auction of Next-Generation Wireless Services, 101 and 102, 83 Fed. Reg. 19660 (proposed May 4, 2018) (indicating that although there has been no direct mention that funds may be available for the NG9-1-1 grant program, the FCC plans auctions in the 24 GHz and 28 GHz spectrum in the near future, auctions 101 and 102, which would provide a full fix for the lack of funding available for PSAPs).

204 Kirby, *supra* note 197; *see also* APCO International, Comment Letter on NTIA and NHTSA Notice of Proposed Rulemaking on the 911 Grant Program, No. 170420407-7407-01 (Nov. 6, 2017), https://www.regulations.gov/contentStreamer?documentId=NTIA-2017-0002-0010&attachmentNumber=1&contentType=pdf.

205 Carter, *supra* note 37.

206 *See e.g.*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 143.

207 NAT'L PUBLIC SAFETY TELECOMM. COUNCIL, *FirstNet and NG9-1-1: High-Level Overview of Systems and Functionality* (Aug. 2015), http://www.npstc.org/download.jsp?tableId=37&column=217&id=3466&file=How_NG911_Will_Work_with_FirstNet_FINAL.pdf; *Top Ten Frequently Asked Questions*, FIRSTNET, https://www.firstnet.gov/sites/default/files/FirstNet_Partnership_FAQs__0.pdf (last visited Nov. 26, 2018).

208 *Key Factors to Consider for the Governor to Opt-In or Opt-Out of the FirstNet Plan*, FIRSTNET, https://www.firstnet.gov/sites/default/files/factors-governor-decision.pdf (last visited Oct. 15, 2018); *Top Ten Frequently Asked Questions*, *supra* note 207; *Public Safety*,

Relief and Job Creation Act of 2012, is not yet in operation but will be "a wireless broadband network that will connect first responders."[209] FirstNet, operating under the authority of the National Telecommunications and Information Administration of the Department of Commerce, is tasked with working with states individually to aid in the deployment of the public safety network and has the potential to serve as a model for increased cooperation between private and public sector organizations.[210] AT&T has been awarded a 25-year deal with FirstNet "to modernize and improve public safety communications by leveraging private sector resources, infrastructure, and cost-saving synergies to deploy and operate the Network."[211] FirstNet's "opt-in/opt-out" approach is a system that can be revolutionary for the relationship between the federal government, and its ability to work with states and local public safety professionals.[212]

Under the FirstNet initiative, States have the option to opt-in and allow FirstNet to deploy, operate, and maintain the state public safety Radio Access Network (RAN) created by AT&T.[213] If a State chooses to opt-out, the state takes the responsibility to deploy, operate, and maintain the RAN.[214] By choosing to opt-in, a state's RAN will effectively operate under FirstNet authority, which in turn means funding for the network comes directly from FirstNet.[215] The alternative option, opting-out, can still result in funding through National Telecommunications Industry Administration (NTIA) grant programs,

---

NAT'L TELECOMM & INFORMATION ADMIN., https://www.ntia.doc.gov/category/public-safety (last visited Nov. 26, 2018).

209 NAT'L PUBLIC SAFETY TELECOMM. COUNCIL, *supra* note 207; *Top Ten Frequently Asked Questions*, *supra* note 207.

210 *Top Ten Frequently Asked Questions*, *supra* note 207 (discussing how "Public safety organizations and associations advocated before Congress for a dedicated, reliable wireless network for first responders").

211 *Id.*

212 *Key Factors to Consider for the Governor to Opt-In or Opt-Out of the FirstNet Plan*, *supra* note 208; *see also* Theo Douglas, *All 50 States Have Joined FirstNet as Deadline Closes*, GOV'T TECH. (Dec. 28, 2017), http://www.govtech.com/public-safety/49-States-Have-Joined-FirstNet-California-Remains-a-Mystery.html (stating that "all 50 states, along with two territories and Washington, D.C.," opted-in for FirstNet prior to the deadline); Jackson, *supra* note 163 (discussing how FirstNet works with each state to make an individualized plan).

213 *Id*.

214 *Id.*

215 *Consultation*, FIRSTNET, https://www.firstnet.gov/consultation/funding (last visited Nov. 26, 2018) (quoting "Members of the FirstNet outreach and design teams will work closely with the designated single officer or governmental body to develop and deliver a network deployment plan that meets their needs. FirstNet will then provide the Governor of each State or territory with a notice of the completion of the request for proposal process; the details of the proposed plan; and the funding level for the state or territory. Upon receipt of the plan, a Governor will have 90 days to choose whether to participate in the plan provided by FirstNet or conduct its own deployment of a radio access network").

although the option has been referred to as "more labor-intensive."[216] Ultimately, all "50 states, two territories, Guam, the Northern Mariana Islands, American Samoa and the District of Columbia" chose to opt-in.[217] The option of having a federally implemented communications network for state and local authorities has clearly gained significant traction in State and local governments, and the FirstNet template can serve as the proper framework that Congress is seeking for the NG9-1-1.[218]

The most transferable concept from FirstNet to NG9-1-1 is the opt-in and opt-out approach.[219] APCO's proposal to condition the grant of 9-1-1 funds to PSAPs, which relies on the PSAPs acceptance and maintenance of certain standards, is akin to an "opt-in" grant program.[220] Similar to a State's acceptance of FirstNet's implementation and operation of their public safety network, when states opt-in, NTIA and NHSTA could grant NG9-1-1 funds on the condition that States follow certain standards and maintain certain operational capabilities.[221] NTIA and NHSTA can serve as the monitoring agency; as with FirstNet, where their duty is to ensure funds are directly utilized to further federal standards set by the expert agencies.[222] To encourage flexibility in the implementation of NG9-1-1 and planning prospectively, states should be able to either apply directly to NTIA and NHSTA, or have the option of submitting an application that outlines and details original implementation plans that are capable of meeting grant requirements, but may not necessarily be the provided implementation procedure.[223] This format does not overextend the federal government, leaves states in control, and provides clear direction by offering immediate incentives to further conditional federal procedures.

With the prospect of the NG9-1-1 grant program having increased engagement and providing more direction and incentive for states to implement next generation networks, an additional and pressing issue is ensuring the

---

216 Eyragon Eidam, *56 Jurisdictions Have Officially Opted in to FirstNet*, GOV'T TECH. (Oct. 2017), http://www.govtech.com/network/With-Jurisdictions-on-Board-FirstNet-Gathers-Forward-Momentum.html (stating that the alternative plan consists of various deadlines an approval processes, at the end of which the State either has the opportunity to purchase FirstNet service, or their plan is disapproved).

217 *Id*.

218 *See id.* (discussing how states have started opting-in to FirstNet as they realized the benefits of the first "dedicated nationwide public safety communications network").

219 *See id.* (explaining that states can opt-in to the network or opt-out and develop their own system).

220 *See* Kirby, *supra* note 197 (explaining eligibility for funding, qualified applications and the grant distribution process).

221 *See Consultation*, *supra* note 215 (outlining the specific requirements that states must comply with in order to receive FirstNet funding).

222 *See id.*

223 APCO International, *supra* note 204.

security following implementation.

B. Centralized Cybersecurity

In Chairman Tom Wheeler's testimony before Congress, he proposed that NG9-1-1 cybersecurity be incorporated into DHS's "Einstein Program."[224] The Einstein Program, managed by the National Cybersecurity Protection System within DHS and originally proposed in 2003, was an initiative "to be the primary cybersecurity system that would provide four major security capabilities to the Federal Government, such as intrusion detection, intrusion prevention, data analytics, and information sharing."[225] The program "was meant to be disseminated and integrated across all 23 Federal agencies' IT networking systems to help safeguard any personally identifiable information (PII) and avoid malicious web hacking attempts."[226] However, while the Einstein Program was a promising idea, the actual implementation was insufficient.[227] The Government Accountability Office (GAO) found that the Einstein Program failed to meet the four objectives stated for itself, because twenty-three Federal agencies were inconsistently adopting the program.[228] While the Einstein Program is currently not the all-encompassing and advanced cyber security system it was created to be, a significant amount of financial resources have been devoted to its improvement, with a forecasted total price tag of $5.7 billion.[229] As of April 2018, DHS was seeking up to $644 million "for a mix of programs to support federal agency cybersecurity, including the Continuous Diagnostics and Mitigation program and the network shield system known as Einstein."[230] It is clear that DHS is committed to not only improving the Einstein program, but also providing general cyber security for all of the federal government.[231]

---

224 *Hearings*, *supra* note 9.

225 Joey Song, *What is DHS EINSTEIN and Why Did It Fail?*, BUS. 2 CMTY. (Feb. 23, 2016), https://www.business2community.com/cybersecurity/dhs-einstein-fail-01462281; *see also* Aaron Boyd, *GAO: $5.7B Einstein Cyber Program Isn't Smart Enough Yet*, FED. TIMES (Jan. 29, 2016), https://www.federaltimes.com/management/2016/01/29/gao-5-7b-einstein-cyber-program-isnt-smart-enough-yet (referring to the cybersecurity tools used by the Einstein Program).

226 Song, *supra* note 225.

227 *See* Boyd, *supra* note 225 (explaining how the technological capabilities of the Einstein Program are limited).

228 *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GOV'T ACCOUNTABILITY OFFICE (Jan. 2016), https://www.gao.gov/assets/680/674829.pdf; *see also* Boyd, *supra* note 225 (detailing how the Einstein Program is failing to accomplish all its objectives).

229 Boyd, *supra* note 225.

230 Mark Rockwell, *DHS Seeks Growth in Cyber Budget*, FWC (Apr. 13, 2018), https://fcw.com/articles/2018/04/13/dhs-cyber-approps.aspx.

231 *Id*.

However, DHS's cyber efforts do not stop at the federal government.[232]

DHS has recently been engaged in providing aid to the Election Assistance Commission in the management of a $380 million spending bill authorized "for state and local governments to improve their election system cybersecurity."[233] Specifically, DHS has offered to provide "penetration testing, vulnerability assessments, exercises, training as well as threat information bolstered by help from the NSA and the intelligence community."[234] The significance of DHS collaborating to provide security to a state function is evidence that DHS is not only capable of providing cyber security to state authorities, but that this process should be a standard DHS procedure. PSAP cybersecurity functions should not only be supported by DHS, but are a natural extension of DHS cybersecurity. Congress should either include PSAPs in the future of the Einstein program as former Chairman Wheeler proposed or adopt a framework similar to Einstein which has a single entity, such as DHS, providing cybersecurity implementation, operation, and enhancement, to all PSAPs.

VI. CONCLUSION

PSAPs are, and should be, considered critical infrastructure, and NG9-1-1 will provide a much needed update to that infrastructure. They provide direction and control to our emergency responders during times of emergency, and with the updates of NG9-1-1, emergency responders and public safety officials will have significantly more information, direction, and overall increased efficiency. These improvements through IP-based networks, will save lives as well as increase the current security of 9-1-1 systems. However, these vast improvements and interconnectivity offer no solution to the security of emergency communications networks. IP-based networks inherently lack proper network security protocols. A long-term solution is vital to ensure continued financial support to such critical infrastructure otherwise these technological advancements will result in a fruitless endeavor. With the proper support for PSAPs, the lifeblood of 9-1-1, cyber vulnerabilities may be significantly mitigated. Given the current state of 9-1-1 and PSAPs being generally well under-funded, the federal government is best positioned to provide support for a nationwide transition to advance efforts. Because the nature of NG9-1-1 will facilitate increased interconnectedness across regions, and eventually the nation,

---

232 *Id*.

233 *Id*.

234 *Id*.; *see also* Chloe Kim, *Maryland Pounces on Federal Funding for Election Cybersecurity*, ST. SCOOP (Apr. 16, 2018), https://statescoop.com/maryland-pounces-on-federal-funding-for-election-cybersecurity.

the federal government must treat future 9-1-1 networks as critical infrastructure. If the 9-1-1 grant program provides the support it promises, NG9-1-1 systems may be capable of hitting NENA's target goal of having nationwide NG9-1-1 by 2020.[235] However, cybersecurity cannot be overlooked and must take a central role of all future IP-based networks. While PSAP cybersecurity concerns are being considered, evident by new legislation and activity within administrative agencies, more must be done.[236] By incorporating PSAPs as critical infrastructure under the protection of DHS, a centralized homeland-cybersecurity command can take a central role in mitigating risks and providing undeviating support to a secure nationwide emergency call network. What our country does now to support our 9-1-1 call centers may make the difference between life and death in the emergencies of the future.

---

235 George Rice, *Coalition Applauds NG911 Caucus Members in Requesting GAO Review*, 911.GOV (June 22, 2016), http://www.ng911now.org/blog/2016/6/22/coalition-applauds-ng911-caucus-members-in-requesting-gao-review.

236 *See Hearings*, *supra* note 9; ASS'N OF PUBLIC-SAFETY COMM. OFFICIALS-INT'L, *supra* note 172.