Lovely-Frances Domingo
lovely.f.domingo@gmail.com
UC Berkeley Information School PhD Applicant Fall 2021
Sample Writing – Written for Operational Risk in Private and Public Sectors course

Transforming Emergency Communications

The emergence of mobile and broadband technologies over the last ten years have ushered an unprecedented growth and impact on both the public and private sector particularly within the Communications Sector. Since 2010, changes to the Communications Sector include rapid innovations in mobile broadband, cloud computing, Internet of Things (IoT), software-defined networks, and voice & data convergence through smartphones and tablets.[1] According to the Communications Sector-Specific Plan (CSSP), mobile data traffic in 2013 alone have grown eighteen times the size of the entire internet in 2000. Furthermore, the CCSP mentions the widespread use of smart phones, tablets, and mobile applications contributed to this increase in data traffic, along with the demand for mobile broadband and the adoption of cloud computing technologies.[2] Mobile and broadband technologies have also increased the general public's expectations and desire for more information, and lack thereof can cause further disruption.[3] Emerging and continuing threats of natural disasters, terrorism, active shooter, etc. have placed critical emphasis on both the public and the private sector to develop strategic goals on how to utilize and implement mobile and broadband technology to improve critical communications during emergency and crisis situations, but with lack of emphasis on the importance of human factors and design of user interface, and the impact of digital transformation on vulnerable communities. The National Emergency Communications Plan

[1] *Communications Sector-Specific Plan*. Department of Homeland Security, 2015. 30 May 2018. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf>, p.1.
[2] Ibid, p. 4
[3] *National Emergency Communications Plan*. Department of Homeland Security, 2014. Accessed 17 May 2018. <https://www.dhs.gov/sites/default/files/publications/2014-11-07%20%20NECP%20Slick%20Sheet_0.pdf>, p. 7.

(NECP) 2014 presents high level strategic goals relevant to both the public and private sectors within the Communications Sector: 1) drive innovation and adoption of mobile application technologies; 2) interoperability, or the ability of disparate systems to exchange and make use of information across mobile technologies; and 3) the need to seamlessly integrate and collaborate across all sectors, institutions, or business units to improve coordination, resiliency, and continuity. This paper will highlight a number of key takeaways for each of these strategic goals, while addressing significant operational risks due to lack of emphasis on human factors and design, strong internal controls, and service limitations for vulnerable populations due to inadequate system infrastructures.

Driving innovation and adoption of emerging technologies to support and deliver "timely, relevant and accessible"[4] emergency information between institutions with their constituents is critical for both the public and private sectors. These technologies can be in the form of wireless and location-based services, mobile video, social media, and other software applications. According to the NECP (2014), the Nationwide Public Safety Broadband Network (established in 2008) have begun to implement wireless and broadband technologies and develop mobile applications for public safety in order to "augment" the use of Land Mobile and Radio (LMR) systems used by emergency personnel.[5] While LMR systems have been and continues to be the primary mode of communications between agencies and emergency personnel due to its high level of reliability, redundancy, coverage, capacity and resiliency against natural and man-made environments,[6] the NECP outlines the need to accelerate deployment and adoption of mobile products, applications, and services which provides critical

[4] Ibid, p. 46.
[5] Ibid, p. 2.
[6] Ibid, p. 8.

information to the greater public as well.[7] For instance, in the event of active shooter scenarios in public spaces, such as in schools, businesses, and/or government buildings, a research study led by The RAND Corporation (alongside the Police Executive Research Forum, RTI International, and the University of Denver) identified two-way communication (between responders and individuals impacted by the crisis) and faster access to information through an all-in-one software or mobile application as top priorities in improving communications and public safety.[8]

The Department of Homeland Security (DHS) through the Office of Emergency Communications (OEC) recognized the need to address the growing importance of utilizing mobile application technology through the Mobile Applications for Public Safety (MAPS) project. The MAPS project provides oversight for the public safety mobile ecosystem in order to promote "consistent security, functionality and performance best practices in the development and adoption of mobile apps."[9] Furthermore, in collaboration with DHS, the Association of Public-Safety Communications Officials (APCO) created an online resource to serve as the single trusted site for public safety mobile applications called the Application Community (www.AppComm.org). The Application Community serves as a vetting mechanism for mobile applications utilized by first responders, and to review, identify & categorize different types of ublic safety data needed, as well as examine how these data types influence cybersecurity of these mobile applications.[10]

---

[7] Ibid, p. 44.
[8] Schwartz, Heather L., Rajeev Ramchand, Dionne Barnes-Proby, Sean Grant, Brian A. Jackson, Kristin J. Leuschner, Mauri Matsuda, and Jessica Saunders, Can Technology Make Schools Safer?. Santa Monica, CA: RAND Corporation, 2016. Accessed 26 May 2018. <https://www.rand.org/pubs/research_briefs/RB9922.html>, p. 6
[9] *MAPS.* Department of Homeland Security, August 1, 2014. Accessed 17 May 2018. <https://www.dhs.gov/maps>
[10] *Securing Mobile Applications for First Responders*. Science and Technology Directorate, Department of Homeland Security, 2017. Accessed 29 May 2018.

The Integrated Public Alert & Warning System Open Platform for Emergency Networks (IPAWS-OPEN), launched in 2012, is an IP-based network system which aggregates and disseminates government-issued alert messages through a variety of IPAWS-OPEN compliant channels using wireless networks and mobile broadband. Emergency management officials from various industries in the private sector, tribal authorities, federal, state, and city municipalities are able to apply for free access to IPAWS-OPEN.[11] One example of IPAWS-OPEN compliant channel is the Wireless Emergency Alert (WEA) system which sends emergency alerts to members of the public who utilize "wireless phones and other enabled mobile devices to receive geographicallytargeted, text-like messages alerting them of imminent threats to safety in their area."[12] WEA is the result of a collaborative partnership between the Federal Emergency Management Agency (FEMA), Federal Communications Commission (FCC), and wireless industry companies. Wireless companies, such as AT&T, T-Mobile, Verizon, etc., volunteer to participate in WEA to enhance public safety.[13] Members of the public receive messages regarding critical emergency situations such as alerts issued by the President, those involving imminent threats to safety or life, and Amber Alerts. IPAWS-OPEN engages the private sector through the Alert Origination Software Providers (AOSP) in order to furnish software interface (mobile and cloud-based software applications) used by public safety and emergency officials to send emergency alerts.[14] One example of this software platform is AlertSense, which serves both private and public sectors, and is IPAWS-OPEN enabled. AlertSense is a cloud-based crisis management and

---

<https://www.dhs.gov/sites/default/files/publications/Securing%20Mobile%20Apps%20for%20First%20Responders%20v13_Approved_Final_508.pdf>, p. 1.

[11] *Integrated Public Alert & Warning System Open Platform for Emergency Networks*. Federal Emergency Management Agency, Department of Homeland Security, 2012. Accessed 29 May 2018. <https://www.fema.gov/integrated-public-alert-warning-system-open-platform-emergency-networks>

[12] *Wireless Emergency Alerts – FAQ*. Federal Communications Commission, January 2018. Accessed 24 May 2018. < https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea>

[13] Ibid.

[14] Alert Origination Software Providers. Federal Emergency Management Agency, Department of Homeland Security, 2018. Accessed 29 May 2018. <www.fema.gov/alert-origination-service-providers>

collaboration platform aimed for enterprise, small-to-midsized businesses, and government. It provides "real-time multi-lingual collaboration, simplifies incident reporting with automated escalation paths and transforms crisis management plans into actionable, personally relevant task lists & information at each user's fingertips."[15]

Inoperability or the ability to share information across platforms in an effective and efficient manner is a key strategic goal outlined by the NECP for emergency communications.[16] This means that data and information are shared across organizations such as the police department, fire department, emergency medical services (EMS), hospitals and other relevant agencies. "Achieving interoperability is a question of designing techniques to make several platforms communicate in the manner that is essential for organizations to collaborate and coordinate."[16] The National Incident Management System (NIMS) Communications and Information Management Standards provide a number of recommended standards for common interfaces, systems, and procedures, and data management systems to align disparate organizations and agencies. For instance, the Common Alerting Protocol (CAP) is the standard used for consistent alert messages to be disseminated simultaneously over various systems, which optimizes critical alerts over IPAWS-OPEN and IPAWS-OPEN enabled platforms and devices. Standardized use of CAP can ensure that messages are translatable for a variety of different media: over cable broadcasting, amber alerts, digital voice formats for radio and telephone, and signals for alert sirens.[17] In addition to CAP, NIMS outlines a standard for Emergency Data Exchange Language (EDXL) Distribution Element. For example, a CAP message

---

[15] "About AlertSense." AlertSense - Crisis Management and Collaboration Platform in the Palm of Your Hand (blog), July 31, 2015. Accessed 24 May 2018. <https://www.alertsense.com/company/about-us> [16] NECP, p. 3

[16] Luzeaux, Dominique, and Jean-Rene Ruault, eds. *Systems of Systems*. London : Hoboken, NJ: ISTE ; Wiley, 2010, p. 198.

[17] *NIMS Doctrine Supporting Guides & Tools*, p. 5

may be sent to a targeted audience as a payload using EDXL-DE, where data can be sent as an XML message, spreadsheet, jpeg image and other forms of digital data to targeted populations (general public or first responders).[18]

The increasing use of mobile broadband technology, cloud computing, and other emerging technologies underscore the need for comprehensive and coordinated approach of aligning people and processes in addition to adopting an integrated approach to adopting communications technologies. CSSP, or the Communications Sector-Specific Plan, highlights the interdependency of Emergency Services within the Communications Sector through wireless and broadband connectivity, LMR systems and networks, and through public alert & warning systems.[19] CSSP also outlines the engagement and outreach from both the public and private sectors, tribal governments, city/federal governments in promoting further collaboration across the emergency services enterprise.

The failure of Hawaii Emergency Management Agency (HI-EMA) in implementing ballistic missile alert (BMA) exercise in January 2018, however, exposes significant risks and vulnerabilities within the Emergency Services Sector despite movement towards adoption of integrated communication platforms. According to CNN, an employee had "pushed the wrong button"[20] which triggered a real BMA emergency alert system to be sent state-wide, rather than message indicating a drill exercise internally. It took HI-EMA thirty-eight minutes to send corrective information and to inform the rest of the state that the BMA message was a false alarm. A follow-up report sponsored by the Federal Communications Commission (FCC) identified three vulnerabilities: human factors, poor design interface of emergency systems

[18] Ibid, p. 6.
[19] *Communications Sector-Specific Plan*, p. 9
[20] CNN https://www.cnn.com/2018/01/14/us/hawaii-false-alarm-explanation/index.html
[22] Hawaii Gov Report

platform, and insufficient management controls.[22] In this report, the investigator details the timeline of events after the initial BMA was sent, subsequent procedures followed according to protocol, as well as the use of AlertSense, the software platformed mentioned in this paper previously.

Making affordances for human fallibility by implementing a strong internal controls framework is essential to the adoption of emerging technologies to transform emergency communications. For example, the HI-EMA employee responsible for incorrectly "pushing the button" became unresponsive as the situation progressed, which led to a coworker to step in to make the necessary steps required. In "The Human Factor within Context of Systems of Systems" from *Critical Infrastructure*, Jean-René Ruault, the employee's state implies information overload, which refers to the impact of information overload in an individual's ability to make timely and accurate decisions. The heightened pressure compounded by information overload often lead to delay in making decision, inaccurate decisions (if any), or none at all.[21] The presentation of information through user-friendly interface can also contribute to information overload and been reported to have contributed to the poor execution of BMA alert procedures. Perhaps the most surprising, yet revealing, evidence from the report is the lack of appropriate internal controls in the form of two-person confirmation procedure (as a "checks and balances" protocol) which would have prompted a secondary approval process for active non-exercise emergency alerts. An intuitive user interface or alert mechanism requesting confirmation of the action (whether through entering a supervisor's password or typing "yes" or "no") may have provided an additional layer of security to prevent

[21] "The Human Factor within Context of Systems of Systems" from *Systems of Systems*, Jean-René Ruault, p. 193.

inadvertent actions. In addition to layered security through a checks and balances protocol and two-factor authorization, significant emphasis on adequate professional development and training, consistent monitoring and evaluation of protocols and Standard Operating Procedures (SOP) are critical to improving HI-EMA's internal controls environment.[22]

Adoption of mobile technologies with no alternative alerting mechanisms can have deleterious impacts on these populations, particularly in the event of crisis, natural, and/or man-made disasters. Potential displacement and isolation of low-income communities for the sake of advancing technology adoption without alternatives can be found in recent news of the New York Metropolitan Transportation Agency (MTA)'s plans to implement mobile transactions and discontinue the use of MetroCard to ride the

NYC subways. Although there are plans to allow options for those who don't have either a mobile device or a credit card,[23] the challenge of providing adequate access may require some monitoring and oversight.

While both WEA and IPAWS-OPEN have widespread reach, and the system can enable location-specific messages, WEA and the use of mobile technologies can isolate low-income, homeless, aging populations, and/or those with Limited English Proficiency (LEP) who may not own or have access to wireless phones and other enabled mobile devices, or who live in areas with sparse wireless network. A Pew Research Center survey correlates internet non-adoption

---

[22] "False Alarm Incident's Internal Investigation Complete, Release of Results and Actions." Hawaii Emergency Management Agency, January 29 2018. Accessed 29 May 2018. <http://dod.hawaii.gov/hiema/false-alarm-incidents-internal-investigation-complete-release-of-results-andactions>

[23] Furfaro, Danielle. "MTA Gets ready to dump the Metrocard." New York Post. 20 October 2017. Accessed 30 May 2018. <https://nypost.com/2017/10/20/mta-gets-ready-to-dump-the-metrocard> [26] Anderson, Monica, Perrin, Andrew, and Jiang Jing Jing. "11% of Americans don't use the internet. Who are they?" Pew Research Center. 5 March 2018. Accessed 31 May 2018. <http://www.pewresearch.org/fact-tank/2018/03/05/some-americans-dont-use-the-internet-who-are-they>

to various demographic variables, such as age, educational attainment, household income and community type.[26] According to this survey, seniors are most likely not to go online. Furthermore, broadband and smartphone adoption for urban and rural populations are not equal, and whites, blacks and Hispanics are all equally likely to be offline.[24] Broadband services in rural communities, and some urban areas, can also vary because they lack the proper infrastructure for high-speed internet, and are often slower than non-rural areas.[25] But even in urban areas, discrimination against lower-income neighborhoods in deployment of home Internet and video technologies pose risk of service disruption due to inadequate mobile and cable broadband infrastructure, and is deemed evidence of "digital redlining."[26] According to the report by the National Digital Inclusion Alliance, for the past decade, AT&T has systematically discriminated against lower-income Cleveland neighborhoods. Citizens in these neighborhoods receive uneven and limited internet access, and in the event of emergency or crisis, their access to critical information may be severely impacted.

Greater dependence on cyber infrastructure can both improve and augment emergency communications through the adoption of mobile and wireless broadband, and the integrated approach in ensuring collaboration across agencies and institutions, as well as implementing effective and efficient data and information sharing practices. However, without strong internal controls and focus on human factors in achieving overall systems design of the future of emergency communications, emergency management agencies, such as HI-EMA, can pose a

---

[24] Ibid.

[25] Perrin, Andrew. "Digital Gap between rural and nonrural America persists." Pew Research Center. 29 May 2017. Accessed 31 May 2018. <http://www.pewresearch.org/fact-tank/2017/05/19/digital-gapbetween-rural-and-nonrural-america-persists>

[26] Callahan, Bill. "AT&T's Digital Redlining Of Cleveland." National Digital Inclusion Alliance. May 27, 2017. Accessed 30 May 2018. <https://www.digitalinclusion.org/blog/2017/03/10/atts-digital-redlining-ofcleveland>

high risk, and high impact scenario. In addition, thoughtful design and collaboration are essential in improving broadband infrastructure servicing vulnerable and rural populations, to ensure that critical information amidst crisis and emergency situations reach the people who need it most.

Works Cited

Alert Origination Software Providers. Federal Emergency Management Agency, Department of Homeland Security, 2018. Accessed 29 May 2018. <www.fema.gov/alertorigination-service-providers>

Anderson, Monica, Perrin, Andrew, and Jiang Jing Jing. "11% of Americans don't use the internet. Who are they?" Pew Research Center. 5 March 2018. Accessed 31 May 2018. <http://www.pewresearch.org/fact-tank/2018/03/05/some-americans-dont-use-theinternet-who-are-they>

"About AlertSense." AlertSense - Crisis Management and Collaboration Platform in the Palm of Your Hand (blog), July 31, 2015. Accessed 24 May 2018. <https://www.alertsense.com/company/about-us>

"About AlertSense." *AlertSense - Crisis Management and Collaboration Platform in the Palm of Your Hand* (blog), July 31, 2015. <https://www.alertsense.com/company/aboutus/>

"AlertSense IPAWS." AlertSense - Crisis Management and Collaboration Platform in the Palm of Your Hand (blog), July 31, 2015. Accessed 24 May 2018. <https://www.alertsense.com/alertsense-ipaws>

Callahan, Bill. "AT&T's Digital Redlining Of Cleveland." National Digital Inclusion Alliance. May 27, 2017. Accessed 30 May 2018. <https://www.digitalinclusion.org/blog/2017/03/10/atts-digital-redlining-of-cleveland>

Common Alerting Protocol. Department of Homeland Security. Accessed 30 May 2018. <https://www.fema.gov/media-library-data/1450108807753-9a5ba3b082b719d9a63d54b500df8193/CAP_Implementation_Fact_Sheet_2016.pdf>

Communications Sector-Specific Plan. Department of Homeland Security, 2015. 30 May 2018. < https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications2015-508.pdf>

"False Alarm Incident's Internal Investigation Complete, Release of Results and Actions." Hawaii Emergency Management Agency, January 29 2018. Accessed 29 May 2018. <http://dod.hawaii.gov/hiema/false-alarm-incidents-internal-investigationcomplete-release-of-results-and-actions>

Furfaro, Danielle. "MTA Gets ready to dump the Metrocard." New York Post. 20 October 2017. Accessed 30 May 2018. <https://nypost.com/2017/10/20/mta-gets-readyto-dump-the-metrocard>

IPAWS. Federal Emergency Management Agency, Department of Homeland Security, 2014. Accessed 29 May 2018. <https://www.fema.gov/media-library/resourcesdocuments/collections/381>

Integrated Public Alert & Warning System Open Platform for Emergency Networks. Federal Emergency Management Agency, Department of Homeland Security, 2012. Accessed 29 May 2018. <https://www.fema.gov/integrated-public-alert-warning-systemopen-platform-emergency-networks>

Luzeaux, Dominique, and Jean-Rene Ruault, eds. *Systems of Systems*. London : Hoboken, NJ: ISTE ; Wiley, 2010.

MAPS. Department of Homeland Security, August 1, 2014. Accessed 17 May 2018. <https://www.dhs.gov/maps>

National Emergency Communications Plan. Department of Homeland Security, 2014. Accessed 17 May 2018. <https://www.dhs.gov/sites/default/files/publications/2014-1107%20-%20NECP%20Slick%20Sheet_0.pdf>

NIMS Doctrine Supporting Guides & Tools. Federal Emergency Management Agency, Department of Homeland Security, 2014. Accessed 26 May 2018. <https://www.fema.gov/nims-doctrine-supporting-guides-tools>

Perrin, Andrew. "Digital Gap between rural and nonrural America persists." Pew Research Center. 29 May 2017. Accessed 31 May 2018. <http://www.pewresearch.org/fact-tank/2017/05/19/digital-gap-between-rural-andnonrural-america-persists>

Securing Mobile Applications for First Responders. Science and Technology Directorate, Department of Homeland Security, 2017. Accessed 29 May 2018. <https://www.dhs.gov/sites/default/files/publications/Securing%20Mobile%20Apps%20for%20First%20Responders%20v13_Approved_Final_508.pdf>

Schwartz, Heather L., Rajeev Ramchand, Dionne Barnes-Proby, Sean Grant, Brian A. Jackson, Kristin J. Leuschner, Mauri Matsuda, and Jessica Saunders, Can Technology Make Schools Safer?. Santa Monica, CA: RAND Corporation, 2016. Accessed 26 May 2018. <https://www.rand.org/pubs/research_briefs/RB9922.html>

Sidner, Sara and Andone, Dakin. "What went wrong with Hawaii's false emergency alert?". CNN. 18 January 2018. Accessed 29 May 2018. <https://www.cnn.com/2018/01/14/us/hawaii-false-alarm-explanation/index.html>

Wireless Emergency Alerts – FAQ. Federal Communications Commission, January 2018. Accessed 24 May 2018. < https://www.fcc.gov/consumers/guides/wireless-emergencyalerts-wea>