NIST Special Publication 1900-203

Global City Teams Challenge Public Safety SuperCluster Progress Report 2018-2019

Brenda Bannan
Samantha Dubrow
Michael Dunaway
Sokwoo Rhee
Dean Skidmore
Elisa Torres

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-203

CYBER-PHYSICAL SYSTEMS

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1900-203

Global City Teams Challenge Public Safety SuperCluster Progress Report 2018-2019

CYBER-PHYSICAL SYSTEMS

Brenda Bannan
Samantha Dubrow
George Mason University

Michael Dunaway
University of Cincinnati

Sokwoo Rhee
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

Dean Skidmore
IoT+LTE Consulting Group

Elisa Torres
George Mason University

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-203

March 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication Series 1900-203
Natl. Inst. Stand. Technol. Spec. Publ. 1900-203, 23 pages (March 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-203

TABLE OF CONTENTS

TABLE OF FIGURES

Executive Summary

The National Institute of Standards and Technology (NIST) Global City Teams Challenge (GCTC) is a collaboration forum for developing and deploying replicable, interoperable, and scalable cyber-physical systems and Internet of Things (IoT) solutions in cities and communities around the globe. With the goal of improving the quality of life of residents using emerging technologies, the GCTC program has identified and nurtured over 200 smart city projects over the course of five years and created nine working groups (i.e., SuperClusters) that cover several application domains to produce documents containing best practices and case studies. The GCTC program has evolved into a successful collaboration space for cities, communities, industry, and academic stakeholders to discuss, collaborate, develop, and document their accomplishments and share their experiences.

In 2018, NIST and the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) co-hosted the GCTC program under the subtitle "Smart and Secure Cities and Communities Challenge (SC3)." The SC3 program was designed to encourage stakeholders to take cybersecurity and privacy as primary concerns and to identify examples and approaches for enabling designed-in security to be seriously considered in developing and deploying smart city solutions.

The Public Safety SuperCluster (PSSC) covers topics such as emergency response, disaster resilience and recovery, emergency communication systems, and flood prediction and management. This report provides a high-level summary of two significant events and accomplishments of the PSSC: the joint participation with the Cybersecurity and Privacy Advisory Committee (CPAC) in a workshop at NIST, Gaithersburg, Maryland, USA, in late 2018 and a live simulation exercise of emergency response at the George Mason University in late 2019, the first in a planned series of use cases and pilot studies of PSSC technology applications and research projects.

Public Safety SuperCluster and NIST hosted a workshop on October 29–30, 2018, in collaboration with CPAC, to bring together a broad range of stakeholders to discuss the latest developments and challenges in public safety and the implementation of smart city technologies to improve public safety. The workshop also covered cybersecurity and privacy in emerging, smart city technologies. Representatives from municipal governments, corporations, federal government agencies, and academic institutions with an interest in public safety, cybersecurity, and privacy participated in the workshop. This report provides a summary of the presentations and discussions held at the event.

The first day of the workshop included a series of presentations and panel discussions by invited speakers, including first responders and government agencies. The first day also featured breakout sessions that discussed the PSSC blueprint/playbook and examples of a reference architecture for public safety systems and first responder priorities to guide research and development in smart public safety. The second day focused on the issues and challenges in cybersecurity and privacy as emerging technology solutions are deployed in cities and communities. The breakout sessions on the second day covered additional topics, including IoT security and global perspectives on cybersecurity.

Building on the results of the workshop, PSSC and CPAC increased their engagement with municipal governments and technology innovators to further encourage their collaboration and successful deployment of secure, privacy-aware, and interoperable solutions in the municipal environment, including a live simulation exercise of emergency response conducted at the George Mason University in partnership with Fairfax County, Virginia, in November 2019.

1. Introduction

A smart city or smart community uses advanced technologies to improve quality of life for its residents. Smart cities are distinguished by cyber-physical systems (CPS) and the Internet of Things (IoT), which connect the built environment — comprising systems such as transportation, telecommunications, electrical power, water distribution and management, public health and safety, commerce, and housing — to enhance the quality of the overall living environment and better manage its impact on the natural environment. This is achieved through interconnected "smart devices," i.e., sensors, data collection processes and protocols, and communications media such as ubiquitous wireless access, in fundamentally new ways to achieve economies of scale and efficiencies that are essentially unattainable through traditional city planning and management processes. When applied to diverse public service sectors in a well-regulated and deliberate fashion, these technologies enable cities and communities to improve services, promote economic growth, and enhance the quality of life.

Cyber-Physical Systems

Cyber-physical systems comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

Cities and communities across the globe are increasingly seeking smart, connected solutions as a way to meet the needs of growing populations. Cyber-physical systems and the integration of data analysis with ubiquitous wireless communications will play a key role in these solutions. Hundreds of cities and dozens of technology providers are working independently on innovative, smart cyber-physical systems across a broad range of services and markets. This is leading to a proliferation of customized solutions, as well as many different proposed standards and protocols. Assuring the interoperability of these and future systems will be challenging in this rapid-growth scenario. Through its CPS Public Working Group,[1] the National Institute of Standards and Technology (NIST) brought together technical experts in an open public forum to help define and shape key characteristics of CPS. In 2017, NIST published its CPS Framework, Release 1.0,[2,3,4] which presents an analysis methodology centered on the concerns about CPS and supports understanding and development of new and existing CPS, including those designed to interact and function in multiple interconnected environments. This analytical foundation also provides supporting principles to develop comprehensive standards and metrics for CPS to support commerce and innovation.

The NIST Global City Teams Challenge (GCTC) is a federal program that has facilitated a broad public–private collaboration of cities, technology developers and commercial entities, research institutes and universities, and private citizens who share a common dedication to developing efficient strategies for technology development and integration of smart city solutions and contribute to the standardization and interoperability of cyber-physical systems for use in communities across the globe. In a closely related effort, NIST convened the International Technical Working Group on Internet of Things-Enabled Smart

[1] https://pages.nist.gov/cpspwg/
[2] NIST Special Publication 1500-201. Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf.
[3] NIST Special Publication 1500-202. Framework for Cyber-Physical Systems: Volume 2, Working Group Reports, Version 1.0, June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf
[4] NIST Special Publication 1500-203. Framework for Cyber-Physical Systems: Volume 3, Timing Annex, Version 1.0, September 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-203.pdf

City Framework (IES-City Framework)[5] to help develop a common architectural framework for smart city solutions.

1.1. Overview of the GCTC Program

In 2013, the smart city technologies market was fragmented, with each city developing its own smart city plans based on an isolated understanding of the requirements of a smart city. Further, cities and communities facing common issues did not typically communicate with each other to share their requirements, which led many communities to "reinvent the wheel" to address issues that might have been already solved by others. As a result, many communities and technology providers developed custom-tailored solutions directed at solving common issues such as traffic congestion, flood monitoring, environmental monitoring, and water quality management. Under this approach, neither municipal governments nor industry stakeholders were able to enjoy economies of scale. In keeping with its mission to promote U.S. innovation and industrial competitiveness, NIST launched the GCTC program to identify and nurture replicable, scalable, and sustainable best practices for smart city solutions that can be shared by large numbers of cities and communities dealing with common issues. Since its inception in 2014, the GCTC program has included over 200 collaboration projects (called "Action Clusters"), led by teams of municipal governments and technology innovators such as companies, research universities and centers, and non-profit organizations. Through this process, over 200 municipal governments and 500 technology organizations joined forces to address common issues communities are facing around the world. A description of the program and its impacts can be found in NIST Special Publication 1900–01.[6] In its 2018–2019 round, NIST partnered with the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) to co-host the GCTC program. The National Telecommunications and Information Administration (NTIA) later joined as the third co-host of the 2019 GCTC Expo.

Long Term Goals for GCTC

To establish and demonstrate ways to incubate and deploy smart, secure, standards-based technology solutions that take advantage of the Internet of Things, Cyber-Physical Systems, advanced computing, and connected devices to provide measurable benefits in cities and communities.

The GCTC program also encouraged Action Clusters in the same application domain to collaborate under the umbrella of "SuperClusters," which are public–private working groups composed of Action Clusters and additional local governments, nonprofit organizations, academic institutions, technologists, and corporations from all over the world with shared interests in the same topic. GCTC hosts workshops and global Expo events that bring together over a thousand municipal officials and IoT/smart city stakeholders to share their experiences and demonstrate replicable and scalable solutions. The GCTC Expo is the largest smart city/IoT event hosted by the U.S. federal government. The GCTC program has evolved into a broad public–private partnership that includes multiple federal agencies and hundreds of municipal governments

[5] International Technical Working Group on IoT-Enabled Smart City Framework website. Available at https://pages.nist.gov/smartcitiesarchitecture/

[6] Global City Teams Challenge 2016. June 2017. NIST Special Publication 1900–01. Available at https://doi.org/10.6028/NIST.SP.1900-01

and private sector stakeholders. A description of the existing SuperClusters and Action Clusters and information about past events are available on the GCTC website.[7]

1.2. Purpose of this Publication

In its 2018–2019 round, NIST and DHS S&T co-hosted the GCTC Smart and Secure Cities and Communities Challenge (SC3) program. The objective was to encourage participating teams to include cybersecurity and privacy as integral project elements alongside goals such as replicability, scalability, sustainability, and interoperability of technologies and systems. In parallel, GCTC's Public Safety SuperCluster (PSSC) sought to bring together domain experts in public safety to discuss the latest issues and developments and to explore designed-in cybersecurity and privacy for public safety solutions.

This report highlights two significant accomplishments of the PSSC:

First, this report describes in detail the workshop hosted by PSSC and NIST in October 2018 to address the latest progress and plans of the Public Safety SuperCluster and, further, to initiate an active collaboration with the Cybersecurity and Privacy Advisory Committee (CPAC) to begin incorporating the dimension of cybersecurity into the PSSC effort. This section describes presentations and group discussions around shared perspectives on the latest developments in public safety and cybersecurity for smart cities and communities. The workshop provided a foundation for PSSC's activities in 2019.

Secondly, this publication includes a summary of the first in a planned series of reports on use cases, technology demonstrations, and exercise summaries involving the work and outcomes of PSSC Action Clusters and Public Safety-related efforts in GCTC communities. It highlights a significant demonstration in November 2019 of a live simulation-based, multi-team training exercise in Mass Casualty Incident (MCI) response that was conducted by the GCTC research team from the George Mason University in collaboration with Fairfax County, Virginia, first responder agencies.

[7] Global City Teams Challenge website. Available at https://pages.nist.gov/GCTC/

2. 2018 PSSC/CPAC Workshop

2.1. Background

In October 2018, the Public Safety SuperCluster (PSSC) of the Global City Teams Challenge (GCTC) held a dedicated workshop at the NIST campus in Gaithersburg, Maryland, USA.[8] The conference was an initial attempt to bring together members of the PSSC Action Clusters—i.e., those Action Clusters whose smart city projects were related to the broad effort to improve public safety within their communities—with members of other SuperClusters with related technologies or collaborations, as well as the broader GCTC and SuperCluster leadership teams. The specific goals of the workshop were to conduct a focused review of the latest PSSC-related projects and to initiate a broad discussion among members about the common themes and challenges that the PSSC Action Clusters have encountered.

"Public safety" is a term that most often invokes references to first responder agencies, i.e., law enforcement, firefighting, emergency medical services (EMS), emergency management, and, more recently, public alerting systems and Public Safety Access Points (PSAPs; e.g., 911 call systems and similar technologies). These services and the integration of new technologies that serve the first responder community have been a central focus of the PSSC from the outset. However, the PSSC has purposely adopted a broader definition and approach to public safety and has included efforts to improve the overall resilience and disaster-resistance of communities, as well as the ability of smart cities to integrate new technologies dedicated to public safety. This overall approach is reflected in the "Blueprint for Smart Public Safety in Connected Communities," published by the PSSC in August 2017 and updated in July 2019.[9] This document describes the formation of public–private partnerships for enhancing public safety, the development of strategies for overall community resilience, and the adoption of a more holistic "Whole Community Approach" as a foundation for public safety in smart cities.

Since its formation, the PSSC membership has held the view that an integrated, holistic approach to public safety should be the foundation of the general concept of a "smart city" and that technology development and deployment of systems for improving public safety should be approached with the goal of enhancing interoperability with other smart city platforms. Among first responders, the terms "blue sky" and "dark sky" distinguish between non-crisis times. "Blue-sky" describes days when crew and team training, table-top exercises, rehearsals, and general system and equipment maintenance can be conducted, while "dark-sky" events involve real-world crises or disasters, when first responder agencies are deployed in their primary life-saving missions. The blue sky/dark sky dichotomy is equally valid for development of smart city technologies from the perspective of cost-savings and economies of scale, which must be achieved if new smart city technologies can be made affordable.

Another guiding principle within the PSSC is that improvements in public safety technologies and concepts must be fully interoperable or compatible with legacy systems currently in use, since existing public safety technologies must maintain fully operational capability even as new systems are developed and brought into use. This is a particular challenge for first responders, for whom additional training and familiarization is often required with new systems, and is also a challenge for the broader community in terms of avoiding

[8] https://www.nist.gov/news-events/events/2018/10/gctc-smart-and-secure-cities-and-communities-challenge-public-safety
[9] https://pages.nist.gov/GCTC/uploads/blueprints/2019-PSSC_Blueprint_201907005.pdf

potential loss of capability or efficiency during the transition period. These were some of the challenges that motivated the PSSC to initiate a dedicated workshop in October 2018.

Finally, given the significant threat and liabilities that are emerging from cyberattacks and intrusions in civilian information management and communications systems, the PSSC Workshop joined with the GCTC Cybersecurity and Privacy Advisory Committee (CPAC) to begin addressing the challenges and integration of cybersecurity into the general approach of the PSSC to the broad considerations of public safety.

2.2. Workshop Scope and Format

As a continuation of the discussion from the February 2018 GCTC/SC3 Conference,[10] the PSSC convened in October 2018 to conduct a dedicated discussion regarding the integration of public safety technologies and strategies for smart cities. The conference consisted of two days of events, including several keynote addresses from federal agency sponsors and research institutes, followed by targeted breakout sessions to address the latest challenges and future strategies.

A series of plenaries and panels were conducted throughout the event to provide federal, state, and regional perspectives and inform participants about the key trends in public safety, cybersecurity, and privacy that are impacting cities and communities across the globe.

On the second day of the workshop, the keynotes and breakout sessions were directed at the specific challenge of integrating cybersecurity into public safety, both as a security concern of growing importance for communities and businesses and as it pertains to the hardening and protection of first responder technologies (i.e., data systems, interoperable communications, and computer-aided dispatch systems). In the end, the workshop identified an agenda and approach for the future work of the PSSC.

2.3. Public Safety in Smart and Connected Communities, Day 1: A Whole-Community Approach

The first day of the workshop was focused on the theme "Public Safety in Smart and Connected Communities: A Whole-Community Approach." The day began with a keynote address from David Kaufman, CNA, followed by a first responder panel addressing questions about the priorities for smart and connected communities from the first responder perspective. Then, multiple groups broke out to discuss specific interests before reporting back to the full conference community. Summaries of key takeaways from the two discussion groups, the PSSC Blueprint and First Responder Priorities, are provided in this report, which reviews the information that was presented, cites lessons learned, and offers future considerations for public safety stakeholders in the context of smart cities and communities.

2.3.1. Keynote: Priorities for Smart and Connected Communities

The kickoff presentation for the workshop was the keynote speaker, David J. Kaufman, Vice President of Safety and Security at CNA. Kaufman focused on the future of community risk and resilience and explained challenges for the future given the changing nature of global public safety.

[10] https://pages.nist.gov/GCTC/event/gctc-kickoff-2018/

Kaufman highlighted the growing population, particularly in urban areas that are expanding at the rate of 1.5 million people per week (PwC Analysis[11]). He noted that the population is also growing, aging, and diversifying and that nations and communities are facing new health issues, such as the increase in antimicrobial resistance and the long-term effects of chronic and non-communicable conditions. Kaufman argued that the global economy is changing, with stagnant, if not declining, incomes in advanced economies. His presentation indicated that at the same time, our infrastructure is under stress, including bridges, roads, dams, and wastewater management. In its 2017 Infrastructure Report Card, the American Society of Civil Engineers[12] indicated that one out of every eleven bridges in the U.S. is structurally unstable and that the need for wastewater infrastructure improvements exceeds $271 billion.

Kaufman also described that along with the environmental, economic, infrastructure, climate, and human population changes and challenges, technology in all fields is advancing at a rapid rate. According to him, technological advancements are increasing the speed and breadth of information flow, and hyper-connectivity is revolutionizing development cycles across the world in nearly all industries. In his view, this hyper-connectivity and speed of information flow is drastically changing how we consume information, and it is becoming increasingly challenging to identify misinformation and to know what sources to trust. He emphasized that even reliable information is so vast that individuals and organizations are suffering from information overload and tasked with challenging decisions regarding what sources and information to prioritize.

The speaker believed that along with all these changes, however, trust in government remains strong at the local level. Additionally, he argued that the power and influence of non-state actors is growing to include non-governmental organizations (NGOs) and volunteers.

The speaker emphasized that changes in the environment are closely related to changes in public safety concerns. According to Kaufman, we are facing increased complexity and decreased predictability, and more events are becoming interrelated with advancements in technology and increased information flow. In sum, he noted, a major challenge is that when a public safety event occurs, a much more widespread group of people are immediately informed and come to help but very few people stay involved when the event dissipates but continued help is needed. Thus, one challenge is the need to engage those who are willing to help and keep them involved over the long term.

Kaufman's presentation provided the conference with a summary of many issues and changes in the environment to consider when addressing public safety. Throughout the conference, these issues were used as a reference point to be considered during more specific presentations and working sessions. To summarize, Kaufman argued that the environment in which public safety operates is characterized by increased dynamism and that a key goal for the field of public safety is to recognize and acknowledge the changes and the trends driving the changes to increase the ability to forecast and prepare to respond to future events. The keynote brought up important questions, including: How will public safety be delivered in the future? Who will be in charge of such delivery? What new value can innovation provide? What challenges will we face due to innovation? How will technology enable innovation? How will technology establish new threats to innovations? And what are the competencies required for public safety professionals to best address the changing future?

[11] PwC UK: Rapid urbanisation https://www.pwc.co.uk/issues/megatrends/rapid-urbanisation.html
[12] https://www.infrastructurereportcard.org/

2.3.2. First Responder Panel: Priorities for Smart and Connected Communities

The first responder panel included former Baltimore City Fire Chief Ray Lehr; Fairfax Fire Department Assistant Chief Jason Jenkins; Maryland Emergency Management Agency Preparedness Branch Manager Brian Bauer; former Deputy Director of the Cybersecurity Division of the Department of Homeland Security (DHS) Scott Tousley; and National Science Foundation (NSF) Program Director David Corman. The primary focus of the first responder panel was on public safety resilience.

The panel noted that planning for first responders includes coordinating with communications and data groups, discovering privacy requirements and challenges, and connecting to external peers in similar positions and to potential data sources. Connections across agencies to allow for the pervasive use of data and information as a continuously available resource was highlighted as a valuable source for first responders.

Echoing the keynote address, panelists highlighted that first responders tend to connect more easily with community partners than with the government. For example, panelists argued, because fire response often consists of volunteers, first responders have found that volunteers are more likely to accept ideas from other volunteers than from governing bodies.

Looking to the future, now that patient care records are electronic and handheld devices are becoming increasingly powerful, panelists noted that it is becoming easier to interact and share intelligence with others. They also noted that since there are many smartphone applications that could be used to enhance public safety, it is not easy to guarantee cybersecurity, consistency of quality, and potential interoperability of programs. These applications are typically not regulated against a single standard, and such fragmentation makes it difficult for first responders to choose which ones to utilize.

The panel also briefly discussed the challenges that have come with the opioid epidemic. They pointed out that while operational command centers are relatively well connected and informed, citizen engagement is still an issue, and future work regarding the opioid epidemic should boost communications with citizens and residents in need of help.

Participants noted that there is a growing trend that individuals are becoming less sensitive about situational awareness of their environmental and personal safety, and to counter this issue, first responders are actively teaching people how to take care of themselves, their families, and their communities in various situations. For example, first responders are educating civilians to become more proactive and self-sufficient in increasing situational awareness around personal safety. The panel argued that this education around self-awareness is becoming increasingly important as we become more reliant on smart and connected devices for communication. The panel also noted that when communities have a better understanding of the situation and trust first responders, first responders are more easily able to engage with the community when it is necessary

According to the panel, the level of understanding and use of technology by residents has a major impact on how smart technologies can be leveraged for public safety, including the capabilities for information sharing and collaborating across public safety stakeholders. In addition to the concerns around citizen engagement, there are also technological concerns around the lack of interoperability that may impede collaboration between relevant agencies and stakeholders.

At the end of the panel, David Corman (NSF) challenged the audience to think beyond deploying technology that was already available and to continue research on community engagement and future technologies that could improve public safety and security through smart cities and communities.

In summary, the panel noted that science and technology are progressing rapidly and government agencies and partnering organizations are working closely in developing the requirements for successful smart and connected cities, community engagement with first responders is growing, and trust and situational awareness are being built. The main takeaway from the panel is that all technologies, communications, and efforts related to public safety need to be developed and considered based on current real-world scenarios, not abstract and unrealistic potential scenarios.

2.3.3. *Discussion Group 1: PSSC Blueprint and OGC Reference Architecture*

The first discussion group was directed by George Percivall, Chief Technology Officer and Chief Engineer of the Open Geospatial Consortium (OGC). Percivall began by reviewing the Open Geospatial Consortium's mission for creating a global forum for the collaboration of developers and users of spatial data products and services and advancing development of international standards for geospatial interoperability.

The group discussed the perils of allowing interoperability to be an afterthought when developing smart cities. A participant mentioned that 77% of Internet of Things experts had named interoperability as the biggest challenge currently facing IoT. The group noted that without interoperability, new technologies can be rendered useless and fail to be implemented. Percivall offered several indicators of potential interoperability failures for designing new smart city projects, including the need for custom integrations, high lifecycle costs, difficulties in rapidly mobilizing new capabilities, duplication of effort, difficulty in sharing critical data across departments in real time, and missed opportunities for improved decision-making. Percivall also noted that designing for interoperability requires developers and engineers to create solutions that are relatively inexpensive, scalable, able to interact with similar and complementary technologies, and able to easily and securely share data and information with relevant stakeholders.

The OGC Smart Cities Spatial Information Framework[13] whitepaper was presented during the group's meeting to aid discussion. Percivall mentioned the whitepaper provides a set of design resources that cities can use to build and implement interoperable solutions, including a common language to be used that can be understood by diverse stakeholders. Percivall also indicated it provides approaches for solving problems common in technological implementation and encourages designers to adhere to the common standards, specifications, and patterns set forth in the framework.

Finally, the group discussed three projects: (1) systEmic standardisation apPRoach to Empower Smart citieS and cOmmunities (ESPRESSO)[14] and the European Innovation Partnership for Smart Cities and Communities (EIP-SCC),[15] (2) Smart Cities India Plugfest, and (3) Smarty City Interoperability Reference Architecture (SCIRA)[16]. First, ESPRESSO is a European Commission project in which the OGC is involved, and the European Innovation Partnership for Smart Cities and Communities aims to improve urban life through more sustainable, integrated solutions and addresses city-specific challenges in areas such as energy, mobility and transport, and information and communications technology (ICT). The EIP-

[13] https://portal.opengeospatial.org/files/?artifact_id=61188
[14] http://espresso-project.eu/
[15] https://e3p.jrc.ec.europa.eu/articles/european-innovation-partnership-smart-cities-and-communities
[16] https://www.opengeospatial.org/projects/initiatives/scira

SCC's Urban Platform is intended to be used by developers, decision makers, and procurement officers to enable smart city initiatives to apply open standards in increasing innovation while avoiding vendor lock-in.

The group noted that ESPRESSO consists of four standards-development organizations: the Deutsches Institut für Normung (DIN), the European Telecommunications Standards Institute (ETSI), OGC, and the British Standards Institution (BSI), along with two cities: Rotterdam in the Netherlands and Tartu in Estonia. The Rotterdam pilot includes sensors connected to a 3D city model. The purpose of the Rotterdam pilot is to test the usability of open data standards (such as from OpenCity GML, BIM, WFS, and SensorThing API) and to test current working principles. The results utilizing multi-use sensor information thus far have made data available to the City of Rotterdam and regional educational institutions, companies, and startups focused on the data marketplace. In this example, vendor lock-in has been successfully avoided, and the sensor solution is not dependent on the applications or protocols of existing vendors. The approach also made the future procurement of additional sensors easier for new applications such as streetlights, parking space openings, and waste containers. The Tartu pilot integrated systems measure energy use to aid Tartu's goal of becoming Europe's most energy-efficient city.[17]

The second project, Smart Cities India Plugfest, is being sponsored by India's Department of Science and Technology (DST). DST's National Spatial Data Infrastructure serves as the data and data services provider. Smart Cities India Plugfest is currently working on four applications: water supply and wastewater management, watershed management, air quality, and health. Water supply and wastewater management should take into account the geospatial aspects of routine maintenance and planning for future water and waste infrastructure. The group noted that watershed management is a critical concern for cities that rely on surface water for their water supply. Air quality measurements in urban environment contexts are also being integrated. Finally, Smart Cities India Plugfest is also considering the monitoring of health and communicable diseases and the potential ties between health, water, and air quality.

Finally, the third project, OGC's Smart City Interoperability Reference Architecture (SCIRA), is an interoperability framework being used to integrate IoT sensors for public safety. SCIRA is being used to advance smart cities in terms of public safety, policing, and urban resilience by focusing on the utilization of open architectures of interoperable IoT devices and solutions. Currently, there is a lack of consensus regarding architectural concepts, leading to divergent and contradictory approaches that could cause problems with interoperability and limit the scalability of IoT technologies in the future.

The group noted that the goal of SCIRA is to produce architectures and deployment guides and to support implementation of future pilot testing. The initial version of SCIRA was based on a stakeholder workshop, landscape assessment, and the architecture viewpoint trade study, with inputs from the Solar Dynamics Observatory. The latest, more refined version of SCIRA has been additionally informed by an architecture views workshop, a hackathon for the identification of innovation functions, a deployment guides workshop, and a smart city pilot, in addition to other ongoing pilot deployments. The hackathon was used to uncover the complexities in four topics: intelligent buildings and first responder awareness, urban canyons and street sensors, critical infrastructure resilience and flood response, and neighborhood safety and common space engagement.

[17] https://www.geospatialworld.net/article/ogc-is-developing-and-applying-data-standards-for-urban-planning/

In summary, the first discussion group showed that interoperability is a critical component for the smart city effort and thus should be included as a top priority during the initial planning phases for new smart cities.

2.3.4. Discussion Group 2: First Responder Priorities for Smart Public Safety

Discussion Group #2 was led by George Mason University Associate Professor of Instructional Technology and Learning Technologies Dr. Brenda Bannan, Fairfax Fire Department Assistant Chief Jason Jenkins, and George Mason University doctoral candidate and research assistant in industrial-organizational psychology Samantha Dubrow.

The purpose of the First Responder Priorities session was to solicit ideas for new research and development based on the needs of first responders and to encourage technology partners to create new action clusters for the GCTC. The discussion was based on the experience of the George Mason University and Fairfax County Fire & Rescue research partnership.

Two scenarios were used as examples to elicit knowledge and feedback from Chief Jenkins regarding what first responders were doing, thinking, and feeling, as well as what their pain points, opportunities, and barriers were at each stage of an event. Two use cases, one involving a garden apartment fire and the other an active shooter, were discussed. Both events require fire, emergency medical services (EMS), and police to work together interdependently.

The session highlighted pain points and barriers, as well as opportunities, to consider during pre-planning, while en route to a scene, and on arrival. During the pre-planning phase, there is an opportunity to implement drones for use in daily routines to provide first responders with visual information such as building models or building layouts prior to their arrival on scene. En route technology has the opportunity to enhance situational awareness for responders. Similar to military units, any visual cues that can be given before walking onto a scene or into a building can be useful to enhance a shared understanding of the environment and to choose best tactics for response. En route access to the information control system and the ability for first responders to see whatever the security system is able to see would also be useful. There are possibilities for utilizing audio, video, physiological, and location-based data during a scenario and post-action reviews. A clear opportunity for improvement is the capability to visualize what is happening on different floors of a building and on what floors potential victims are located.

Participants in the discussion noted that once first responders arrive on scene, the primary goal is efficiency — i.e., rapidly understanding, engaging and controlling the situation at hand. There is a need to provide first responders with as much information as possible about the situation into which they are walking, whether there are living beings, and, if so, where they are. IoT possibilities include a head-mounted display that could provide critical visual information from cameras and any useful data to be visually delivered to responders as early as possible. There are many important future considerations regarding how much information, to whom, and when data should be transferred. Finally, there is an opportunity to monitor real-time biodata and physiological data of first responders to enhance their safety.

Participants also noted that during an incident response scenario, first responders typically paint pictures in their mind of what they expect the event to look like when they arrive on scene. Unfortunately, everyone's picture may not turn out to be the same. Participants suggested that first responder technologies should focus on allowing responders to understand what they are going into before they enter a building, without wasting any time. This would allow for enhanced situational awareness and shared mental models across

teams, allowing them to respond faster and more effectively. The goal is for information to be delivered as quickly as possible, while remaining digestible and interpretable. First responders face many environmental challenges, including high levels of noise, lack of visibility, limitations of communications access, and elevated temperatures too high for many sensors and video and audio recorders to withstand. Thus, it is important for technologists to have experience observing emergency response events or simulations and to interact directly with first responders to develop technologies that can improve performance within contextual constraints.

At the end of the session, future opportunities for technologies for first responders, specifically firefighters, were brainstormed. Ideas included smart speakers, video cameras in homes and apartments that can be shared like those in commercial buildings, helmets capable of capturing and sending video back to incident command in real time, physical building mapping technologies using drones, location sensors to signal where people are located in a burning building — specifically, on what floor — and smart smoke detectors capable of sending specific information to firefighters before they arrive.

To summarize, the major issues that emergency response technologies should aim to address are: helping responders to go into scenes better informed; providing visuals that are unobtrusive, using tools such as drones and helmet cameras; and creating backups through redundant communication channels. Technologists, researchers, and first responders should continue working together to better understand how much information, and in what format, can be easily digestible and interpretable before it becomes overwhelming and causes a potentially negative effect on performance. Moving forward, the group and the entire PSSC community are encouraged to consider implementation opportunities for wireless and unobtrusive technologies for first responders.

2.4. Cybersecurity and Privacy Workshop, Day 2

The second day of the workshop included keynote presentations from Mark Kneidinger regarding the DHS Cybersecurity Strategy, followed by Ron Ross on NIST's perspective on cybersecurity and Lan Jenson on the draft of the GCTC Cybersecurity and Privacy Guidebook. The plenary session was followed by breakout sessions for multiple discussion groups. In this section, the key takeaways from the three keynote speakers and two discussion groups are summarized.

2.4.1. Keynote: DHS Cybersecurity Strategy

Mark Kneidinger, Deputy Director, DHS National Risk Management Center, spoke about cybersecurity and privacy, stating that there is a need to have a national risk management center as cybersecurity risks cross the state, federal, and private sectors. Specifically, he noted, there is a need to examine national risk from a long-term and strategic perspective and to consider the interdependencies of entities across sectors. Cyber challenges should be examined collectively to identify the most immediate vulnerabilities and allow for proactivity about potential risks, working within and across agencies and both within and outside of the government.

Kneidinger explained that current DHS cybersecurity efforts include working across sixteen sectors in public and private domains to identify the critical functions that are most important across the sectors. He also noted that the effort is currently in the management stage, working to identify key functions and components that task forces will need to address. A number of gaps and future directions have been identified thus far, and collaboration across sectors is commonly needed.

In sum, this presentation recognized the need for the identification of national and critical functions for cybersecurity, along with the associated risks and interdependencies across such functions. Kneidinger noted that the National Risk Management Center is attempting to address these needs by creating task forces to work across sectors, that integration and collaboration across sectors will be the key to future cybersecurity, and that there is a strong need to consider and address issues collectively.

2.4.2. Keynote: NIST Perspective on Cybersecurity

Ron Ross, a NIST Fellow in the Information Technology Laboratory at NIST, gave a keynote address to review the landscape of cybersecurity. Ross noted that there are two types of issues in the world — issues that are critical and issues that are not — and that cybersecurity is to be considered a critical issue. Technological innovations are happening more rapidly than ever before, and computers are continually being pushed to the edge of their capabilities. He pointed out that if it is not possible to defend the technologies being created, risks of these new technologies may outweigh the potential benefits. Ross argued that there is a critical need to focus on cybersecurity and that it is imperative to act on the knowledge that these are critical functions.

Ross also noted that vulnerability in cybersecurity is partially driven by the fact that the attacker has the ability to choose the time, place, and intensity of the attack, without any prior knowledge by responders. The increasingly interconnected and vastly complex network of technology is also, in some ways, becoming easier to infiltrate. In essence, he argued that technological advancements are rapidly exceeding our ability to protect such technologies.

Ross indicated that cyberattacks are pervasive across industries ranging from energy to transportation to defense to manufacturing. In reality, it is impossible to protect all assets. Therefore, he pointed out, it is imperative to reduce potential attack surfaces using multidimensional strategies for cybersecurity incident response. For the attacks that will inevitably be successful, he suggested that the goal should be to make systems more resilient to limit damage. Dimensions of a system used to reduce susceptibility to cyber threats include hardening the target, limiting potential damage to the target, and making the target resilient.

According to Ross, the model of cybersecurity preparation is cyclical and includes steps to categorize, select, implement, assess, authorize, monitor, and then return to the task of categorizing the next threat. In summary, cybersecurity is a potential threat to everyone, especially to smart communities. Attacks are not only possible but also likely to occur, and there is a need to address attacks quickly and productively, while learning from the attacks to build more resilient systems in the future. Moving forward, partnerships need to be formed between government, academia, and industry to enhance smart community resilience to cybersecurity threats.

2.4.3. Keynote: Draft GCTC Cybersecurity and Privacy Guidebook

The final keynote speaker was Lan Jenson of Adaptable Security Corporation and Co-Chair of the Cybersecurity and Privacy Advisory Committee (CPAC). She discussed the current state of smart, secure cities. Jenson began by stating that cyberspace has enabled nearly every industry to be reinvented and that a hyperconnected world has been created to transform the global economy.

The speaker indicated that the way to increase security now is for end users, developers and manufacturers, and organizations to adopt best practices for security and privacy. According to her, convincing these stakeholders to adopt best practices will require incentives and/or consequences. Otherwise, such measures will not be taken until after hacks and breaches occur. Additionally, Jenson suggested the need for public

and private sector partnerships and transparency to encourage adoption. She noted that larger businesses can provide visibility and opportunities to engage employee volunteers to reduce cybersecurity risk and that for the government, unbiased and affordable expertise and advise could be offered. Finally, she argued that people can be empowered to engage in cyber protection by learning who to trust and what intuitive tools can be used to provide better visibility.

In sum, cybersecurity is becoming a major priority due to the increasing number of data breaches. Government, public sector, and community members must all get involved in developing and adopting cybersecurity and privacy best practices to increase cyber resilience.

2.4.4. Discussion Group 3: Global Perspective

Nadya Bliss, Director of the Global Security Initiative at Arizona State University, led the cybersecurity discussion group on global perspectives. This group highlighted the interests and perspectives of the participants. Some participants were interested in exploring the fair and sustainable use of technology in smart cities and how such technologies are related to public trust and social cohesion. Others noted that it is important to establish a set of cybersecurity standards, which are currently missing from smart cities. While standards may be helpful in aligning cities, compliance issues are expected to arise as well. From a first responder perspective, more information is desired, but it is unclear how information can be collected and aggregated in real time. Participants of this group agreed that there is a need for government, non-profits, industry, academia, and first responders to work together on these issues.

The major question this group attempted to answer was how to identify and mitigate potential risk. While interoperability is important, having a single system may not be the most secure or practical option either. In the area of emergency response management, the group argued that standards should utilize open-source APIs. In conclusion, smart cities need some set of standards to at least serve as a model for developing new technologies with both interoperability and security in mind. Focus should be placed on integrating social sciences and research on human factors to design and implement smart cities with cybersecurity as a primary concern.

2.4.5. Discussion Group 4: Internet of Things Security

The final discussion group of the workshop explored issues on IoT security, led by Bryan Schromsky, Director of Federal Government and Public Safety, Verizon Wireless. Schromsky highlighted the challenge of integrating old and new technologies so that they can work together. This issue spans many industries, including tele-health, tele-medicine, and patient safety, yet it is unclear who is responsible for making integration possible.

The speakers in the group emphasized that most technologies are currently IoT-enabled, but IoT is not necessarily centralized. For example, technologies may connect vehicle to vehicle directly or indirectly via cloud systems or other infrastructure. The group noted that IoT and security must be evaluated with these complexities and that there is often no assumption or consideration of privacy as information is shared. For example, the group discussed a scenario in which an individual shops for a car: facial recognition could be used to identify an individual entering a dealership, their credit score could then be checked when they buy the car, and so on, leading to many potential vulnerabilities for data breaches and security breakdowns. In summary, people often do not pay enough attention to privacy when using technologies in everyday life, and technology is not necessarily developed with privacy considered as an important factor.

3. 2019 Case Study: Live Simulation Exercise of Emergency Response at an Instrumented Public Facility

On November 18th, 2019, at the George Mason University's EagleBank Arena in Fairfax, Virginia, six separate teams, including over 70 local firefighters, EMS personnel, law enforcement first responders, and volunteers participated in a live, simulation-based, multi-team training exercise. This was the first multi-agency exercise organized through a joint industry–academia effort between the Center for Innovation Technology (CIT), Smart City Works, and the George Mason University, facilitated by the Department of Homeland Security (DHS), Science and Technology Directorate's "Smart City Initiative."

This exercise was a part of a continuing research and development effort begun in the Global City Teams Challenge (GCTC) program geared toward a better understanding of how the integration of multiple data streams can be securely utilized to enhance public safety and response effectiveness in emergency situations. Specifically, the staged scenario was part of research into smart building and smart first responder technology systems that can help first responders save lives and improve public safety. Figure 1 shows responders in pursuit of a shooter during the exercise.

Figure 1: Responders in pursuit of a shooter during the exercise.
(Photo used with permission from the George Mason University.)

Utilizing insights gleaned from Discussion Group 2: First Responder Priorities for Smart Public Safety on Day 1 of the 2018 PSSC/CPAC Workshop, the exercise pilot tested several technologies instrumented in the EagleBank Arena, including video, location-based and occupancy sensors, and displays from a variety of technology innovators. Key technology partners developed the core IoT infrastructure, providing the

analytics platform to improve building operation on a daily basis and developed a 3D digital twin visualization of the EagleBank Arena. During routine operations, these technologies were designed to improve the operational and energy efficiency of the arena, enhance comfort, and provide additional services to patrons. However, in the case of an emergency, the 3D digital twin visualization, video, and sensors can also be available to help responders determine more rapidly the location and type of emergency, find victims more quickly, and, ultimately, save lives.

Specific sensors and displays included 24 sensor pods incorporating remote video capability, Wi-Fi detectors, blue-force tracking, LiDAR occupancy detectors, particulate and environmental sensors, along with 2D/3D visualization tools. The analytics platform, along with a digital twin of the facility, and Wi-Fi-based indoor location platform allowed for rich information data streams to be captured along with real time first-responder team tracking capabilities for review in the simulation debrief to enhance team learning. Figure 2 shows responders viewing analytics.

Figure 2: Responders viewing analytics during the exercise.
(Photo used with permission from George Mason University.)

The live, simulation-based training engaged the teams of first responders, who, prior to this effort, had never engaged in a joint exercise together.

The incident staged was an active violence incident/mass casualty exercise in the large arena, which required the joint efforts of local fire, EMS, and law enforcement first responders. As this event was meant to test the instrumented technology system, first responders were not provided the system interface with available data, such as the 3D digital twin of the building, prior to arriving on scene. However, during a feedback session, leadership representing the participating agencies were presented with the opportunity to review the technology system and provided favorable feedback.

Echoing insights from the 2018 PSSC/CPAC workshop, the panel emphasized the desire for increased situational awareness for first responders. Members of the response agencies mentioned the usefulness of the 3D digital twin visualization for providing an enhanced and shared understanding of the operational environment and for incident command for managing the personnel and response efforts. This was deemed

especially helpful for first responder teams who were unfamiliar with the layout and structure of the building. Additionally, the occupancy and location-based sensors were seen to provide helpful data streams when engaging in search and rescue, after the exercise suspect was neutralized. The security of the collected data streams was also cited as an important consideration by all involved. As such, when designing the technology system, the security of data and mitigation from cybersecurity attack or intrusion were highlighted as critical components of the technology system.

This effort also provided an opportunity for learning scientists, organizational psychologists, and engineering researchers affiliated with the George Mason University's new Center for the Advancement of Human Machine Partnerships (CAHMP) to design and employ an initial prototype of an Artificial Intelligence (AI)-enabled system that seeks to augment the learning experience of emergency responders in the live simulation training exercise. The AI-enabled system was created to support training instructors with multimodal learning analytics for enhanced training debriefs (e.g., post-action reviews). The system applied AI methods of computer vision and machine learning to process the various multimodal data streams in near real-time, collected during the training exercise by the aforementioned state-of-the-art sensing technologies.

A core objective of the training simulation debrief after various scenario runs was to review and analyze the effectiveness of specific events of interest, such as the time differential between the response dispatch and the neutralization of the shooter or time of interaction between the responders and victims or patients. The AI-enabled system provided first responders with an experimental user interface that displays information for these key indicators. Additionally, the AI-enabled system provided a starting point for important insights for coordination activities within-teams and between the different responder teams. This effort can help facilitate both within- and between-team learning, which is an often-neglected component of emergency response management operations. Future exercises will further explore the effectiveness of technologies, such as AI-enabled systems, in initiating change in behavioral patterns of multi-team collaboration among first responders.

Preliminary insights from the exercise and initial data analyses indicate that first responders and their leadership see significant value in this type of joint agency training event in building levels of trust amongst the different agencies that would respond and work together in an actual event. Participation by technology developers in these events enables the resulting technologies to become increasingly suited to the dual-uses of daily efficiency and emergency response effectiveness. Live simulation training exercises, combined with corresponding research cycles to evaluate the outcome, may provide a unique opportunity for researchers to explore new technologies in situ, incorporating direct insights from first responders. The integration of technology systems may provide enhanced situational awareness and security within a building, and first responder wearable devices for collecting sensor data for use in emergency preparedness training will also allow researchers to study team interaction in real time.

4. Conclusion and Next Steps

As this workshop report and case study illustrate, the work of the Public Safety SuperCluster is maturing beyond the realm of program definition and organization and into the realm of concept exploration and collaboration (particularly with the other GCTC SuperClusters) and technology application and demonstration.

The 2018 GCTC–SC3 PSSC/CPAC workshop was an important event to discuss the latest issues and developments on the adoption of emerging technologies for public safety, cybersecurity, and privacy by cities and communities. The workshop successfully summarized the critical issues and the ongoing efforts to mitigate and address many of them.

The speakers provided insights into the latest threats, including growing populations and the increasing complexity of technical solutions being adopted by a broad range of industries. Panelists highlighted the growing need for first responders to gain more situational awareness in real time and how emerging technologies such as social media platforms and IoT might be used to achieve that goal. The workshop also included examples of international collaboration with Europe and India.

Speakers and participants expressed concerns that cyber threats are becoming increasingly pervasive across a number of sectors, including energy, transportation, defense, and manufacturing. Risk management is important, but it should be accompanied and followed up by strategies and actions to reduce potential attack vectors and improve cybersecurity incident response. Resilience should be considered in the system design to limit the damage from successful attacks. Cybersecurity efforts are cyclical and requires partnerships and collaboration between industry, academia, and government.

Similarly, the collaboration in 2019 between the George Mason University, EagleBank Arena, the Virginia Center for Innovative Technology, Smart City Works, the DHS Science & Technology Directorate, and a host of technicians and developers illustrated both the technical complexity and the potential for collaborative research and development to enhance first responder capabilities. In addition, the integration of facility instrumentation, artificial intelligence-based display and analysis tools, and simulation-based exercise evaluation involving the dedicated time of six real-world response agencies and 70 responders showed the power of collaboration between technology developers, research institutions, and operational units in developing advanced capabilities to solve real-world challenges in public safety.

There are a number of promising areas in which emerging technologies can help improve public safety. As technologies become more broadly adopted by industry, it is necessary to pay more attention to novel cyber threats and the attendant issue of privacy. It is not enough to analyze risks; it is important to attempt to reduce possible attack surfaces in advance and plan for efficient and swift incident responses. When developing and deploying solutions, it is important to consider cybersecurity—as well as operational efficiency and effectiveness—as a primary concern rather than an afterthought. The concept of designed-in security and privacy will be essential in reducing risks and possible attack vectors.

The PSSC and CPAC working groups will continue to work together with municipal governments to help them improve their preparedness for public safety and cybersecurity using emerging technologies, consensus-based standards, and collaborative research and development approaches.

Acknowledgements

We acknowledge valuable contributions of the speakers and participants at the workshop and the simulation exercise, who provided their perspectives on future opportunities, needs, and challenges for smart and secure cities and communities. We also acknowledge the Department of Homeland Security's Science & Technology Directorate for co-hosting the 2018–2019 GCTC program and to the GCTC CPAC members who provided valuable insights and presentations.