NIST SPECIAL PUBLICATION 1900-201

Global City Teams Challenge 2018 Kickoff and IES-City Framework Workshop: Smart and Secure Cities and Communities Challenge

Sokwoo Rhee
Martin Burns

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-201

C Y B E R - P H Y S I C A L S Y S T E M S

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

NIST SPECIAL PUBLICATION 1900-201

Global City Teams Challenge 2018 Kickoff and IES-City Framework Workshop: Smart and Secure Cities and Communities Challenge

C Y B E R - P H Y S I C A L S Y S T E M S

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-201

October 2018

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 1900-201
Natl. Inst. Stand. Technol. Spec. Publ. 1900-201, 34 pages (October 2018)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-201

TABLE OF CONTENTS

Executive Summary **1**

1. Introduction **3**

1.1. Overview of the GCTC Program 4
1.2. Overview of the IES-City Framework 4
1.3. Purpose of this Publication 5

2. GCTC 2018 Kickoff: Smart and Secure Cities and Communities **6**

2.1. Background 6
2.2. 2018 Kickoff Event Scope and Format 7
2.3. Plenary and Panel Sessions 7
2.4. Open Forums and Sidebars 8
2.5. SuperCluster Breakout Session Results 10
2.5.1. Transportation and Cybersecurity/Privacy 11
2.5.2. Public Safety and Cybersecurity/Privacy 12
2.5.3. Data Platforms and Governance and Cybersecurity/Privacy 13
2.5.4. Utilities and Cybersecurity/Privacy 14
2.5.5. Wireless and Cybersecurity/Privacy 15
2.5.6. Agriculture and Rural Communities and Cybersecurity/Privacy 16

3. IES-City Framework **18**

3.1. Background 18
3.2. IES-City Framework Workshop Scope and Format 18

4. Next Steps **20**

Acknowledgements **21**

Agenda **22**

Acronyms/Abbreviations **29**

Useful Links **30**

Executive Summary

The National Institute of Standards and Technology (NIST) Global City Teams Challenge (GCTC) is a strategy to contribute to the standardization and interoperability of cyber-physical systems emerging for use in our nation's communities. The GCTC program has evolved to become a collaborative platform for the development of smart cities and communities. The program strives to create an environment where communities can benefit from working with others to improve efficiency and lower costs. The International Technical Working Group on IoT-Enabled Smart City Framework (IES-City Framework) is a closely related effort. NIST convened this working group to help develop a common architectural framework for smart city solutions. The draft Framework was posted for public comment in February 2018.

In 2018, NIST and the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T) are co-hosting the GCTC Smart and Secure Cities and Communities Challenge (SC3) program. The objective is to encourage participating teams to include cybersecurity and privacy as integral project elements in addition to existing GCTC goals such as the replicability, scalability and sustainability of technology and systems.

This report highlights the first GCTC SC3 event held on February 6 to 8, 2018 to foster discussion and collaboration on the cybersecurity and privacy challenges that face cities as they implement smart technologies. Nearly 500 representatives from cities, industry, government, private institutions and academia with an interest in smart cities attended the event. The first two days of the event included a series of plenary and panel sessions, interactive networking breakouts, and open forums related to the GCTC domains. The last day of the event focused on the IES-City Framework to gain feedback from stakeholders. Table E-1 summarizes emerging projects and topics for SuperClusters, as well as the primary topics covered during the IES-City Framework Workshop.

Highlights of the 2018 GCTC SC3 Kickoff

- Nearly 500 attendees
- Over 30 cities, communities, states and countries represented
- Existing 6 SuperClusters represented
- New SuperCluster launched
- Breakout sessions for 6 important domains
- New Action Clusters formed
- Many security and privacy experts in attendance
- IES-City Framework presented for public comment and feedback

Breakout sessions fostered networking, collaboration and project team building for existing and new SuperClusters (SCs) and Action Clusters (ACs). Breakouts covered six SuperCluster domains, integrated with cybersecurity/privacy: Transportation, Public Safety, Data Platforms/ Governance, Utilities, Wireless, and the newly formed SuperCluster for Agriculture and Rural Communities. A new Action Cluster launched for Smart Buildings, with a wide spectrum of participation from this community. An interest group for Education met to discuss possible collaborations, and a new component (Data Governance) added to the Data Platforms SuperCluster. During the IES-City Framework workshop, a public comment period kicked off and organizers called for additional use cases to help refine and improve the Framework.

Given the success of the kickoff, planned events over the next year for GCTC-SC3 will further help ACs and SCs accomplish their goals. These include a Global Tech Jam in Portland, OR and an Exposition of GCTC projects, projected for early 2019. Several SCs are planning their own workshops in 2018 as well.

Table E.1 GCTC-SC3 Summary

SELECTED EMERGING SUPERCLUSTER PROJECTS/TOPIC AREAS					
Transportation	**Public Safety**	**Data Platforms/ Governance**	**Utilities**	**Wireless**	**Agriculture/ Rural Communities**
Connected intelligent transportation Electric and autonomous vehicles Last 50' Freight Protecting vehicle user data Urban shuttles Waterfront transport	Smart emergency medical teams (data from multiple digital sources) Mobile Intelligence from land mobile radios, devices and city systems	Optimized city data collection, use and interpretation Secure data from IoT sensors Data analytics Common measurement and standards	Smart street lighting (security and public safety, WiFi) District energy models (rooftop solar, electric vehicles) Secure data analytics for municipal utilities	Large scale aggregation of wireless solutions Securing IoT networks from users to cloud and the device side Integrated network architecture to reduce costs of WiFi	Smart agriculture University-based rural test beds Healthcare and ability for aging in place in rural areas Precision agriculture and livestock management Better broadband-enabled access
IES-CITY FRAMEWORK TOPICAL INTEREST AREAS					
Framework Goal and Methodologies		**Technology Artifacts**		**Application Management Framework**	
Framework goals and artifacts: how they are produced, composed, the evergreen state, methodologies, tools that help with composability of systems.		Side-by-side comparison of technology suites deployed to foster harmonization; uses cases for a "day in the life" of a smart city in 10 years.		Pivotal points of interoperability and zones of concern, alongside the NIST Cyber Physical Systems Framework (a central foundation for the IES-City Framework).	

1. Introduction

Smart cities are enabled by cyber-physical systems (CPS), which include interconnecting smart devices and systems—such as Internet of Things (IoT) technologies—in fundamentally new ways. When applied to diverse sectors such as transportation, energy, public safety, and healthcare, these technologies will enable cities and communities to improve services, promote economic growth, and enhance 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.

In mid-2014, the National Institute of Standards and Technology (NIST) established the CPS Public Working Group (CPS PWG) to bring together CPS experts in an open public forum to help define and shape key characteristics of CPS, and to better manage development and implementation within and across multiple "smart" application domains. The CPS PWG is developing a shared understanding of CPS and its foundational concepts and unique dimensions, now described in the CPS Framework, Release 1.0, which is available to the public. [1,2] The Framework presents an analysis methodology centered on the concepts of CPS domains, facets and aspects, 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 a comprehensive standards and metrics base for CPS to support commerce and innovation.

Studies show that 54 percent of the world's population now lives in urban areas, with this proportion projected to increase to 66 percent by 2050.[3] When combined with population growth, studies also note this could add another 2.5 billion people to urban populations by 2050. Cities and communities across the globe are increasingly seeking smart, connected solutions as a way to meet the needs of growing urban areas. Cyber-physical systems 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 under this rapid growth scenario.

NIST Global City Teams Challenge (GCTC) is a strategy to contribute to the standardization and interoperability of cyber-physical systems emerging for use in our nation's communities. In a closely related effort, NIST has convened the International Technical Working Group on IoT-Enabled Smart City Framework (IES-City Framework), to help develop a common architectural framework for smart city solutions. The following sections provide a brief overview of these activities.

---

[1] NIST Special Publication 1500-201. Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. June 2017. Accessed 8/17/18. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf.
[2] 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
[3] *World Urbanization Prospects, 2014 Revision.* United Nations Department of Economic and Social Affairs, Population Division. 2014. Accessed 3/1/2018. https://esa.un.org/unpd/wup/

1.1. Overview of the GCTC Program

NIST launched the GCTC program to encourage collaboration and industry's leadership for the development of voluntary, consensus standards in technical areas related to cyber-physical systems. The program has been in place in some form since 2013; a short history of the program and its impacts are found in NIST Special Publication 1900-01. [4]

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

The GCTC program has evolved to become a collaborative platform for the development of smart cities and communities. The program strives to create an environment where communities can benefit from working with others to improve efficiency and lower costs. The GCTC is led by NIST, an agency of the U.S. Department of Commerce, in partnership with other U.S. federal agencies including the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T), the National Science Foundation, International Trade Administration, and National Telecommunications and Information Administration (NTIA), as well as other organizations from the public and private sectors. New partners are continuously emerging and committing to involvement with the GCTC. The GCTC website maintains a listing of current GCTC partners.[5]

The GCTC encourages local governments, nonprofit organizations, academic institutions, technologists, and corporations from all over the world to form project teams – "Action Clusters" and "SuperClusters" – to work on groundbreaking IoT and CPS applications within the city and community environment. Action Clusters (ACs) are partnerships between cities/communities and innovators working together around a specific issue or problem to jointly identify and develop solutions that are scalable and replicable. Action Clusters sometimes include multiple cities/communities and as many as 10 to 15 partners. SuperClusters (SCs) are larger efforts typically involving multiple cities/communities, multiple Action Clusters, and as many as 50 partners working on wide-ranging issues and solutions under a common umbrella. A description of the existing SuperClusters and Action Clusters are available on the GCTC website.

1.2. Overview of the IES-City Framework

NIST and its partners convened the International Technical Working Group on IoT-Enabled Smart City Framework (IES-City Framework) to develop a consensus framework of common architectural features that will better enable interoperable, portable smart city solutions. Deployments of information and communications technologies (ICT) in cities are often customized systems that are not interoperable, portable across cities, replicable, or cost-effective. In addition, a number of architectural design efforts are underway through different organizations (e.g., ISO/IEC JTC1, IEC, IEEE, ITU and consortia) but have not yet converged, creating uncertainty among stakeholders.

NIST and its partners published a draft of the IES-City Framework for smart city stakeholder review and feedback in February 2018. Dozens of participants from around the world who are seeking methods of

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

[5] https://pages.nist.gov/GCTC/

convergence and harmonization for smart city deployments developed the Framework. It is available for public viewing and comment.[6]

1.3. Purpose of this Publication

In 2018, NIST and DHS S&T are co-hosting the GCTC Smart and Secure Cities and Communities Challenge (SC3) program. The objective is to encourage participating teams to include cybersecurity and privacy as integral project elements in addition to existing GCTC goals such as the replicability, scalability and sustainability of technology and systems.

This report highlights the first GCTC SC3 event of 2018. It describes the many speakers and presentations, open forums and sidebars, and breakout sessions that contributed to team building for new Global City Team Challenge projects.

Dr. Sokwoo Rhee, NIST, addresses participants during the first event of the 2018 Global City Teams Challenge. Photo Credit: Energetics

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

2. GCTC 2018 Kickoff: Smart and Secure Cities and Communities

2.1. Background

Cities are taking advantage of the IoT and connected systems at a remarkable pace. While smart technology offers cities many opportunities to improve economies and quality of life, it also presents new challenges for cybersecurity and privacy. Consumers are using smart meters, home security systems, appliances, building controls, and many other devices. Devices within a home are relatively insecure and thus potentially vulnerable to an adversarial attack or misuse. Outside the home, automobiles, businesses, the energy grid, public meeting places, streetlights and a host of systems and devices are becoming smart and interconnected, requiring security that is more sophisticated. Further connecting these systems to consumers in turn leads to additional points of vulnerability.

Highlights of the 2018 GCTC Kickoff

- Nearly 500 attendees
- Over 30 cities, communities, states and countries represented
- Existing 6 SuperClusters represented
- New SuperCluster launched
- Breakout sessions for 6 important domains
- New Action Clusters formed
- Many security and privacy experts in attendance

Taking advantage of the IoT and interconnected devices exposes cities to a greater array of cyber security threats as well as criminal exploitation. A recent report notes that misuse or attack on a single smart city vulnerability could potentially create risk for an entire city.[7] Preparing for and recovering from such attacks also requires access to reliable digital forensic data – which means that sufficient data from smart city systems must be available and secure.

Ensuring the cybersecurity of systems as well as data privacy presents an integrated challenge. Systems that trigger emergency response, for example, must also protect privacy while being secure. Citizens are becoming digitized, offering a growing array of instrumented data available about their location, preferences, activities, and other personal factors. This interaction between people, networks, systems and devices creates enormous privacy challenges that go hand in hand with addressing concerns for security.[8]

Addressing the challenges of cybersecurity and privacy is the overall theme of the 2018 GCTC Smart and Secure Cities and Communities Challenge. The first event, described below, kicked off the year by bringing together experts in the field and stakeholders from many public and private sectors to discuss the important issues and potential solutions.

[7] R. Khatoun, S. Zeadally. Smart cities: concepts, architectures, research opportunities**.** Communications of the ACM, 59 (8) (2016), pp. 46-57

[8] Adel S.Elmaghraby Michael M.Losavio. Cyber security challenges in Smart Cities: Safety, security and privacy. https://doi.org/10.1016/j.jare.2014.02.006
https://www.sciencedirect.com/science/article/pii/S2090123214000290

2.2. 2018 Kickoff Event Scope and Format

The 2018 GCTC kickoff event, titled Smart and Secure Cities and Communities Challenge was held on February 6-8, 2018 to foster discussion and collaboration on the cybersecurity and privacy challenges that face cities as they implement smart technologies. Nearly 500 representatives from cities, industry, government, private institutions and academia with an interest in smart cities attended the event.

The event included a series of plenary and panel sessions, interactive networking breakouts, and open forums. During the first two days of the event, speakers from federal, state and local government provided their perspectives on cybersecurity and privacy, including the latest trends and challenges with an impact on the nation, communities, and citizens. A fireside chat and open forum discussions allowed for interactive dialog with the audience on key issues.

During the event, breakout sessions fostered networking, collaboration and project team building for existing and new SuperClusters and Action Clusters. The following sections provide highlights of speaker and breakout sessions from the first two days. Breakouts were organized around six domains and integrated with cybersecurity/privacy:

- Transportation
- Public Safety
- Data Platforms, Governance
- Utilities
- Wireless
- Agriculture and Rural Communities

The third day of the event focused entirely on the IoT-Enabled Smart City (IES-City) Framework, described in Section 3. The following sections provide highlights of speaker and breakout sessions from the first two days.

2.3. Plenary and Panel Sessions

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 cybersecurity and privacy that are impacting cities and communities across the globe. Table 2.1 shows the complete list of speakers for each session.

Table 2.1. Plenary and Panel Sessions

Track	Speakers
Welcome and Keynote	• **Chris Greer**, Senior Executive for Cyber-Physical Systems, National Institute of Standards and Technology (NIST) • **Doug Maughan**, Director of the Cyber Security Division (CSD), Department of Homeland Security (DHS) Science and Technology Directorate (S&T) • **André Hentz**, Acting Deputy Under Secretary, DHS S&T
Perspectives from State Governments on Smart Communities and Security/Privacy	• **Tim Blute**, Director of Future, National Governors Association • **Kirk Lonbom**, Acting Secretary, Department of Innovation & Technology, State of Illinois • **Karen Jackson**, Former Secretary of Technology, Commonwealth of Virginia
Smart Cities and the Internet of Things (IoT) and Cybersecurity and Privacy	• **Sokwoo Rhee**, Associate Director of Cyber-Physical Systems Program, NIST • **Scott Tousley**, Deputy Director, CSD, DHS S&T: DHS S&T Programs • **Donna Dodson**, Chief Cybersecurity Advisor, NIST Information Technology Laboratory (ITL) and Director of the National Cybersecurity Center of Excellence: NIST ITL and NCCOE Programs • **Martin Burns**, Smart Grid and Cyber-Physical Systems Program Office, NIST • **Allan Friedman**, Director of Cybersecurity, National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce • **David Corman/Meghan Houghton**, National Science Foundation • **Jeb Benson**, Public Safety Communications Research, NIST
Panel: Cybersecurity and Privacy for Smart Cities and Communities	*Moderator:* **Scott Tousley**, Deputy Director, CSD, DHS S&T • **Erin Kenneally**, Program Manager, CSD, DHS S&T • **Bob Bennett**, CIO, Kansas City MO • **David Heyman**, Co-founder, Smart City Works and Past DHS Assistant Secretary of Policy

2.4. Open Forums and Sidebars

Cross Connections for Cybersecurity – This moderated session explored the common cyber security and privacy issues that cut across SuperClusters, Action Clusters and the various domains. Attendees and Cybersecurity and Privacy (CS/P) experts exchanged ideas on some of the key challenges and cross-cutting solutions. The objective was to spark cross-fertilization and interaction to help identify and solve some of the larger challenges in CS/P. SuperCluster leads were asked to identify some of the major CS/P problems that emerged in their breakout sessions. The audience was asked to give their perspectives on cross-sector issues, in particular: CS/P challenges that are important to the sector but not yet being addressed; big emerging challenges that could have broad impacts on cities in the future; and CS/P issues that impact multiple sectors and organizations where common solutions could be applied. Some of the common CS/P considerations identified included:

- *Cybersecurity*
  - Considerations of both cybersecurity and cyber safety; cybersecurity is a job for experienced professionals; cyber safety is an all-community issue, and everyone has a role to play.
  - Options for building-in versus buying cyber security solutions, including: buying a new system; tearing down and starting over if insufficient cyber security measures are implemented (preference of CS professionals); "bolting on" additional CS measures (given municipal resource constraints, may be more realistic but not condoned by CS professionals); and encapsulation (i.e., quarantining vulnerable systems). Many cities do not have expertise to know what questions to ask as they get started – making choices is difficult.
  - Using both active and passive CS: passive CS includes technical systems (software and hardware) designed to prevent intrusions and encrypt data; active CS includes risk management plans and systems that guide developer/user behavior. Both are important; if risk factors are not identified or if unforeseen vulnerabilities exist, passive measures cannot be implemented. Passive CS keeps out 99% of threats; it is how we identify and deal with the 1% that needs more effort. The main issues are (1) prioritizing resources and (2) prioritizing threats.
  - Securing the IoT and WiFi; a lot of data is being collected from WiFi, i.e., cities may not realize they're tracking addresses and other data. Cities need guidance on the IoT and security, which is more than encryption but includes data integrity (e.g., data coming into the system). Cities need to decide about how to approach Public WiFi – buying a packaged system locks the city in to a private supplier for service and security. Building CS needs into the system from the beginning is necessary. Right-of-way fees for access to fiber infrastructure are a hot issue – and an opportunity for cities to work closely with neutral host providers/ISPs to get the best solution.
  - Difficulty in complexity, scale and modeling of CS solutions; this is a common theme throughout data management, aggregation, integrity, and reliability. It is not feasible to just wade in and manage information; experts with experience need to review so municipalities can consider solutions from an informed position.
  - Ownership of data; determining whose obligation it is to protect data from theft as well as data manipulation. This includes assurances that data coming out of systems are reliable, especially for mission critical systems and infrastructure.
- *Privacy*
  - Community buy-in on data collection and its use; not collecting data without community buy-in and understanding that communities may want to focus data on particular uses. Issues arise on how to share data – not necessarily concerns about misusing data, but that data may not be valid or correct, or could be misinterpreted.
  - Service provider aggregation and data use policies; policies impact what data is being collected, how it has collected, and how it can be used. Aggregating otherwise innocuous

data together in one place can create additional security and privacy problems: 1) data becomes more of a target (more data, more value to hackers); 2) data asymmetry;[9] 3) data management, i.e., cities have to protect access and audit logging. Communities may want control over what collectors/aggregators can do with that data, retroactively (e.g., vendor cannot sell data to third parties).

SuperCluster Sidebar Meetings – A number of sidebar meetings launched new partnerships, identified gaps in capabilities, and formulated demonstration plans for projects. These groups were well-attended and provided excellent networking opportunities. Highlights included:

- *Launch of the Smart Building Action Cluster (SBAC)* – The NTIA, NIST and the Telecommunications Industry Association hosted initial discussions and team formation for a new SC, which will focus on the crucial nexus of smart buildings and smart communities' interoperability.
- *Data Governance* – This relatively new addition to the Data Platforms SC will address the address the challenge of building a governance and exchange model for IoT data and a plan for governments and technology providers to successfully customize and deploy it. The group discussed blueprints, directions, best practices, and future actions for this topic.
- *Interest Group for Education SuperCluster* – This group assembled to begin addressing the critical need for education, training and awareness of advanced technologies in urban environments; discussions included, for example, digital awareness, online learning, and workforce development.
- *Public Safety SuperCluster (PSSC) Leadership* – This informal session focused on ACs and cities who want to join the Executive Leadership team for the PSSC and help define future directions in smart public safety; topics included disaster preparedness, community resilience, crisis communications, infrastructure protection, First Responder technologies, and related fields.

2.5. SuperCluster Breakout Session Results

Breakout sessions provided information on the progress and scope of existing and new SuperClusters; gave cities and communities an opportunity to discuss their needs and gaps in capabilities; introduced potential partners; incorporated elements of CS/P; and encouraged the formation of new Action Clusters. Sessions included a mix of representatives from cities, States and counties; SuperClusters; existing Action Clusters; potential partner participants; and observers from many types of organizations.

Each session kicked off with a number of speakers, followed by an introductory networking process and team formation/planning. Both cities and partners participated in the networking process designed to help create partnerships for existing and future SuperClusters and Action Clusters. During the networking process, each participating partner representative spoke 2-3 minutes about their organization, areas of interest, potential technology solutions, and elements related to cybersecurity and privacy. Cities and communities talked about their goals, challenges and needs for solutions. Information from short

[9] D**ata asymmetry** refers to disparity in access to data, i.e., the data steward gains more value from the data than the contributor.

introductory talks posted at the front of the room provided context for networking and partner-building sessions.

This process provided a quick but efficient way to introduce partners and their capabilities and products to cities and communities in need of technology solutions. Afterwards, potential partners with common interests participated in interactive small group sessions and produced a number of project ideas, which could potentially lead to new Action Clusters and demonstrable, replicable solutions. Some created potential action plans for new projects, which included performance targets, outcomes, key performance indicators (KPIs), milestones, and possible team members and their roles.

The following sections describe the participating speakers as well as the potential Action Cluster topics emerging from these sessions, organized by economic sector or topical area. The process resulted in nearly 30 potential new topics for Action Clusters. A report out session on the second day of the event summarized the highlights of these discussions.

2.5.1. Transportation and Cybersecurity/Privacy

This session covered a number of transportation technologies important to cities, including intelligent vehicles and transport systems; traffic technologies; first and last mile vehicles (including shared, low speed and autonomous); and the building of smart communities around transfer points and mobility hubs.

A variety of speakers (inset) provided insights on new transportation technologies currently used to help cities improve traffic, citizen and freight mobility, and overall transportation safety and flow. During the breakouts, about 30 potential partners provided introductory information and networked with existing SuperCluster and Action Cluster teams. Discussions included a number of existing projects as well as potential for new partnerships. Figure 2.1 shows those groups in the process of becoming an AC (or with serious intent to become an AC).

Transportation SuperCluster presents on existing/potential new Action Cluster topics. Photo credit: Energetics

Transportation SuperCluster

Chairs: Skip Newberry, President, Technology Associates of Oregon and **Wilf Pinfold**, CEO, Urban Systems

Presenters:

- Connected Intelligent Transportation: **Christine Kendrick**, Portland Bureau of Planning and Sustainability, OR
- Farm to Fork Crop Tracking: **Shawn Irvine**, Economic Development Director, City of Independence, OR
- Protecting User Data in the Smart City Scenario: The Case of the NGSI Encryption Layer w/FIWARE and Mexico City: **Nestor Velasco Bermeo**, Researcher, Computer Science Department - Tecnologico de Monterrey
- Transportation Data Analysis - **Catherine Nikolovski**, Hack Oregon
- City Data Security and Privacy - **Isaac Potoczny-Jones,** Tozny LLC

In addition, a number of challenges, technologies and potential solutions were discussed that could potentially be applied transportation problems emerging in a city intelligent transportation environment. Presentations given in the following area have potential as future ACs:

- Autonomous vehicle (AV) solutions
- Transportation analytics
- City data security and privacy (Green Route)
- Testing of new transportation technologies within cities (Urban Leap)
- Smart Car (CryptoMove)
- Smart cities data security (Virginia Transportation)

- Connected Intelligent Transportation, Sensors (City of Portland, OR)
- Hong Kong Science Park Electric Vehicles (EV) and Autonomous Vehicles (AV) (Mobility Cubed, Inc.)
- Last 50' Freight (Telocity)
- Berry Harvest (City of Independence, OR)
- Protecting User Data (Tecnologico de Monterrey)
- Portland Central Eastside Shuttle (Urban Systems, Inc.)
- CIVIC Data Portal (Hack Oregon)
- Washington Waterfront – potential AC (QED Associates LLC)

Figure 2.1. Emerging Transportation and Cybersecurity/Privacy Action Clusters

2.5.2. *Public Safety and Cybersecurity/Privacy*

The Public Safety and Cybersecurity/ Privacy session covered technologies, processes and strategies to enhance public safety and resilience within smart connected communities; improved preparedness, response and recovery from hazards and risks that threaten local and regional stability; and the role of cybersecurity and privacy in safety. Speakers from the private sector and academia (inset) provided their perspectives on the nexus of safety and cybersecurity, as well as the challenges emerging from the increasing use of connected systems and the IoT.

The Public Safety SuperCluster lead covers some of the key solutions and concepts identified in the breakout session. Photo credit: Eneraetics

Public Safety SuperCluster

Chair: **Michael Dunaway**, Director, NIMSAT, University of Louisiana, Lafayette

Presenters:

- Recent Trends in the Public Safety Cybersecurity Landscape: **George Popovich**, Director of Products & Services Cybersecurity Governance, Motorola Solutions
- A Strategic Approach to IoT Security: Focus on Public Safety Mission: **Andrew Osborn**, Lead Mobile Cybersecurity Architect, AT&T Public Sector Solutions
- Mutualink/Amazon Web Services Project: **Michael Wengrovitz**, VP of Innovation, Mutualink
- UAS-Borne Wireless Networks: **Kamesh Namaduri**, University of North Texas

Over 50 potential partners provided introductory information and networked during the session. Discussions produced potential AC concepts and identified a variety of solutions with potential application to the current SuperCluster and ACs. Figure 2.2 describes possible new ACs.

- Smart Medical Emergency Teams – Alignment of data from multiple digital sources (e.g., sensor, video, audio) and different agencies to enhance near-time incident decision making and analysis. CS/P components include security of data streams, authentication, and authorization (Fairfax County, VA).
- Mobile Intelligence City Protect and Enterprise – Integrating, correlating and extracting actionable data from land mobile radios (LMRs), devices, and disparate city systems to improve community safety. CS/P components include securely integrating cyber and physical devices for true situational awareness.

Figure 2.2. Emerging Public Safety and Cybersecurity/Privacy Action Clusters

2.5.3. *Data Platforms and Governance and Cybersecurity/Privacy*

The Data Platforms, Governance and Cybersecurity/Privacy session incorporated a broad perspective on optimizing data collection, utilization, and interpretation. Topics included secure and private data as an enabler for smart city systems; common data measurements and standards; a comprehensive strategy for handling the data from thousands of existing IoT sensors and those envisioned for the future; and optimizing data as a way to improve operations and the delivery of services.

SuperCluster representatives and speakers from the public and private sectors (inset) provided perspectives on security and privacy issues and solutions, in the context of the collection and use of data as well as governance and exchange of data from the IoT.

Members of the Data Platform and Governance SuperCluster report on major findings from their breakout session. Photo credit: Energetics

Data Platforms/Governance SuperCluster

Chair: Bob Bennett, CIO, Kansas City, MO; **Additional Leads: Jason Whittet**, Rockefeller Foundation, and **Alex Huppenthal**, Aspenworks, Ltd.

Presenters:

- Hardwired Privacy by Design: **Scott Shipman**, General Counsel, Verizon Smart Communities, and **Tahir Khan**, Global Products and Solutions Information Security Officer, Verizon Smart Communities
- Virginia State Data Governance: **David Ihrie**, Chief Technology Officer, Center for Innovative

Session attendees included more than 50 potential partners from diverse sectors working in the field of data security, big data, and solutions for data analytics. Discussions focused on projects that are currently

ongoing within SuperClusters as well as those with relevance or potential to become future Action Clusters, as shown in Figure 2.3.

- FiWARE (ongoing)
- Kansas City, MO (ongoing)
- Bellevue, WA (ongoing)
- U. of Southern California / Los Angeles, CA: I3 Consortium
- Seat Pleasant, MD / IBM Intelligent Operations Center
- Akron, OH: Akron Connect
- Oakland, CA: Smart Oakland
- Pittsburgh, PA / Carnegie Mellon: Smart Infrastructure

Figure 2.3. Ongoing Projects and Emerging Data Platforms/ Governance and Cybersecurity/ Privacy Action Clusters

2.5.4. *Utilities and Cybersecurity/Privacy*

This session focused on a range of topics related to municipal utilities, including smart, connected and innovative energy, water and waste management systems; intelligent ways to reduce water lost through leaks in water transmission and distribution; weather analytics solutions for cities; improving city resilience through advanced energy systems; and new strategies for zero waste.

SuperCluster representatives and speakers (inset) provided perspectives on advances in connected systems being used for utilities. With more connected devices made possible via the IoT, Blockchain and other business models as well as concepts that incorporate smart grid, advanced lighting and other technologies are emerging. Mobile, online, and networked telecommunications are fueling innovations in these areas. Cybersecurity and protection of personal information will play a key role as utilities adopt new concepts which utilize consumer information.

The Utilities SuperCluster covered a range of smart city solutions for energy, water and waste management. Photo credit: Energetics

Utilities SuperCluster

Chair: Kreg Christoff, Vice President, Motorola Solutions

Presenters:

- **James Chong**, CEO, Vidsys
- Smart Grid: **Gary McCarthy**, Mayor, City of Schenectady, NY, and **John P. Coluccio**, Signal Superintendent, City of Schenectady, NY
- Optimizing Energy and Labor Costs using Secure and Private Connectivity: **Usha Mohan**, Chief Architect, AT&T Global Business - Public Sector Solutions

The session included about 45 participants and potential partners with an interest in innovative approaches for utilities. A number of ideas and solutions were identified with potential for new Action Clusters, as shown in Figure 2.4.

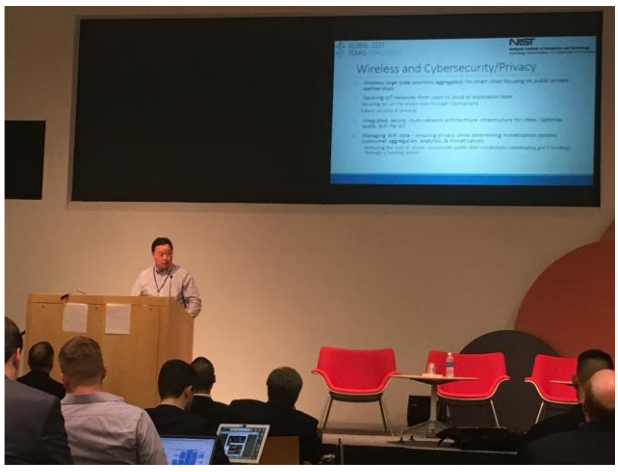
- Smart Street Lighting – Street lighting system (LED, solar, etc.) with possible sensors to improve security and public safety (e.g., video surveillance, air quality, WiFi connectivity, etc.). CS/P component is related to the security and privacy of sensor data.(Bharatpur, Nepal and Sebrany Perai, Malaysia)
- Secure Smart Lighting – Use of lighting platforms to provide safer policing, enhanced traffic flow, WiFi in high risk areas, capture of health-related data, etc.). Security and privacy of data collected and how data will be used are primary CS/P components.
- Community Iterative Smart Energy District – District energy model where energy from small sources such as rooftop solar and electric vehicles (EVs) can be produced/sold; includes transactive energy and Blockchain elements; and secure transactions with personal identity protection.
- Smart Secure Data Analytics for Municipal Utilities – Systems to enable secure actionable use/ interpretation of massive amounts of data from utilities; secure data exchange between departments/ divisions and citizens; and how to aggregate data to create operational efficiencies.

Figure 2.4. Emerging Utilities Action Clusters

2.5.5. *Wireless and Cybersecurity/Privacy*

The Wireless and Cybersecurity/Privacy session focused on Public Wi-Fi for communities; best practices for the deployment of wireless systems in municipalities; and solving challenges in deploying/sustaining wireless systems over time.

SuperCluster representatives and speakers from government (inset) provided perspectives on successful projects that are currently ongoing in San Mateo County and San Leandro, CA, and in Singapore. Speakers from the private sector provided insights on new technologies and solutions, including an IoT platform that spans wireless devices to cloud servers and enables rapid development and deployment of various connected solutions. The session was attended by about 30 potential partners with an interest in



Wireless SuperCluster representatives discuss key solutions and concepts. Photo credit: Energetics

Wireless SuperCluster

Chair: Tony Batalla, CTO, San Leandro, CA, and **Benny Lee**, Project Manager, San Mateo County, CA

Presenters:

- SmartWAVE, San Mateo County, CA, Roaming Wi-Fi, San Leandro, CA: **Tony Batalla**
- San Mateo County IoT Plans: **Benny Lee**
- Secure, Federated, Free Connectivity in a Digital Economy: **Khoong Hock Yun**, Chief Digital Evangelist, Info-Communications Media Development Authority of Singapore
- Fybr/Amazon Web Services Team

optimizing wireless for municipalities. A number of potential concepts and solutions were identified with potential for new Action Clusters, as shown in Figure 2.5.

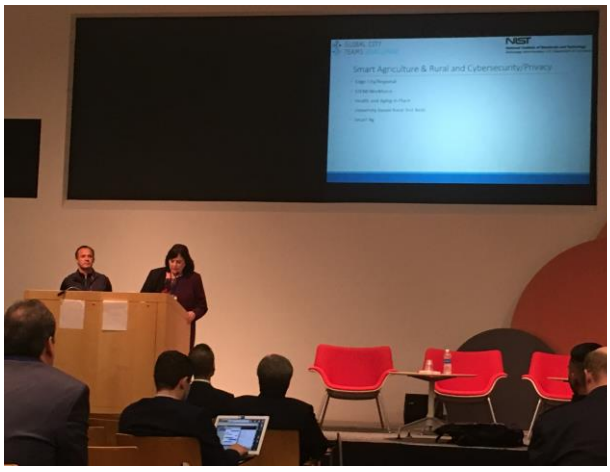
- Wireless Large Scale Solutions Aggregation for Smart Cities – Creating new replicable large-scale solutions for wireless in cities, with a focus on effective public-private partnerships.
- Securing IoT networks from Users to Cloud at Application Layer and Securing IoT on the Device Side through Cryptography – Exploring hardware requirements around security to enable system-wide protection against cybersecurity threats; solutions that ensure client security and privacy.
- Integrated Network Architecture for Cities – Integrated, secure, multi-network architecture infrastructure for cities; optimizing public WiFi for IoT; and developing use cases with multiple protocols (e.g., LoRa, WiFi).
- Managing and Reducing the Costs of WiFi Networks – Ensuring privacy while determining monetization options (consumer aggregation, analytics, and monetization); reducing the cost of secure, sustainable public WiFi installations via new funding models; and certificate security or authentication protocols/policies.

Figure 2.5. Emerging Wireless Action Clusters

2.5.6. *Agriculture and Rural Communities and Cybersecurity/Privacy*

This newly formed Agriculture and Rural Communities and Cybersecurity/Privacy SuperCluster covered a broad range of topics, including technologies for increasing the productivity and quality of life for rural communities and agriculturists; improved educational resources; healthcare and ability for aging in place; economic development; and best practices for precision agriculture and livestock management, including better broadband-enabled access.

SuperCluster representatives and speakers from government, non-profits, academia, and universities (inset) provided perspectives on some of the recent developments in smart technology impacting agriculture and rural communities.



The newly formed Agriculture and Rural SuperCluster brought together a diverse set of stakeholders interested in improving rural communities. Photo credit: Energetics

Agriculture and Rural Communities SuperCluster

Chairs: Jean Rice, Senior Broadband Program Specialist, NTIA; **Debra Lam**, Managing Director, Smart Cities and Inclusive Innovation, Georgia Institute of Technology; and **Mo Shakouri**, Director, Community Broadband initiative, Joint Venture Silicon Valley

Presenters:

- Smart Farming: **Mark Lewellen**, Manager, Spectrum Advocacy, John Deere on Smart Farming
- Smart Agriculture Innovation: **Gabriel Youtsey**, Chief Innovation Officer, University of California, Agriculture and Natural Resource
- Telehealth: **Mahesh Nattanmai**, Chief Digital Health Strategist, New York State Health Department
- Results of the NSF Workshop on Smart and Connected Rural Communities: **Tho Nguyen**, Department of Computer Science, University of Virginia

The session was attended by about 25 potential partners with an interest in bringing the IoT and innovation into this sector, with benefits to agriculturists and citizens. A number of potential concepts and solutions were identified with potential for new Action Clusters, as shown in Figure 2.6. These will be further explored and developed over the next year.

.

- Edge City/Regional
- STEM/Workforce
- Health and Aging in Place
- University-based Rural Test Beds
- Smart Agriculture

Figure 2.6. Potential Topics for Agriculture and Rural Communities Action Clusters

3. IES-City Framework

3.1. Background

The last day of the 2018 GCTC-SCE focused entirely on the IES-City Framework to further publicize the document and elicit public comments from the community of interest involved with smart city solutions.

3.2. IES-City Framework Workshop Scope and Format

The IES-City Framework Workshop included a series of plenaries and panel sessions to present the results of the draft Framework. About 120 smart city stakeholders from government, industry, professional societies, non-profits, and academia attended the Workshop.

Discussions throughout the day focused on the essential elements of the Framework. These included:

- **Framework Document**: Sets the stage, and describes goals, methodologies and artifacts (how to produce and compose artifacts, their composition, how they can be evergreen, etc.). The goal of the Framework is to provide smart cities with tools that help with the composability of systems.
- **Technology Artifacts**: Allows a side-by-side comparison of technology suites offered/deployed in the market today so developers can see what other organizations are doing and harmonize efforts. Use cases presented included a "day in the life" of a smart city in 10 years, and a scenario of smart city managers making use of the Framework to achieve deployment of a flood management system.
- **Application Management Framework**: Includes pivotal points of interoperability (PPI) and zones of concern (ZofC) alongside the NIST CPS Framework (a central foundation for the IES-City Framework).[10] The Application Framework tool provides a directional database of a breath of applications, readiness/requirements, and benefits.

Table 2 illustrates the full range of topics covered at the Workshop. Plenary presentations are available online.[11]

The Workshop concluded with the beginning of a 60-day review period for the draft IES-City Framework and associated artifacts. All interested participants were encouraged to review and comment to ensure the document is a robust and effective resource for smart city stakeholders. Organizers issued a request for submission of additional case studies; these allow cities to learn from existing applications. The draft Framework and review instructions are available online.[12]

[10] The NIST Cyber-Physical Systems (CPS) Public Working Group, CPS Framework, Version 1 (see footnotes 1 and 2)
[11] https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFrameworkDraftReveal20180208-presented.pdf
[12] https://pages.nist.gov/smartcitiesarchitecture/

Table 3.1. IES-City Framework
Workshop Topics
IES-City Framework Overview **Panel – Framing the Opportunity** (Sokwoo Rhee, NIST, Moderator) • **Bob Bennett**, CIO, Kansas City, MO • **Greg Toth**, IoT Dev Lab, working with DC and Montgomery County, MD • **Derek Loftis**, Virginia Institute of Marine Science, representing Newport News, VA • **Jose Gonzalez**, InterInnov representing FIWARE
USE CASES • Day in the Life of Smart City Resident 2027 • Using the IES-City Framework
APPLICATION FRAMEWORK • Demo Application Framework Tool • Breadth • Readiness • Benefits • Case Studies
TECHNOLOGY ANALYSIS • CPS Framework Concerns • Zones of Concern • Technical Analyses Results
Framework Review Process and Feedback

4. Next Steps

The 2018 GCTC-SC3 kickoff workshop was an important milestone to gauge the level of interest in adopting CS/P as a primary concern for smart city projects. The workshop has successfully catalyzed formation of new teams from around the world including a number of ACs and additional SCs. Given the success of the kickoff, planned events over the next year for GCTC-SC3 will further help ACs and SCs accomplish their goals. These include a Global Tech Jam in Portland, OR and an Exposition of GCTC projects, projected for early 2019. Several SCs are planning their own workshops in 2018 as well.

Various activities continue to occur to build new teams and Action Cluster projects. SuperClusters continue to make headlines by starting new pilot programs and creating smart city blueprints. Projects are diverse and cover the full spectrum of smart city solutions – with many now incorporating cybersecurity and privacy elements.

A number of communities and organizations have announced grants, challenges, and initiatives to get new smart city projects off the ground. These include, for example, the 2018 Smart Infrastructure Challenge (Regional Smart Cities Initiative), which provides grant funding, support resources, and access to project financing. Another effort is the Georgia Smart Communities Challenge, which offers funding and support for Georgia communities working toward a 'smart' future. The NIST Public Safety Communications Division (PSCR) Point Cloud City solicitation takes applications from state and local governments to create a model "Point Cloud City." GCTC will continue to collaborate with such parallel initiatives and create synergy throughout its 2018 round.

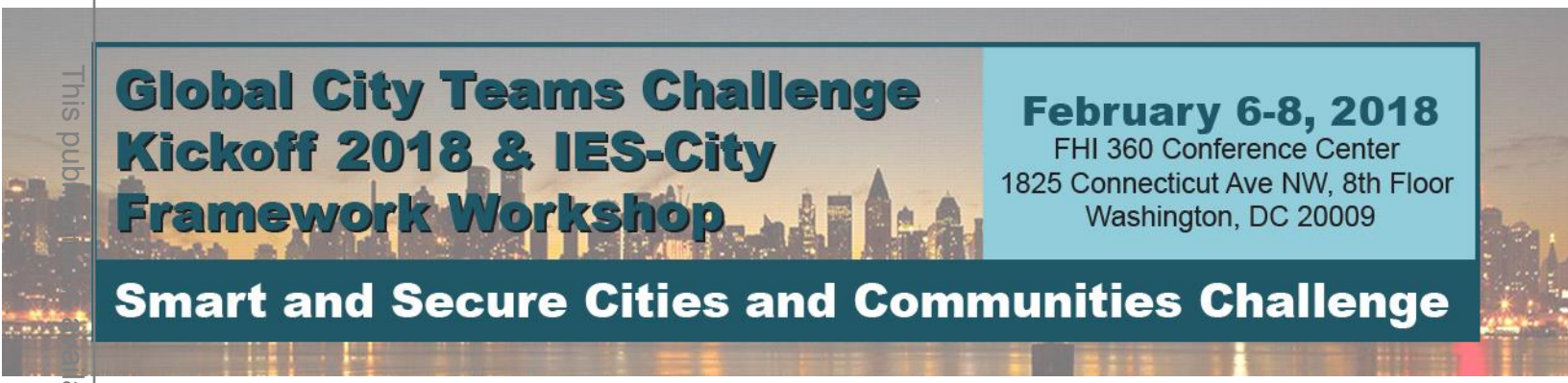
As noted, the publication of the IES-City Framework at the 2018 GCTC-SCE kicked off a public comment period. Additional public comments received will serve to refine and improve the Framework. Additional case studies and use cases will further enhance the usability of the Framework for cities implementing smart solutions.

Acknowledgements

The Global City Teams Challenge (GCTC) 2018 - Smart and Secure Cities and Communities Challenge (SC3) kickoff and Internet-Enabled Smart City (IES-City) Framework workshop event was held on February 6-8 in Washington, DC. The event was co-hosted by the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, and the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T). This report recaps the various sessions held throughout the event.

Thanks are extended to the organizers including Scott Tousley, DHS S&T, as well as to the speakers and panelists who provided their perspectives on future opportunities, needs, and challenges for smart and secure cities and communities. Thanks are also extended to the Energetics team for coordinating and facilitating the event.

Agenda



AGENDA

Tuesday, February 6, 2018

8:00 am	***Registration***
9:00 am – 12:00 pm	**OPENING PLENARY SESSION** ***Main Stage - Academy Hall ABC*** *Overflow Broadcast - Vista Room AB, Angle Room ABC, and Balcony D*
9:00 am	**Welcome** ➢ **Chris Greer**, Senior Executive for Cyber-Physical Systems, National Institute of Standards and Technology (NIST) ➢ **Doug Maughan**, Director of the Cyber Security Division (CSD), Department of Homeland Security (DHS) Science and Technology Directorate (S&T)
9:15 am	**Keynote** ➢ **André Hentz**, Acting Deputy Under Secretary, DHS S&T
9:30 am	**Perspectives from State Governments on Smart Communities and Security/Privacy** ➢ **Tim Blute**, Director of Future, National Governors Association ➢ **Kirk Lonbom**, Acting Secretary, Department of Innovation & Technology, State of Illinois ➢ **Karen Jackson**, Former Secretary of Technology, Commonwealth of Virginia ➢ Fireside Chat: Kirk Lonbom and Karen Jackson, moderated by Tim Blute
10:20 am	**Smart Cities and the Internet of Things (IoT) and Cybersecurity and Privacy** ➢ **Sokwoo Rhee**, NIST: GCTC-SC3 Overview: ➢ **Scott Tousley**, Deputy Director, CSD, DHS S&T: DHS S&T Programs ➢ **Donna Dodson**, Chief Cybersecurity Advisor, NIST Information Technology Laboratory (ITL) and Director of the National Cybersecurity Center of Excellence: NIST ITL and NCCOE Programs ➢ **Martin Burns**, NIST: IES-City Framework Overview
11:00 am	***Break***
11:15 am	**Smart Cities/IoT and Cybersecurity/Privacy continued** ➢ **Allan Friedman**, Director of Cybersecurity, National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce ➢ **David Corman/Meghan Houghton**, National Science Foundation ➢ **Jeb Benson**, Public Safety Communications Research, NIST
11:55 am	**Instructions for Breakout Sessions: Purpose and Process** ➢ **Joan Pellegrino,** Energetics
12:00 – 1:00 pm	***Lunch (on your own)***

Tuesday, February 6, 2018 (continued)

1:00 – 3:30 pm

CONCURRENT BREAKOUT SESSIONS

Transportation and Cybersecurity/ Privacy (Academy Hall ABC)

- Chair: **Skip Newberry**, President, Technology Associates of Oregon and **Wilf Pinfold**, CEO, Urban Systems
  - Connected Intelligent Transportation: **Christine Kendrick**, Portland Bureau of Planning and Sustainability, Oregon
  - Farm to Fork Crop Tracking: **Shawn Irvine**, Economic Development Director, City of Independence, Oregon
  - Protecting user Data in the Smart City scenario: the case of the NGSI Encryption Layer w/FIWARE and Mexico City: **Nestor Velasco Bermeo**, Researcher, Computer Science Department - Tecnologico de Monterrey

Public Safety and Cybersecurity/ Privacy (Vista Room AB)

- Chair: **Michael Dunaway**, Director, NIMSAT, University of Louisiana, Lafayette
  - Recent trends in the public safety cybersecurity landscape: **George Popovich**, Director of Products & Services Cybersecurity Governance, Motorola Solutions
  - A strategic approach to IoT security: Focus on Public Safety mission: **Andrew Osborn**, Lead Mobile Cybersecurity Architect, AT&T Public Sector Solutions
  - Making Cities Smarter and Safer: **Michael Wengrovitz**, VP of Innovation, Mutualink, **Hardik Bhatt**, Leader, Smart Cities and Mobility verticals, Amazon Web Services (AWS)

Utilities and Cybersecurity/Privacy (Balcony Room E)

- Chair: **Kreg Christoff**, Vice President, Motorola Solutions
  - **James Chong**, CEO, Vidsys
  - Smart Grid: **Gary McCarthy**, Mayor, City of Schenectady, NY, and **John P. Coluccio**, Signal Superintendent, City of Schenectady, NY
  - Optimizing Energy and Labor Costs using Secure and Private Connectivity: **Usha Mohan**, Chief Architect, AT&T Global Business - Public Sector Solutions

All participants are invited to participate in professionally facilitated breakouts to build new Action Clusters and/or add partners to existing Action Clusters.

The objective is to build as many Action Clusters as possible that are aligned with the goals of 2018 Global City Team Challenge (GCTC) and the Smart and Secure Cities and Communities Challenge (SC3).

Data Platforms/Governance and Cybersecurity/Privacy (Angle Room ABC)

- Chair: **Bob Bennett**, CIO, Kansas City, MO, additional leads: **Jason Whittet**, Rockefeller Foundation, and **Alex Huppenthal**, Aspenworks, Ltd.
  - Hardwired Privacy by Design: **Scott Shipman**, General Counsel, Verizon Smart Communities, and **Tahir Khan**, Global Products and Solutions Information Security Officer, Verizon Smart Communities
  - Virginia State Data Governance: **David Ihrie**, Chief Technology Officer, Center for Innovative Technology
  - WiseTown – Situation Room: **Andrea Cruciani**, CEO, TeamDev srl, **Shawn Irvine**, Economic Development Director, City of Independence, Oregon

Breakouts begin on Tuesday and continue into Wednesday. Each session will begin with a few 2018 teams describing their project goals and cybersecurity/ privacy considerations,

	Wireless and Cybersecurity/Privacy (Balcony Room D) ➢ Chair: **Tony Batalla**, CTO, San Leandro, CA, and **Benny Lee**, Project Manager, San Mateo County, CA o SmartWAVE, San Mateo County, CA, Roaming Wi-Fi, San Leandro, CA: **Tony Batalla** o San Mateo County IoT Plans: **Benny Lee** o Secure, Federated, Free Connectivity in a Digital Economy: **Khoong Hock Yun**, Chief Digital Evangelist, Info-Communications Media Development Authority of Singapore (IMDA) o Fybr/AWS: **Mrinal Wadhwa**, CTO, Fybr, **Sri Elaprolu**, Global Leader & Senior Manager, Public Sector IoT, AWS	*followed up by facilitated discussions by all attendees.*
	Smart Agriculture & Rural and Cybersecurity/ Privacy (Balcony Room C) ➢ Chair: **Jean Rice**, Senior Broadband Program Specialist, NTIA, and **Debra Lam**, Managing Director, Smart Cities and Inclusive Innovation, Georgia Institute of Technology o Smart Farming: **Mark Lewellen**, Manager, Spectrum Advocacy, John Deere on Smart Farming o Smart Agriculture Innovation: **Gabriel Youtsey**, Chief Innovation Officer, University of California, Agriculture and Natural Resources	
3:30 – 3:45 pm	**Networking Break**	
3:45 – 5:00 pm	**Plenary Cross-Connection Session (for all attendees)**	***Academy Hall ABC***
5:00 pm	**Adjourn Day 1**	

Additional Meetings on Feb 6, 2018

- **Smart Building Action Cluster Launch**: 5:00-6:00pm (Vista Room AB)
  NTIA, NIST and the Telecommunications Industry Association invite you to the launch of the Smart Building Action Cluster (SBAC). This SBAC will focus on the crucial nexus of smart buildings and smart communities' interoperability. We hope you will join us for the SBAC launch and brainstorming discussion.
- **Data Governance SuperCluster Sidebar Meeting**: 5:00-6:00pm (Angle Room ABC)
  The Data Governance and Exchange SuperCluster aims to address the challenge of building a governance and exchange model for IoT data and a plan for governments and technology providers to successfully customize and deploy it. The group will work to collect best practices and produce blueprints for data exchange and governance, as well as deployed proofs to share with other teams and stakeholders.
- **Education SuperCluster Interest Group Meeting**: 5:00-6:00pm (Balcony Room C)
  The Education SuperCluster assembled in response to a critical need identified in other SuperClusters in GCTC. The lack of education, training, and awareness of advanced technologies in some urban environments is a major hurdle in the adoption of innovative technological applications. This group plans to identify and share best practices in areas including, but not limited to, digital awareness, online learning, and workforce development.
- **Public Safety SuperCluster (PSSC) Sidebar Meeting**: 5:00-6:00pm (Balcony Room D)
  The PSSC is holding an informal session for Action Cluster and City Team members who want to join the Executive Leadership Team of PSSC and help define future directions in Smart Public Safety. GCTC members interested in disaster preparedness, community resilience, crisis communications, infrastructure protection, First Responder technologies, and related fields are welcome to join and help build the PSSC Team.

Wednesday, February 7, 2018

8:00 am	***Registration and Networking***	
9:00 – 10:30 am	**PLENARY SESSION** ***Academy Hall ABC*** **CYBERSECURITY AND PRIVACY FOR SMART CITIES AND COMMUNITIES** ➢ Moderator: **Scott Tousley**, Deputy Director, CSD, DHS S&T ○ **Erin Kenneally**, Program Manager, CSD, DHS S&T ○ **Bob Bennett**, CIO, Kansas City MO ○ **David Heyman**, Co-founder, Smart City Works and Past DHS Assistant Secretary of Policy ○ **David Choffnes**, Assistant Professor, Northeastern University	
10:30 – 10:45 am	***Break***	
10:45 am – 12:00 pm	**CONCURRENT ACTION CLUSTER TEAM BUILDING BREAKOUTS**	*During breakouts, new partners and Action Clusters continue to build and expand their teams.* *At the end of the day, each group will report on the newly formed teams and potential projects.*
	Transportation and Cybersecurity/ Privacy (Academy Hall ABC) ➢ Chair: **Skip Newberry** and **Wilf Pinfold** ○ Transportation Data Analysis - **Catherine Nikolovski**, Hack Oregon ○ City Data Security and Privacy - **Isaac Potoczny**-Jones, Tozny	
	Public Safety and Cybersecurity/ Privacy (Vista Room AB) ➢ Chair: **Michael Dunaway** ○ UAS-borne wireless networks: **Kamesh Namaduri**, University of North Texas	
	Utilities and Cybersecurity/Privacy (Balcony Room E) ➢ Chair: **Kreg Christoff**, Vice President, Motorola Solutions	
	Data Platforms/Governance and Cybersecurity/ Privacy (Angle Room ABC) ➢ Chair: **Bob Bennett**, additional leads: **Jason Whittet**, and **Alex Huppenthal**.	
	Wireless and Cybersecurity/Privacy (Balcony Room D) ➢ Chair: **Tony Batalla**, and **Benny Lee**	
	Smart Agriculture & Rural and Cybersecurity/ Privacy (Balcony Room C) ➢ Chair: **Jean Rice**, and **Mo Shakouri**, Director, Community Broadband initiative, Joint Venture Silicon Valley ○ Telehealth: **Mahesh Nattanmai**, Chief Digital Health Strategist, New York State Health Department ○ Results of the NSF workshop on smart and connected rural communities: **Tho Nguyen**, Department of Computer Science, University of Virginia	
12:00 – 1:00 pm	***Lunch (on your own)***	

1:00 – 3:00 pm	**CONCURRENT ACTION CLUSTER TEAM BUILDING BREAKOUTS**	*During breakouts, new partners and Action Clusters continue to build and expand their teams.* *At the end of the day, each group will report on the newly formed teams and potential projects.*
	Transportation and Cybersecurity/ Privacy (Academy Hall ABC)	
	Public Safety and Cybersecurity/ Privacy (Vista Room AB)	
	Utilities and Cybersecurity/Privacy (Balcony Room E)	
	Data Platforms/Governance and Cybersecurity/ Privacy (Angle Room ABC)	
	Wireless and Cybersecurity/Privacy (Balcony Room D)	
	Smart Agriculture & Rural and Cybersecurity/ Privacy (Balcony Room C) ➢ Chair: **Jean Rice**, and **David Logston**, Senior Director, Public Advocacy, CompTIA ○ Cyber Security and Privacy Issues: **Allan Freidman**, Director Cybersecurity, NTIA ○ Homework gap program in Virginia with partner Mid-Atlantic Broadband: **Melissa Sassi**, Program Manager, Microsoft	
3:00 – 4:30 pm	**BREAKOUT SESSION REPORT OUTS**	
4:30 pm	**ADJOURN**	

Thursday, February 8, 2018 IES-City Framework	
9:30 – 9:45 am	**WELCOME** ***Academy Hall ABC*** ➢ NIST CPS Smart City Effort
9:45 – 11:15 am	**IES-CITY FRAMEWORK OVERVIEW**
9:45 am	**Overview of IES-City Framework**
10:10 am	**Framing the Opportunity (Panel)** ➢ **Bob Bennett**, CIO, Kansas City, MO ➢ **Greg Toth**, IoT Dev Lab, working with DC and Montgomery County, MD ➢ **Derek Loftis**, Virginia Institute of Marine Science, representing Newport News, VA ➢ **Jose Gonzalez**, InterInnov representing FIWARE ➢ **Sokwoo Rhee**, NIST (moderator)
10:55 am	**Day in the Life of Smart City Resident 2027**
11:05 am	**Using the IES-City Framework**
11:15 am	**Break**
11:30 am – 12:35 pm	**IES-CITY FRAMEWORK DETAILS: APPLICATION FRAMEWORK**
11:30 am	**Demo Application Framework Tool**
11:40 am	**Breadth**
12:00 pm	**Readiness**
12:20 pm	**Benefits**
12:40 pm	**Case Studies**
12:50 – 1:50 pm	**IES-CITY FRAMEWORK DETAILS: TECHNOLOGY ANALYSIS**
12:50 pm	**CPS Framework Concerns**
1:10 pm	**Zones of Concern**
1:20 pm	**Technical Analyses Results**
1:50 – 2:10 pm	**REVIEW PROCESS AND FEEDBACK**
2:10 pm	**ADJOURN**

Additional Meeting on Feb 8, 2018

➢ ITE and Transportation SuperCluster sidebar meeting: 2:10-4:00pm (Academy Hall ABC)

Acronyms/Abbreviations

AC	GCTC Action Cluster
AV	Autonomous Vehicle
CIO	Chief Information Officer
CSD	Cyber Security Division
CPS	Cyber-physical system
CS/P	Cybersecurity/privacy
DHS	U.S. Department of Homeland Security
DHS S&T	DHS Science and Technology Directorate
DOC	U.S. Department of Commerce
EV	Electric vehicle
GCTC	Global City Teams Challenge
ICT	Information and communications technology
IES	IoT-Enabled Smart City
IoT	Internet of Things
ITL	NIST Information Technology Laboratory
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunication Union
JTC1	Standards development environment for ICT standards
NCCOE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
SBAC	Smart Building Action Cluster
SC	GCTC SuperCluster
SC3	Smart and Secure Cities and Communities Challenge
STEM	Science, technology, engineering and mathematics

Useful Links

Global City Teams Challenge

https://pages.nist.gov/GCTC/

2018 GCTC Kickoff: Smart and Secure Cities and Communities

Event Website

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

International Technical Working Group on IoT-Enabled Smart City Framework (IES)

Website and Draft IES-City Framework

https://pages.nist.gov/smartcitiesarchitecture/

Presentations

https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFrameworkDraftReveal20180208-presented.pdf

Cyber-Physical Systems Public Working Group (PWG)

Website

https://pages.nist.gov/cpspwg/

CPS Framework, Version 1.0

https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

CPS Framework Overview, Version 1.0

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf