Homeland Security
Science and Technology

Homeland Security Science and Technology Advisory Committee (HSSTAC): Subcommittee on Internet of Things

Internet of Things Smart Cities Report

March 10, 2017

Homeland Security
Science and Technology

This publication is presented on behalf of the Homeland Security Science and Technology Advisory Committee, Quadrennial Homeland Security Review Subcommittee, Cybersecurity, chaired by Dr. Vincent Chan with contributions from Dr. Cynthia Dion Schwartz, Chief Keith Bryant, Mr. William Crowell, Mr. Byron Collie, Chief Jay Farr, Dr. Eric Haseltine, Dr. James Hendler, General Harry Raduege, USAF (Ret), Mr. Gary Schenkel, Dr. James Schwartz, Mr. John Sims, Mr. Daniel Dubno, Dr. Kathie Olsen, part of recommendations to the Department of Homeland Security, Under Secretary for Science and Technology, Robert Griffin (Acting). This report was prepared by the Internet of Things Smart Cities Subcommittee under the Homeland Security Science and Technology Advisory Committee at the request of Dr. Reginald Brothers, Under Secretary for Science and Technology.[1]

<Signature on File>

_____

Vincent W.S. Chan
The Joan and Irwin Jacobs Professor of EECS
Massachusetts Institute of Technology

HSSTAC Staff: Michel Kareis, HSSTAC Executive Director/DFO and Gretchen Cullenberg, IoT Smart Cities Subcommittee support.

[1] Certain parts of this report were based on prior works of Professor Vincent Chan and his doctoral candidate Manishika Agaskar, captured by her in an internal MIT memo titled: IoT/Smart-City, May 2016.

Homeland Security
Science and Technology

Subcommittee on Internet of Things Smart Cities Report

Charge of the committee

The Under Secretary for Science and Technology (USST) seeks guidance and recommendations on the strategic path forward with regard to developing recommendations to strengthen Science and Technology (S&T) efforts as they relate to the Internet of Things (IoT) and Smart City. Specifically S&T is interested in "how can DHS best develop a framework for managing constantly changing information from various IoT data streams, particularly in limited time and with imperfect information such as the case when one or more networks experiencing unusual latency or outages during an emergency response situation as it relates to Smart Cities". In support of this effort, the USST has asked the Homeland Security Science and Technology Advisory Committee (HSSTAC) to establish a subcommittee to review, discuss and advise the HSSTAC by engaging private industry and academia on critical issues, best practices and current and future capabilities of public and private sector commercialization, pivotal technology research and development, technology transition and technology transfer programs.

This subcommittee facilitated discussions with industry, government agencies, thought leaders and other private sector stakeholders on the best practices and key potential R&D investments for these efforts which are critical for maximizing S&T's mission and fulfilling the USST's responsibilities pursuant to 6 U.S.C. 182. The ultimate goal of the subcommittee was to develop recommendations on, among other things, strengthening and adding to S&T's current efforts and ways that S&T can improve its relationships with traditional and non-traditional private sector partners and stakeholders and also other government agencies with relevant technologies and in place infrastructures.

This subcommittee had four objectives:

1. Identify what the Smart City of the future will look like.
2. Identify what the security challenges will be.
3. Identify steps or processes on how to make Smart Cities more resilient.
4. Recommend how the government can compose new applications on top of the richness of the deployed IoT and what additional research and development is necessary.

Introduction

IoT, broadly defined, encompasses current sensors, networking infrastructure, computing and storage elements as well as future 5th generation cellular and fiber architectures, new cognitive networking paradigms for heterogeneous networks and data analytics. The vast amount of potential data from sensors and mobile devices, the increased traffic demand from end-users, and the ever-increasing number of end-users (up to 50 Billion worldwide) will require smarter

approaches to sensor, network and computing resources deployment, interconnection, usage and management.

Researchers and technologists have envisioned a wide range of Internet of Things applications; the most prominent of these fall into the general areas of public safety, healthcare, “smart grid” power infrastructure, vehicular telematics including autonomous vehicles, manufacturing and logistics, and, of course, entertainment. A significant portion of IoT research and development is application-focused, either identifying new use cases for the integration of sensor networks and mobile devices with the greater Internet and computing/storage elements connected by the network or describing the infrastructure and protocols required for the more complex of these use cases. Additionally, research and development in big data analytics continues with an eye towards processing the vast expected quantities of generated IoT data. One critical issue identified by the committee is the security aspect of IoT/Smart-City. These include end-devices, networks and computing and storage elements.

The general consensus seems to be that machine learning will be the basis of a lot of IoT data processing. One issue to be addressed is the value of historic data in handling extreme “black swan” events (such as a “zero-day” attack on the network or the end devices), especially for time-critical applications. Black Swans by definition have not occurred before and would not be in any data base or historic data. Thus, pure learning algorithms are likely not to be adequate in dealing with Black Swans. A class of different techniques must also be brought into the solution space of the problem

On the software side, a considerable amount of research and development has been done to develop IoT “middleware” solutions to enable easy integration of heterogeneous devices with different purposes, data formats, and probably different manufacturers. This is especially relevant for what is sometimes known as the “Web of Things:” the interconnection, perhaps via IPv6, of web-enabled devices. A common software platform ideally would enable rapid deployment of “composable applications,” applications that utilize available IoT nodes in new ways. However, multiple standards continue to be developed and the question is ‘what is the role of the government in standards setting?’

The utility of composable IoT could be vast – and indeed the benefit of composability is that we need not know today what we may need tomorrow – but the political issues will be as complex if not more as the technical issues. A critical point is that there would need to be some method of defining “available” information so as to take privacy and user permissions into account. Privacy and human rights are clear examples where the technical and political interact, but there are others as well. Different standards bodies will have competing priorities; where the U.S. Government will prioritize security, the IEEE may prioritize fairness while commercial companies put profit as their priorities. In any case, the global marketplace may reject the options put forth. The adoption of middleware could have unintended consequences, e.g. an artificial monopoly and the resultant stifling of innovation. Thus even the technical aspects of the IoT architecture will be dependent on the resolutions of political questions.

Summary of findings and recommendations

1. **What will the Smart City of the Future look like?**

The current trend towards connecting everything to anything else in order to maximize efficiencies of productivity (IoT) dominates attentions of city managements. Major cities around the world have attempted to capitalize on the concept to make city services, government, management, Public Safety and Public Works/ delivery of services more accessible, transparent, effective and efficient. We have also seen that disparity in the delivery of service can lead to the disenfranchisement of segments of populations. (i.e. HVE, Homegrown Violent Extremist)

In the near term, (3 to 7 years), the following (not exhaustive) are likely to occur:

a. Smart Cities will have driverless cars in many of the major cities mixed with traditional transportation.

b. There will be an increase in centralized control of utilities and some services including the use of satellites, cellular, fiber WAN/MAN/LAN (wide area network, metropolitan area network, local area network) for networking, standardized applications, centralized and distributed data repositories and computing (e.g. fog computing).

c. There will be lower power protocols (new) and more energy harvesting.

d. *In order to properly implement the Smart Cities of the future standards are needed to support data interchange. There is the concern that propriety protocols may impede interoperability leading to having government regulators and agencies to be involved.

e. *Data analytics will be automatically applied directly to sensed objects like automobile traffic flow.

The government most likely will have to be involved in the last two items*.

In the longer term, (seven plus years), there following items also will be in play:

a. Ubiquitous sensors and actuators.

b. Proliferation of networks to support data from the Internet of Things.

c. Widespread use of CCTV/sensors with built in biometric recognizers.

d. *Integration and control systems to support decisions with quality information and efficient and responsive city services.

e. *New applications for businesses, government and citizens to access the IoT and data analytics recognizing outliers and potential compromises, etc.

f. *IoT security rising to the forefront and its potential applications to protect cyber-physical systems.

Items* (d) through (f) indicate likely government involvement. These are security related issues and often require insights of multiple systems under different jurisdiction and make for correlation and cross-checks.

Disaster Response and Emergency Networks

The potential of ubiquitous communications devices to assist in disaster relief scenarios is a promising area of current IoT research. It is also an area that the commercial sector has little incentive – or worse, a competitive disincentive – to pursue. Improved capabilities influenced by the government in directions of interests can have many positive effects on homeland security. These include national security and emergency preparedness, crime prevention, first responders' capabilities, transportation efficiencies and effectiveness, energy efficiencies and effectiveness, educational improvements, retail business efficiencies and effectiveness, and all aspects of the entertainment industry.

Battery-powered smart devices that survive a critical infrastructure failure could (via multiple short-range device-to-device hops) replace an unusable long-range communications channel. IoT devices could not only provide important situational data to both remote operations centers and first responders on the scene, but could also supplement the short-range radios carried for low data rate voice communications. The energy limitations on such a network are obvious – but the goal would be to enable temporary (especially for emergencies) network capabilities while more permanent solutions were developed. The challenge is that vendors of IoT products have no incentive to cooperate with one another (i.e. share their designs and allow access to their devices) to create an integrated crisis response network. Furthermore, end-users have little incentive to allow their devices to be co-opted for such a purpose, especially given privacy concerns. Emergency networking then presents a natural setting for government investment in the IoT. For example the government can arrange full access of the architecture of each individual vendor so it can practice with and, in an emergency, deploy an interconnected architecture to make use of all possible assets in the field.

All connectivity may not be necessary all the time, so in the interest of security and efficiency, ability to connect and disconnect when appropriate is paramount. In addition, all components may not be willing to connect, so a critical review must be undertaken of the value and need to connect. Connectivity and or collecting and archiving data just for the sake of having it without an identified purpose only adds to the vulnerability of the network and the data base. In fact, some components or some data may not be accessible due to proprietary information, laws (e.g. CJIS, Criminal Justice Information Services), or purely personality driven. A smart app/account will be able to determine if a virtual connection, separate data set or redacted capabilities may suffice. An operational construct should be developed (and modeled) in advance that identifies the need, demonstrates the value to the whole and or the separate entities before technological capacity can be properly resourced and developed (essential or useful data only and flexibility to

exclude and or incorporate new sets as the needs change). This 'safe' practice is especially important for cyber-security.

Interoperability between the delivery of services, public works and public safety enhances quality of life and will also contribute to quality of life issues that have societal impact such as HVE and criminal activities. Connectivity such as this will contribute to transparency in the delivery of services and reduce misperception of delivery.

Technologies must be developed to serve a variety of service delivery. Technologies developed for traffic and crowd control can be leveraged to serve a large sporting event as well as a needed evacuation or routing of emergency service delivery. The Common Operating Picture (COP) must serve multiple users to include intelligence, dispatch of activities, data analytics, determination of distribution of resources and ability to connect and disconnect to the IOT/ Smart City Platform as necessary. Here near real time synchronization of data bases must be enabled by networks with low and predictable delays and good data security protection.

Congress created the First Responder Network Authority (FirstNet) under the U.S. Department of Commerce to develop and deploy a nationwide public safety broadband network that would enable first responders to communicate across departments and municipalities. FirstNet is an attempt to address the repeated instances of communication failure during crises: the incompatibility of police, fire, and Port Authority radio systems during the 9/11 attacks, the infrastructure collapse in the aftermath of Hurricane Katrina, and more recently, communications breakdowns during Hurricane Sandy, the Boston Marathon bombing, and even the Ferguson, MO protests. Across the U.S., radio systems used by different units are often incompatible, and the sheer volume of traffic during events and catastrophes can incapacitate whole networks. In Japan the Fukushima earthquake disabled the communication infrastructure which took 30 days to restore (ref: Keynote speech by Minister of Telecommunication Infrastructure, Japan at OFC, Optical Fiber Communication Conference, 2013). The lack of communication prevented the first responders to be more effective in the disaster relief efforts during the critical first few days. The Japanese Government now has a program in place to address this problem. The President in reaction to both domestic and foreign disasters tried to put in place an R & D program in 2012, towards solutions for the instant infrastructure problem but was not able to create enough support in the Congress. FirstNet released its RFP in January 2016, so a fully deployed solution is likely years away. The growth of the IoT over that timeframe could result in an enhanced network for first responders, affording them Internet connectivity, low-latency communications, and up-to-date situational awareness from fielded sensors. We envision in the future that incompatible radio systems will be bridged by digitizing communications in the cloud or even via voice-to-text conversion and ad-hoc networking at the edge.

Recommendation**:** *Develop an operational nominal and emergency network construct that will*

maximize the IOT/ Smart City Concept utilizing both Operations and Technical expertise.

The following are brief descriptions of a few alternative emergency network designs:

a. One emergency communications solution contains three major parts: rapidly deployable low-altitude aerial platforms, portable terrestrial stations, and satellites to fill coverage gaps. Low-altitude platforms and portable terrestrial base stations could temporarily replace local infrastructure and re-establish basic Internet connectivity to smart devices that could benefit emergency personnel. Because the coverage requirements of a disaster area would be non-uniform, the optimal placement of these base stations and aerial platforms involves a tradeoff between covering as much area as possible while supplying enough capacity to critical points.

b. A cluster-based hierarchical structure has been proposed for wireless data delivery in an emergency scenario. Since the IoT will consist in large part of wireless sensor networks, a self-organized post-disaster wireless network could supply important situational data. Mobile nodes (such as cell phones carried by first responders) could act as "information ferries" to exchange data between isolated sensor subnets albeit often with no guaranteed delay bounds. Location awareness and trajectory prediction would enable a proactive routing scheme to reduce latency. The deployment of aerial platforms may be necessary to fill coverage gaps and reach remote sensors. A similar "bootstrapped" wireless mesh network can be used as a means of reaching critical sensors and actuators during a power outage by using self-organized smart devices operating on locally-generated energy.

c. If a disaster impacts terrestrial network infrastructure on a large scale, satellite links may be necessary to connect a remote crisis center to the sensors, actuators, and first responders at the disaster site. First responders could carry portable multifunctional radios to communicate with nearby IoT devices (together these radios and sensors would form an ad-hoc "incident area network"), and relay nodes (e.g. UAVs) would provide a satellite connection to the Internet and to the central control center. There is the possibility of using software defined radios at the IoT access points without having to replace first responders' radio with multi-function ones.

All three of these scenarios involve aerial vehicles, highlighting the importance of UAVs to disaster relief applications.

Future IoT Architecture

To fully realize the IoT as it is often imagined, a major change in the current network architecture may be required. Incremental changes such as those that have led to today's Internet will likely not suffice. There are several reasons for this architecture overhaul:

a. Energy efficiency will become much more relevant due to resource constrained IoT

devices.

b. Interference mitigation techniques will be needed to accommodate large numbers of devices with diverse spectrum requirements.

c. Cross-layer protocols will be required to account for differences in latency and reliability requirements among different network nodes and applications.

d. High device mobility combined with higher data rates and larger traffic demands will require new paradigms for routing and congestion control.

e. The "coherence time" of network dynamics is likely to drastically decrease due to highly variable loads and requirements. The network coherence time is the length of time during which traffic requirements across a network or subnetwork are roughly constant. It is thus dependent on the frequency of major events that produce many and/or large data transactions, and also on the frequency and prevalence of node movement.

Network monitoring in the future IoT will need to be smarter to handle large volumes of data traffic. Similarly, network routing and transport protocols will need to be smart about what data is necessary to make decisions. While massive data analytics could still occur in the cloud, collected data will need to be pared near the network edge to avoid overloading the backhaul. Applications that make rapid data-based decisions may not tolerate the transmission delay of sending data to the cloud for processing. For example, disaster prevention for vehicles must have time deadlines of less than ~1-5 mS and thus processing should be done near the edge. We note that transmission delay is determined not by propagation time but by software delays, e.g. electro-optic packet conversion, processing and routing. A balance must be struck to avoid straining limited resources at the edge without congesting the core network. A hierarchical network management structure should be explored as a solution.

2. What are the security challenges?

The committee has identified security as a very serious issue for IoT/Smart-City for public safety and infrastructure protection. Some potential vulnerability areas (not all) were flagged without detailed articulation of threat surfaces, assessment of capability of adversaries, detection and mitigation techniques and gaps in protection tools and techniques. An adequate treatment will need discussions and expositions at the classified level which has not yet been conducted within this committee. Any adequate safeguards will need the collaboration of partner agencies both in the technologies they have and will develop/ed and also their in-place capabilities in the field. DHS only has been and will be able to work on a small subset of these security technologies and deploy necessary infrastructures. Clear and present danger of attacks on our critical infrastructures and services warrant immediate and full attention to mitigate this problem.

Inherent tradeoffs between privacy, performance, security and cost limit the financial incentive for commercial entities to devote adequate attention to the issue. As a result, there is need for additional academic and government development of industry-wide security tools and standards. Research in this area is largely focused on device and/or user authentication and resource-constrained encryption, along with some research on the physical layer security of the IoT. However, having a huge number of objects on the network substantively increases the risks of

insider attacks and constant presence of compromised nodes. *A new security paradigm that allows good operations in the presence of compromised nodes and constant insider attacks* is a major shift from previous models assumed.

There are several different types of security that must be considered. Vehicle safety is an extreme example; communication between vehicles and road-side units about local road information must be accurate and timely. For driverless cars, the threats of denial-of-service or jamming attacks are of particular concern. For large data networks, the integrity of link state data will be important for network control and management functions. With the growth of SDN (software defined networks) and perhaps NFV (network function virtualization), control plane security becomes very critical. If learning algorithms are used in support of network operations, then data contamination can be especially dangerous, impacting not only immediate actions, but also future decisions.

Securing the IoT is an obvious open problem that needs to be addressed from all parties involved in developing and deploying new IoT applications. But security must be addressed in the context of the huge and hugely dynamic future network. Network protocols – including security – must therefore scale to support billions of nodes and to respond rapidly to changes in traffic and link states. Because of the large number of resource-constrained devices entering and leaving the network, it cannot be assumed that all nodes are non-malicious. In fact, the network should be designed under the assumption that some fraction of nodes is compromised, and there should be graceful performance degradation as the size of the compromised fraction grows. There should be a ubiquitous sensing function to assess the integrity of nodes and active query techniques to further vet node integrity. One possibility is to maintain satellite connectivity to most nodes for queries and communicate with the "good" nodes and periodically rekey them.

There are several near term challenges (between now and seven years from now) that needs attentions:

a. Control systems and applications must be secure but also provide easy access to IoT.
b. We must have secure network systems for IoT.
c. Most sensors and actuators are not likely to be secure due to power/computation constraints therefore creating the challenge to accommodate unsecure endpoints but secure the system.
d. Autonomous vehicle hardware and software security.
e. Patching software and updating infrastructure for endpoints in IoT with security.
f. IoT security requires cooperation of multiple entities and organizations but can be impeded by Intellectual Properties and business profit issues.
g. Separation of security and authentication requirements for monitoring and action based channels.

i. Action based channels require significantly more authentication and verification for the execution of control functions.

ii. Any IoT system which can potentially impact life safety should be considered a supervisory control and data acquisition (SCADA) system and subject to certification.

h. IoT security or lack-of can affect the following:

i. Theft of intellectual property or strategic plans.

ii. Physical criminal activity can be increased

iii. Financial fraud

iv. Reputational damage

v. Business disruption

vi. Destruction of critical infrastructure, and can threaten health and safety.

i. IoT systems are likely to use cloud technologies for cost effectiveness which means organizations will have data related to their physical presence and activities potentially stored in locations outside of their control unless they plan for trusted, integrated solutions providers.

j. Different vendors may use separate and non-interoperable cloud provider, leading to a loss of interoperability.

k. Cyber & Physical Security are increasingly interlinked: IoT can be used as an overlay for cyber-physical security applications but also can be used a point of entry and resources for attacks (which has already occurred in the US and elsewhere)

l. IoT is really a SCADA/ICS(Industry Control System) at large and poses the same risks and challenges such as:

i. Patching and upgrading should be planned and executed with foresights (we have a chance to design in now as opposed to limited by legacy SCADA systems). Critical issues to consider include: security of codebases and development channels at vendors, verification of patch veracity before implementation on the IoT device, reboot challenges, and vulnerability management.

ii. The supply chain challenge for trusted systems will expand for consumer and commercial vendors to develop code in less trusted locations.

iii. It is extremely likely that sensitive government entities will end up in commercial facilities that have untrusted IoT systems for efficiency purposes increasing vulnerability for denial of service.

iv. Very hardware oriented IoT implementations will likely face a similar End of Life, legacy and maintenance challenges that the Intelligence Communities and other

embedded systems currently face. Modularity is the solution to allow for an easy upgrade of relevant hardware components.

The long term (seven years and beyond) challenges of IoT security is even more daunting with the wide spread globally of cyber-attack technologies. The following is a set of critical areas to consider:

a. Comprised nodes and fraction of network infrastructure will be routine. A system must be planned for operation in the presence of compromised assets.

b. "Insider" attacks are a distinct possibility. There should be in place automated systems to sense, isolate, mitigate and operate through such attacks.

c. Preventing "normal accidents" and deliberate sabotage in complex composed IoT systems is a must.

d. Security in the dynamic changing IoT system must be maintained.

e. Cyber and physical security are increasingly interlinked. IoT can be used as an overlay for cyber-physical security applications but also can be used as a point of entry for attacks.

f. Data volumes and criticality of network connectivity are going to skyrocket with IoT. This poses questions for how devices function when connectivity is not available and device susceptibility to exploitation in this state. There needs to be a "fail safe" standard for operating these devices in the event of impaired network connectivity's.

g. IoT have massive vulnerability for electromagnetic disruption, either man-made (EMP, electromagnetic pulse; HERF, high energy radiation field etc.) or natural. Similar to the fail-safe situation, IoT devices should have minimal essential functionality that is not dependent on connectivity etc.

h. Plans for disaster recovery and critical systems restoration must take into account distributed sensor networks and loss of communications with responders and devices.

3. **How do we make it more resilient?**

Almost surely, the IoT/Smart-City infrastructure will be attacked in the future either from forces outside the infrastructure or from insider attacks. Isolated cases have already occurred here in the US and overseas. This system should not be fragile that becomes dysfunctional under a limited scope attack. A properly designed architecture should ride through these attacks albeit with degraded performance. Graceful degradation to failures is a necessary property of that part of the system that is depended on for critical services such as first responder support, power and water infrastructure integrity and medical and financial systems. Resiliency to benign failure and attacks requires a planned architecture, hopefully before the infrastructure deployment. The retrofitting of security overlay features on systems are both costly and often in-effective.

Resiliency is a different issue than security. One must resign to the fact that somehow, somewhere, sometime that a part of the system is going to break down, either naturally, because of natural disaster, or due to adversarial attacks. The question is how will the architecture

perform when such events occur? Some architectures might just collapse. Some might heal itself. What are the necessary attributes of those architectures that make it self-healing and at least have some part of the system survives? How does one reconstitute whatever is left and retain some form of infrastructure capability– no matter how thin – to perform the most critical tasks?

The following items should be considered now to make smart cities more resilient:

a. There needs to be a comprehensive security architecture and plan in place.
b. Protecting critical assets against known and emerging threats across the ecosystem, this includes: perimeter defenses, vulnerability management, asset management, identity management, and data protection.
c. Gaining detective visibility and preemptive threat insights to detect both known and unknown adversarial activities including threat intelligence, security monitoring, behavioral analytics, and risk analytics.
d. There should be a substantial increase in strength and ability to recover when incidents occur; through incidence responses, fast adaptive and automated responses to contain damages, analyzing and inferring from forensics, crisis management and reconstitution of thin-line capabilities post-attack.
e. Information sharing and collaboration among agencies and departments is a must.
f. Red Team exercises and certifications are vital for preparation.
g. There will need to be constant monitoring of IoT control systems and improvement on responses to faults.
h. Create a new security paradigm and architecture construct that assumes compromised resources and insider proliferations but IoT still provide useable services.
i. Create an architecture for time-critical applications to react to and function through “black swan” events, e.g. zero-day attacks. Architectural resilience for disaster recovery is key.
j. Create an architecture to management and control plane security, especially with SDN (software defined networks).
k. Use of satellites as thin-line heart-beat network, e. g. for emergency command and control and reconstitution.
l. We will need security research focused on dynamic (but bounded by M2M machine to machine, devices) environments.
m. New standards should be created to support interoperability at different timing and data volume scales.

n. New algorithms to support data fusion and validation/cross-checking of large number of measurements with unknown certainties, including machine learning interfaced with a corrective control system.

o. Create new applications to improve cyber-physical systems security.

p. Develop control system theory where the internal states and feedback mechanisms of networks are intimately affected by inputs (traffic) and network algorithms used.

q. Develop cognitive networking where "network" senses current network conditions to improve resource management based on observables.

4. **How would the government compose new applications on top of the richness of commercial IoT? What would be the add-on Research and Development necessary?**

With all the future commercial, government owned IoT devices and system in place, there is the opportunity to compose new applications on top of these infrastructures. It is not just a DHS exclusive or government exclusive issue. The innovative, commercial sector should participate. The question is can DHS keep track what the industries are thinking about? Can the government also think along with them and use government influence and resources to shape and respond in the right directions. The government's role should be to point to the directions of interests and stimulate research and development by coordination, funding, tax-incentives and also on rare occasion declaration of national emergency.

For example looking at the Local 311 emergency management call system, if the system was augmented to have broader regional and national centers to supplement existing citizen call-in mechanisms this would allow for other regions to help municipalities and states when they are hit with attacks on IoT infrastructure. It would also provide feedback for other disasters that affect a region like hurricanes, flooding, and oil-spills. The following are items that need special attentions:

a. There needs to be increased government funding for R&D to improve the government related Smart City needs.

b. We need to foster architecture of interoperability between services, public works, and public safety for an enhanced quality of life.

c. There needs to be Common Operating Procedure (COP) developed to serve multiple users to include intelligence, dispatch of activities, data analytics, determination of distribution of resources and ability to connect and disconnect to the IoT Smart City Platform as necessary.

d. There needs to be an IoT security "add-on" encryption, especially to control systems to insure security of the system and detect problems in critical infrastructure.

e. IoT sensing will monitor various IoT systems to sense large-scale faults and correlate data among different IoT systems (e.g. atmospheric monitoring with electrical grid with seismic sensing for natural disasters).

f. Applications should be developed to add to the security of other systems.

g. Support the use of IoT, SDR (software defined radios), SDN, and cloud technology to connect multiple radio modalities for emergency disaster relief.

5. What Actions should the government take?

The above should be translated into actionable items that DHS can undertake. Some of these actions are S&T investments, others are interagency collaborations and reaching out more broadly to the industry. The following items are recommendations that the government should consider:

a. Reach across multiple departments and agencies, including state and local government, to create an integrated approach and coordination to protect IoT Smart Cities.

b. Develop an operational construct that will maximize the IoT/ Smart-City concept utilizing operations and technical expertise.

c. The government must develop more focused and secure applications to ride the richness of the commercial IoT.

d. A critical government review must be undertaken of the value and need to connect various sensors, processing and storage, (allowing for connectivity without an identified purpose only adds to the vulnerability of the network).

e. Government funding for R&D must be increased in order to improve the government-related Smart City needs.

f. Create a governance and operating model, identify policies and standards including interoperability.

g. Review and assess management processes and capabilities.

h. Create rapid and accurate risk reporting of all threats.

i. Provide risk awareness and security culture education.

j. It is extremely likely that sensitive government entities will end up in commercial facilities that have untrusted IoT systems for efficiency purposes. Security measures must be developed to mitigate potential threats on denial of service, loss of data in transit and during computing and data integrity.

k. The government may need to look at common criteria like certification processes to develop trust in IoT, particularly for life and safety oriented applications similar to the ARINC 653 specification for avionics systems; use critical mass between localities, state, federal acquisitions to enforce standardization.

l. The government should engage in privacy and human rights discussions in lieu of the new horizons defined by IoT and Smart City.

Summary

IoT/Smart-City is a new paradigm and not merely a linear extension of the Internet. It provides basic services as well as innovative services that can enrich human life. However, the security challenges will be huge due to the large number of deployed devices and possibilities of insider attacks. Currently, there is inadequate considerations of the security aspect and urgently requires attention. DHS should proceed aggressively to catch up to developing threats. Collaborations with other government agencies that have rich tools and infrastructures in place is critical. Close engagement with the commercial sector can also provide forefront knowledge and emerging techniques and systems to keep pace with the rapidly evolving IoT/Smart-City development.