About this Research Brief

CompTIA’s *Building Smarter Cities* research brief examines how federal, state, and local governments are navigating the quickly evolving Internet of Things (IoT) trend, and by extension, the Smart Cities trends. This brief focuses on three primary areas:

- Market Overview
- Adoption Factors: Drivers and Inhibitors
- Policy and Regulatory Issues

The data for this brief was collected via an online survey conducted during June/July 2016. A total of 172 U.S. federal, state, or local government personnel with some degree of technology decision-making responsibility participated in the survey. The overall margin of sampling error at 95% confidence is +/-7.6 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@compbia.org.

CompTIA is a member of the Market Research Association (MRA) and adheres to the MRA’s Code of Market Research Ethics and Standards.

For additional insights into the IoT and related emerging trends, see the following reports and briefs available at [CompTIA.org](http://compia.org):

- *Internet of Things Insights and Opportunities* research study
- *Internet of Things Ecosystem* analysis
- *Mastering the Internet of Things* case study
- *Tech on the Horizon: From VR to Bots* research brief

Several icons used in this report were sourced from [www.flaticon.com](http://www.flaticon.com). Electric tower by Zlatko Najdenovski; Park bench by Eucalyp; Bus stop by Freeipik; Water pipe by Freeipik; and robot by Freeipik. The remaining icons were created by CompTIA.
Key Points

- Many facets of our cities – from transportation and water management to building design and public safety, are ripe for reinvention. Inexpensive computing, sensors, and data storage, coupled with reasonably fast wireless connectivity and a large base of tech-savvy users provide the foundational ingredients for digitizing our cities. Add in cloud computing, big data, artificial intelligence, robotics, and a host of other cutting-edge technologies and a Jetsons-like future seems increasingly within reach.

- The research, conducted among government respondents at the federal, state, and local levels, confirms the continuing transition of IoT and smart cities from theory to practice. Nearly 3 in 4 respondents report having more positive views of IoT today compared to two years ago. Moreover, 11% of government entities claim to have a formal IoT initiative underway, while 25% report some type of pilot project in the works. Many of these early stage efforts can be characterized as smart city initiatives, a sub-segment of the broader IoT trend. The areas where governments see the most likely applications in the short-term include energy management, public safety, and transportation. As the market further matures, expect offerings such as smart cities-as-a-service to gain traction, allowing cities with time or expertise constraints to utilize technology solution providers and MSPs for end-to-end service.

- According to the research consultancy Gartner, an estimated 1.6 billion connected things will be used in smart cities by year-end 2016, a figure projected to grow 42% through 2017. CompTIA’s IoT Ecosystem Framework, which can be applied to smart cities, reinforces the need to think beyond simply the number of connected things and focus on the interdependencies between the hardware, software, services, and rules components. The rules piece, which covers both the regulatory side and the standards side, is where much of the uncertainty surrounding IoT and smart cities developments resides. Policymakers, city leaders, the business community, and private citizens will need to work through issues ranging from security and data privacy, to spectrum allocations, funding, and workforce requirements.
Market Overview

In 1914, one of the world’s first electric traffic signals was installed in Cleveland, Ohio. It directed the rapidly increasing volume of automobile traffic through the familiar red, green, and yellow lights still used to this day. It also included rudimentary logic to prevent signaling conflicts and user error. At the time, this was a momentous technological leap over the existing practice of a police officer standing in the middle of an intersection directing traffic. In the mid-1950s, another innovation surge occurred when the first computer-controlled traffic lights were installed in Denver, Colorado, providing for additional efficiencies and new capabilities such as pressure-sensitive detectors to adjust stop/go times.

As seen in the traffic light example, technology has been making cities smarter for more than 100 years. Of course, measures of ‘smarter’ are relative. Advances in one era are eventually viewed as obsolete in another.

Today, many facets of cities – from transportation and water management to building design and public safety, are viewed as ripe for reinvention. Inexpensive computing, sensors, and data storage, coupled with reasonably fast wireless connectivity and a large base of tech-savvy users provide the foundational ingredients for digitizing our cities. Add in cloud computing, big data, artificial intelligence, robotics, and a host of other cutting-edge technologies and a Jetsons-like future seems increasingly within reach.

This emerging future is commonly referred to as the Internet of Things era. Under this expansive umbrella falls the concept of smart cities. Although definitions and interpretations of this concept are still evolving, elements of the smart cities trend are starting to solidify.

A CompTIA survey of federal, state, and local government technology decision-makers confirms a number of established themes. Even though this data focuses on IoT, many of these elements could just as easily apply to smart cities.

Connected and intelligent systems top the list of words most associated with IoT. Conversely, this implies that cities lacking IoT-enabled smarts remain digitally disconnected and likely missing opportunities for efficiency gains or better service delivery.

Other terms associated with IoT include machine-to-machine, data streams, and futuristic. These semantic opinions are certainly influenced by media coverage of IoT and smart city trends. According to the research, nearly 7 in 10 government respondents report getting news about these topics from tech blogs or tech news websites, while 32% have had internal discussions with colleagues, and 27% were exposed to information at a conference. Top-level awareness of IoT among the government audience stands at about 59%. To put this into context, awareness of 3-D printing (84%), drones (81%), and
autonomous vehicles (76%) rate higher, while technologies such as augmented reality (28%) and chatbots (22%) rate quite a bit lower (see Appendix for more).

With just about any new innovation, the typical pattern is one of low information and confusion in the early stages, followed by information gains and a better understanding leading to more positive views. In the case of IoT, a net 73% of government respondents indicate more positive views today compared to two years ago. The remaining 27% reported unchanged views, or a more negative view, possibly due to increased concern over security risks. While word associations lean towards the favorable, a few negatives do make the list. Fifteen percent of respondents associate IoT with ‘a security disaster waiting to happen,’ with a similar percentage associating it with the quip ‘a solution looking for a problem.’

Sizing the Smart Cities Market:

- According to the Gartner, an estimated 1.6 billion connected things will be used in smart cities by year-end 2016. This figure is projected to grow to 2.3 billion in 2017, an increase of 42%. Smart commercial buildings, transportation, and utilities will account for two-thirds of the total.

- For context, there are nearly 20,000 cities and towns in the United States. The U.S. Census Bureau uses the classification of metropolitan statistical areas (MSAs) to describe cities of 50,000 or more residents; of which, there were 382 of these designations in 2015. Among all cities and towns, 85% have fewer than 10,000 residents.

- The research consultancy MarketandMarkets estimates the smart cities component of the Internet of Things market will grow to $147.5 billion worldwide by 2020, yielding a compound annual growth rate of 23%. MarketandMarkets includes remote monitoring, data, application and device management, building automation, and energy management technologies in its forecast.

- The consultancy McKinsey and Company takes a similar approach, projecting the smart cities component of the IoT market will range between $930 billion on the low end of the forecast to $1.7 trillion on the high end by 2025. See CompTIA’s Internet of Things Insights and Opportunities study for additional IoT market projections.

- The CompTIA smart cities research did not specifically address the dollars spent on smart cities technologies, but applying the adoption rate data to the number of cities and towns with 10,000+ residents translates to about 1,000 locations across the U.S. with some type of formal or pilot IoT and/or smart cities initiative underway. One in three government respondents indicated these initiatives were funded with new budget allocations, confirming the flow of net-new dollars into these investments.
The Path to Smarter Cities

The path to smarter cities will not be a straight line from point A to point B. There will be starts and stops, twists and turns as the many factors at play respond to market and political forces. While there are examples of where smart city solutions can be thought of as discrete products or services, that is more the exception than the rule. For the same reason the smart cities movement is so fascinating – the seemingly limitless number of ideas for making cities smarter – its vastness can be quite daunting.

Applying CompTIA’s IoT ecosystem framework to the smart cities concept provides a mechanism for reducing the scope to more manageable sub-components. The four dimensions of the framework are:

**Hardware**: as it pertains to smart cities, this may include end points such as street lights or parking meters, as well as embedded sensors which could be placed in pretty much anything.

**Software**: software sits at the heart of any smart cities deployment. This may entail the code used to control devices, the platforms for aggregating and managing data, and the mobile apps for real-time interaction. Cloud-based software-as-a-service will take a prominent role, but as is often the case, there will be a need for customized software development to connect legacy city management systems through APIs.

**Services**: while large, well-funded cities may have extensive internal IT expertise capable of managing smart city systems, most will need the assistance of outside experts. This may occur at the initial planning and deployment stages via an IT solutions provider, or via an ongoing relationship with a managed services provider (MSP) for day-to-day support when troubleshooting, security, or maintenance issues arise.
Rules: the first component of this category covers the standards and protocols associated with any technological development. For products to connect to the Internet, to one another, to carrier networks, and so on, requires common standards. The process – or battle as some may say – for setting these standards for IoT and smart city applications is well underway. Industry groups such as the AllSeen Alliance, Open Interconnect Consortium, Thread, Industrial Internet Consortium, Wireless IoT forum, and others are working feverishly to develop standards to govern the many interactions between hardware, software, and services. See the following section and the Appendix for more on the policy and regulatory landscape.

City managers, city IT staff, and elected officials will require, at a minimum, a basic understanding of the framework and its interdependencies. Realistically, though, decisions regarding whether to invest or how to proceed with smart cities initiatives will be contingent on outputs rather than inputs. Smart city investments will be judged by metrics such as improvements to livability, cost savings, citizen engagement, business community support, and votes at the ballot box.

From the research, government respondents have high expectations for the value smart cities’ solutions will deliver. Again, using IoT as a proxy for smart cities, 50% of respondents definitely see value, while 39% indicate probable value. Among perceived benefits, improved decision-making through new or better streams of data ranks highest. Given the many layers of bureaucracy, agencies, jurisdictions, and constituencies, the interest in data-driven decision-making is not surprising. Even small improvements in empowering government workers with the right data at the right time can pay dividends.

Staff productivity and cost savings from operational efficiencies, both closely related to data-driven decision-making, rank second and third as smart city value proposition factors. With the number of public sector employees remaining essentially flat despite a growing population (+38 million since 2000), finding ways to improve staff productivity is critically important to governments and constituents.

### Pushing Ahead: The Factors Affecting Adoption

**Drivers / Value Expectations**

1. New / better streams of data to improve decision-making
2. Staff productivity gains
3. Cost savings from operational efficiencies
4. Automating work processes
5. New / better citizen experiences
6. Better visibility / monitoring of assets
7. Automating infrastructure processes
8. Revenue growth from new products or services

**Inhibitors / Concerns**

1. New cybersecurity risks
2. Lack of skilled workers with IoT expertise
3. Upfront investment cost
4. Interoperability with existing systems / devices
5. Ongoing fees / maintenance costs
6. Complexity / difficulty in understanding how IoT comes together
7. Quantifying the return on investment (ROI)
8. Inability to take advantage of new data streams

*Source: CompTIA’s Building Smart Cities research brief | Base: 372 U.S. government respondents*
Technology, however, is only one piece of the puzzle. The always-useful **people-process-technology** model provides this reminder. Without sufficient investments in staff training and workflow optimization, technology investments rarely reach their full potential. With the many complexities and interdependencies of smart cities’ initiatives, it will be imperative to get the people and process elements right. Note: the [Smart Cities Readiness Guide](#) from the Smart Cities Council provides a useful framework in developing a smart cities roadmap.

Touching on one other adoption driver, the topic of revenue, which is an interesting subject as it relates to smart cities. While city treasurers may be hopeful IoT and smart city initiatives can generate revenue, the research suggests this is viewed as a secondary factor or a longer-term objective. This may be a function of how government revenue is typically characterized as a tax or fee. While there may be opportunities to collect revenue more efficiently, government respondents are likely very aware of the political limits to pushing new fees onto local residents or businesses.

The other side of the adoption equation consists of the inhibitors or concerns that could slow forward progress. Starting with cost, which unsurprisingly is ranked as a concern among survey respondents. Beyond the upfront investment, ongoing service fees are another key variable in assessing IoT and smart city total cost of ownership. Relatively small monthly fees multiplied across many applications or devices can quickly add up, especially if usage exceeds original projections. This operating expense approach (OPEX) may be preferable to heavy upfront capital expenditures (CAPEX), but city planners will need to assess the tradeoffs and implications of these cost scenarios.

The research confirms the astute observation of government respondents that security and workforce will be of paramount importance. The frequency and severity of security breaches targeting government entities has led to a heightened sense of security awareness among government staff at all levels (more on this topic in the following section).

Other challenges involve complexity and interoperability. Even tech-savvy city staff may quickly find themselves in unfamiliar territory when it comes to systems integration. Moreover, pilot projects may be manageable with existing city IT staff, but insufficient when it comes time to scale to full production.

In these situations, cities will likely turn to technology solution providers for assistance. Tech firms with expertise in integration, APIs, cloud computing, data, and security will be key to facilitating smart cities’ growth. Expect concepts such as ‘smart cities-as-a-service’ to gain traction as a means for providing efficient and effective end-to-end solutions. With economies of scale, standardization, and commoditization smart city technologies will become more accessible and affordable over time. The ‘smart cities-as-a-service’ approach brings it all together into what many city planners will view as an appealing option.
Smart Cities in Action

**Water management:** According to a [GovTech.com article](https://www.govtech.com) on smart city IoT applications, the city of Houston, Texas, was losing an estimated 15% of its water – 15 billion gallons each year due to leaky pipes. Using embedded sensors and intelligent pump control systems, the city was better equipped to regulate the flow of water and quickly identify issues before they became major problems. Examples of other water-related problems addressed through smart city solutions include: water quality, irrigation, stormwater runoff, flooding, and household water management.

**Energy conservation:** The New York State Energy Research and Development Authority (NYSERDA) announced it will begin work on a new Real Time Energy Management (RTEM) program. Commercial buildings, especially older structures, consume enormous amounts of energy. The New York State program will leverage sensors, smart meters, and big data analytics to help buildings optimize their energy usage. Beyond energy efficiency at the building or household level, there is a recognized need to upgrade the aging power grid. While a massive undertaking, smart grid technologies have the potential to revolutionize our nation’s approach to energy.

**Transportation:** The U.S. Department of Transportation recently selected Columbus, Ohio, as the winner of its Smart City Challenge. Columbus will use part of the $40 million prize to deploy electric self-driving shuttles, which will operate in conjunction with a new rapid transit center. The system will also enable better vehicle-to-vehicle data exchange and communication with traffic signals and other transportation infrastructure. With traffic and parking frequently cited as major detriments to a city’s livability, many city leaders will view this as a good starting point for smart city initiatives. Along with lighting, traffic or parking management can be thought of as smart city ‘on-ramps.’

**Public safety:** Copenhagen, the capital of Denmark, is frequently referenced as a leader in the smart cities movement. As part of its effort to become the first carbon-neutral city by 2015, the city replaced more than half of its street lights with energy efficient smart LED lights. The intelligence comes in the form of sensors and connectivity to the city’s network. This provides capabilities such as automatic dimming based on time of day or the presence of a full moon, as well as the detection of walkers or bikers with a corresponding increase in brightness for added safety. Other examples within the public safety category include: video surveillance systems with advanced analytics, forest fire fighting drones, and incident reporting and monitoring systems for citizens.

**Environment:** CITISENSE, a consortium of 14 European nations, is working to deploy a network of ‘citizen observatories’ to monitor air quality through wearable sensors. Similar crowdsourcing approaches to environmental monitoring are underway in Beijing and several other cities. With micro-climates and the influences of on-the-ground factors, environmental conditions can vary greatly from neighborhood to neighborhood within a city. Comprehensive networks of sensors and data analytics is a first step in helping cities get smarter and greener.
The Stakes Get Higher for Public Policy

As IoT and smart cities move from concept to reality, questions surrounding the government’s role in these emerging markets become more pressing. Eye-opening incidents involving hijacked cars, zombie refrigerators, or hacked power plants have already made the headlines. There are countless other scenarios, many seemingly out of science fiction movies, that will put governments, citizens, and businesses to the test.

For many regulatory bodies and policy makers, the rapid pace of innovation has quickly eclipsed their best efforts to get out in front of looming issues. While hearings or other activities have taken place in the U.S. Senate, the House of Representatives, the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Department of Transportation, the EU Commission, as well as other industry bodies, most issues remain unresolved.

Somewhat paradoxically, private sector companies want regulatory clarity before pursuing IoT opportunities, and yet, they also express concern over a rush to new rulemaking. After compliance costs, this ranks as the second greatest concern among private sector companies considering IoT initiatives (see below). Given the many parts of IoT and smart cities, new regulations in these areas are especially prone to the law of unforeseen and unintended consequences.

Regulatory and policy discussions will continue to revolve around several core elements:

Security

Security tops the list of IoT policy concerns. With the projected growth of connected devices and the corresponding increase in potential vulnerabilities, especially in new domains such as critical infrastructure, the security component of IoT provokes a number of thorny questions. For example, could security flaws be classified as product defects, making connected cars or appliances subject to recalls? Could support and service firms, such as IT solution providers, electricians, or mechanics, be held responsible for security incidents? Could corporate boards of city council members face liability for security negligence?

The research indicates about 1 in 3 government bodies rate themselves as being well equipped or very well equipped to manage the security component of IoT.

The FTC whitepaper, *Careful Connections: Building Security in the Internet of Things*, outlines key considerations and best practices for securing IoT. This includes not only the need to build robust security safeguards into IoT devices and systems at the earliest stages of development, but also ensuring
ample resources are devoted to providing guidance and training to all types of users, whether they are consumers, small businesses, city employees or multinational corporations. The NIST Framework for Improving Critical Infrastructure Cybersecurity provides guidance for managing the unique security risks associated with critical infrastructure. The power grid is often cited as the example here; others include the water supply, dams, bridges, food supply, communications, defense, and the chemical sector.

Data Privacy

Closely related to security is the issue of data privacy. Most users of technology are not fully aware of the extent to which their personal data is collected, bought, sold and used by various parties. This could be considered the tip of the proverbial iceberg. In a hyper-connected smart cities world, the depth and breadth of data privacy concerns will greatly exceed those of today. Of course, many users willingly hand over certain data in return for access to services or capabilities. Issues related to acceptable use, opt in vs. opt out, right to be forgotten, data breach notification, data ownership, video or drone surveillance, facial recognition, customer privacy bill of rights, and cross-border legalities will be of particular interest to regulators.

Spectrum and Standards

While it is impossible to know exactly how the IoT market will evolve over the next decade, it is fairly certain that IoT advances will strain existing spectrum allocations as billions of new wireless IP devices come online. When a mobile phone drops a call, it is chalked up as an annoyance. Should a driverless vehicle lose its connection, the consequences could be far more severe. Pervasive and robust broadband coverage is a recognized need, which the FCC has taken steps to promote through recent auctions of spectrum well suited for sending mobile signals over long distances. Beyond commercially licensed spectrum, the FCC and tech companies will also need to continue to evaluate options associated with unlicensed or white space spectrum – bands used by Wi-Fi or Bluetooth, for example.

As covered previously in this paper, standards play a pivotal role in ensuring interoperability and efficiency in IoT and smart city ecosystems. Historically, many standards and protocols in the tech space emerge from industry-led efforts, typically in conjunction with ANSI or ISO. In some cases, the market can support multiple competing standards; while in others, a single standard ultimately takes hold. Industry consortiums, trade associations, standard setting bodies, and companies with sufficient clout will continue to hammer away at establishing a market-optimized set of IoT and smart city standards and protocols.

Commerce

The intersection of IoT and commerce has not received as much attention as other higher profile issues such as security, but there are a number of policy questions in this arena that will require attention. Consider the issue of data ownership. It is not always clear who owns what. Do households own the detailed usage data from water, gas and electric meters, or do the utility companies own it? Additionally, what are the rules that govern third party access to this type of data through APIs? Debate is underway in states such Illinois (see Illinois Grapples with Question of Who Owns Energy Data) to sort through these issues, which have potentially far reaching implications for IoT commerce.
Another interesting issue involves taxation. In most cases, IoT products and services will fall under existing tax law. But, could IoT facilitate new ways to assess or collect taxes? Could a cash-strapped state or city decide to impose a tax on certain types of IoT commercial activities? Could a foreign government impose restrictions on U.S. IoT providers which act as an import tax? These scenarios will undoubtedly spur intense tax policy and commerce debates.

**Public-Private Partnerships (PPP)**

Many of the early stage smart city pilot projects were made possible because of public-private partnerships. These arrangements help technology providers run proof-of-concept or beta tests, receiving valuable feedback and insights into go-to-market strategies. City leaders may get access to technology they may otherwise not be able to procure, as well as a firsthand look at how smart city technologies can be deployed. As initiatives move beyond the pilot project phase, public-private partnerships will evolve to best leverage each entity’s strengths.

**Workforce**

As discussed throughout this paper, any discussion of technology must be accompanied by a discussion of workforce. This includes the core IT professionals, such as the network engineers, technology support specialist, software developers, and cybersecurity experts, needed to keep systems running smoothly, as well as the executive leadership and end users who rely on technology for day-to-day operations. CompTIA research consistently shows the demand for tech talent exceeding the supply. With looming retirements and new skills requirements coming online, tech workforce challenges show no signs of abating. As the smarter cities’ trend unfolds, expect the workforce component, including training, certification, and professional development, to become a more critical issue.

<table>
<thead>
<tr>
<th>Manufacturing Sector</th>
<th>Retail Sector</th>
<th>Government Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of compliance</td>
<td>Concern over “questionable” new regulations taking hold</td>
<td>Cost of compliance</td>
</tr>
<tr>
<td>Concern over “questionable” new regulations taking hold</td>
<td>Cost of compliance</td>
<td>Concern over “questionable” new regulations taking hold</td>
</tr>
<tr>
<td>Liability uncertainties</td>
<td>Liability uncertainties</td>
<td>Possibility of having to manage a patchwork of state or international regulations</td>
</tr>
<tr>
<td>Challenge of finding necessary legal expertise to navigate IoT regulations</td>
<td>Possibility of having to manage a patchwork of state or international regulations</td>
<td>Liability uncertainties</td>
</tr>
<tr>
<td>Possibility of having to manage a patchwork of state or international regulations</td>
<td>Challenge of finding necessary legal expertise to navigate IoT regulations</td>
<td>Challenge of finding necessary legal expertise to navigate IoT regulations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hospitality Sector</th>
<th>Healthcare Sector</th>
<th>AMUTC Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of compliance</td>
<td>Cost of compliance</td>
<td>Cost of compliance</td>
</tr>
<tr>
<td>Liability uncertainties</td>
<td>Liability uncertainties</td>
<td>Concern over “questionable” new regulations taking hold</td>
</tr>
<tr>
<td>Concern over “questionable” new regulations taking hold</td>
<td>Challenge of finding necessary legal expertise to navigate IoT regulations</td>
<td>Liability uncertainties</td>
</tr>
<tr>
<td>Tax implication uncertainties</td>
<td>Concern over “questionable” new regulations taking hold</td>
<td>Challenge of finding necessary legal expertise to navigate IoT regulations</td>
</tr>
<tr>
<td>Possibility of having to manage a patchwork of state or international regulations</td>
<td>Possibility of having to manage a patchwork of state or international regulations</td>
<td>Possibility of having to manage a patchwork of state or international regulations</td>
</tr>
</tbody>
</table>

**IoT Regulatory/Policy Concerns by Sector**

Source: CompTIA’s Internet of Things Insights and Opportunities study | Base: 512 U.S. end-user firms
Choosing Sides: The Standards Battle Unfolds

Many organizations have formed in an attempt to define standards for IoT. Standards are needed in each area of the IoT stack—applications, services, network, and access. Some companies are throwing their full support behind a single endeavor, while others are participating in multiple groups in order to be well positioned as the landscape shifts. These are some of the primary groups in this space today:

- **AllSeen Alliance:** One of the first groups to form, AllSeen has used Qualcomm’s AllJoyn device interconnect framework as a foundation. Other members include IBM, Cisco, Microsoft, and LG.
- **Open Interconnect Consortium:** Driven by concerns over Qualcomm’s interests in promoting AllJoyn, the OIC is seeking a more ground-up protocol creation. Members include IBM, Intel, Dell, and Samsung.
- **Thread:** Thread is another ground-up effort to create a networking protocol with better security and low-power features than Wi-Fi, NFC, Bluetooth, or Zigbee. Members include Nest (a division of Alphabet), Samsung, ARM, and Freescale.
- **Industrial Internet Consortium:** The IIC is focused on bringing connectivity and intelligence to industrial applications. Members include GE, IBM, Intel, AT&T, and Cisco.
- **Wireless IoT Forum:** This group has a particular focus on spectrum, with a goal to drive standards and counter fragmentation in licensed and unlicensed wireless M2M market. Members include Cisco, Arkessa, Telensa and WSN.

Source: CompTIA
Government Expectations are High for IoT Initiatives to Deliver Value

How Government Respondents Describe Their IoT Initiatives

- 61% Mostly about enabling and extending technology for broader organization objectives
- 36% Mostly separate and distinct
- 3% Don’t know

Expectations Are High for IoT to Provide Value

- 50% Definitely will provide value
- 39% Probably will provide value
- 11% Likely a distraction from our core mission

Source: CompTIA’s Building Smarter Cities research brief | Base: 172 U.S. government respondents

Providing Context – Self-Assessment of Tech Utilization

Government Self-Assessment of Intensity of Technology Use

- 55% Heavy use
- 32% Moderately heavy
- 13% Middle or lower

Perceptions of Factors Contributing to Above Average Use of Technology within the Government

1. Tech-savvy workforce from top to bottom
2. Top-notch technology partners
3. Senior leadership that supports / funds tech initiatives
4. Reliability of technology – everything just works
5. Ability to identify and quickly implement innovation
6. In-house software development expertise
7. Experimental mindset / avoidance of status quo

Source: CompTIA’s Building Smarter Cities research brief | Base: 172 U.S. government respondents