AVASCENT

WHITE PAPER

APRIL 2016

Smart Bulbs & Smarter Policies:

Preparing Government for the Internet of Things

Jason Layman · Jake Silverman

Everywhere & Nowhere – A successful future for federal IoT starts by understanding the digital phenomenon as much more than the sum of its parts

Smart Bulbs & Smarter Policies:

Preparing Government for the Internet of Things

In the first white paper of a series, Avascent will explore the Internet of Things (IoT) as a digital phenomenon derived from new connections between rapidly evolving sensors and systems that create a dynamic platform for new, innovative, services leveraging data-aggregation and analytics.

KEY THEMES

- **Federalizing IoT will be the biggest test for technology leaders in the next 10 years**
- **Impacted federal spending is projected to rise from $4-$6B/yr in 2015 to $57B in 2025**
- **Commercial IoT approaches fail to address the potential and peril for public sector IT**
- **Industry can help mitigate the biggest risks – and make a business of it**

I. Everywhere and Nowhere: The Emerging Internet of Things

The signs of change are everywhere. The most obvious are the ubiquitous fitness tracker or "smart" bracelets imbued with positional sensors and networking capabilities that would have made a NASA engineer swoon two decades ago. The monumental number of such devices, each with their own IP address, along with smart light bulbs, switches, bathroom scales and other "improved" traditional products, form the foundation of a new technology reality. Tens of billions of new connected devices will come online worldwide in the next few years alone.[1] Consumers and businesses alike understand the potential of the Internet of Things (IoT) and invest accordingly. How about the federal government?

The toughest federal IoT challenges are not necessarily technical. Like many promising solutions climbing the Gartner "hype cycle" curve, IoT can be seen as everything to everyone. Solutions are often defined narrowly, and technically, with one describing IoT as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."[2] Narrow definitions benefit acquisition officers and hardware providers alike, but miss the mark in capturing IoT's full impact and potential to align citizen services with the nation's rising expectations in the digital domain. Narrow definitions also unnecessarily cap IoT's game-changing and enabling potential.

As with the "World Wide Web," the IoT envisioned by Cisco Systems and other IT leaders is more than a basket of technologies. With the right approach, it can form the dynamic connective tissue between government programs, industry partners, senior leadership and frontline users. For citizens, IoT hits the refresh button on their relationship with government services, and enables revolutionary options to

engage and expand on those services. From a contracting perspective, however, the definitions obscure the potential – much of the current understanding of IoT is driven by commercial technology-focused marketing:

- Cisco foresees as many as 100 billion connected devices by 2020. In the time it takes to read this sentence, 100 devices have been added, according to Cisco's metrics.

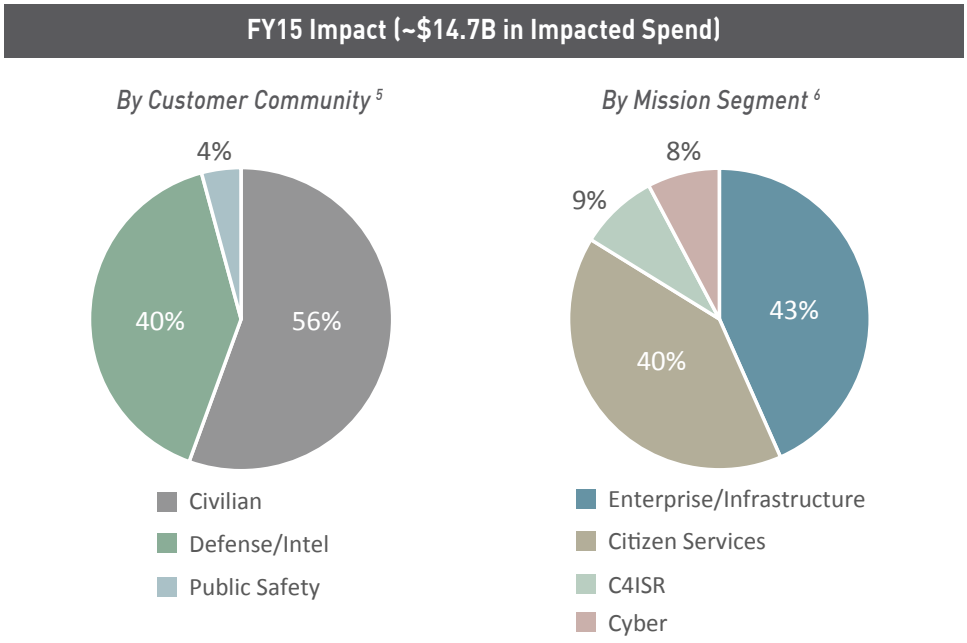
- Consider how IBM describes the recent information haul: "90% of the data in the world today has been created in the last two years alone."[3] The firm estimates there are 9 billion connected devices today, yet as little as 10% of sensor-gathered data is retained.[4]

So just what *is* the federal IoT? And, more importantly, what *can* it become?

II. IoT as a Digital Phenomenon: New Frameworks for New Capabilities

Avascent defines IoT as a phenomenon derived from new connected sensors and systems that create a dynamic platform for new solution / capability innovation.

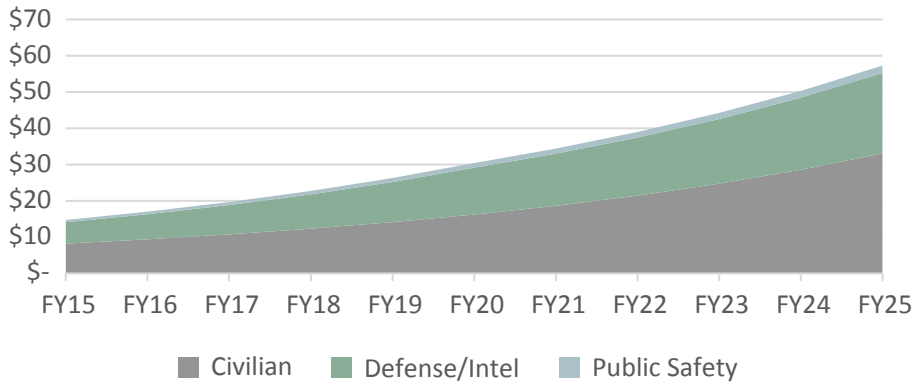
Avascent also believes the lack of a common IoT definition requires establishing company- or agency-specific market context around the applications and investments that will be impacted over a given time horizon. This application-oriented understanding supports a rapidly expanding adoption rate that will be driven or delayed by how well government and industry collaborates.



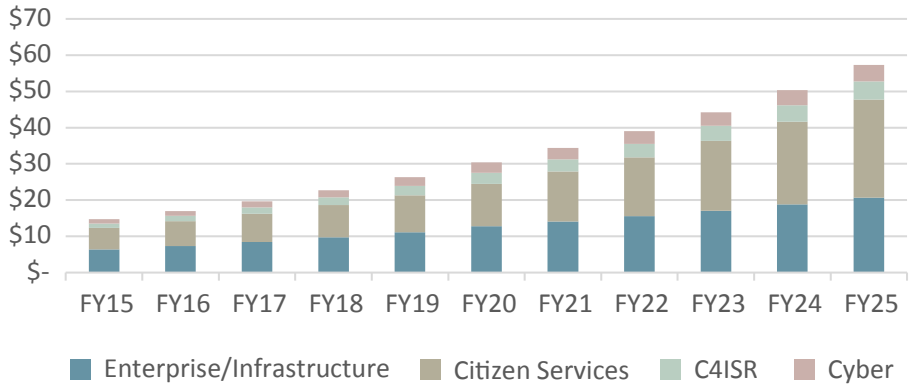
To that end, existing enterprise and mission solution investments should be viewed as promising areas for federal adoption. According to Avascent estimates, in fiscal 2015 alone, there was nearly $16 billion in federal spending with potential IoT applications. By 2025, this could rise to more than $57 billion, with citizen services accounting for the largest share at over $27 billion; defense- and intelligence-related spending could be at least $22 billion.

Federal IoT Impacted Spend ($B)

By Customer Community [5]



By Mission Segment [6]



So far there are few public-sector models for how to approach IoT even as spending is projected to rise dramatically within the next decade. Among agency technology officials, attention is currently spread thinly between fundamental policy challenges like Federal Information Technology Acquisition Reform Act

(FITARA, NDAA 2015), ongoing modernization, and tightened budgets – all overshadowed by the potential policy sea changes following this year's presidential election.

There are official signs, however, that IoT's potential is being recognized by national governments. One notable example is from the United Kingdom. The UK government's approach to IoT focuses upon its transformative potential. As officials wrote in their 2015 strategy report: "There is a danger of trivializing the importance of the Internet of Things through examples that are used to stereotype it – for example, the 'fridge that orders fresh milk'. The Internet of Things has the potential to have a greater impact on society than the first digital revolution." The strategy proposed by the UK is focused on government partnership with industry and research centers, but starts with an appeal for the UK government to "foster and promote a clear aspiration and vision for the Internet of Things."

No matter the nation, fostering the right public and private partnerships is essential to success. As the United States has the most vibrant technology market-place in the world, it also has the greatest potential to take advantage of ongoing work in and around IoT in the commercial sector and apply it to federal government missions. That means forging alliances on privacy and data transmission standards, for example, between national labs, commercial technology innovators, telecommunications firms and the aerospace and defense sector. ***In an upcoming white paper, Avascent will explore specific cases demonstrating IoT's transformational impact on government services and operations.***

III. U.S. Federal IoT Challenges: Technology and People

With all the promise for IoT comes bigger questions about the tradeoffs associated with different technical standards and adoption or implementation strategies. From a cyber perspective, billions of devices add up to billions of potential vulnerabilities. The emerging bring-your-own-device approach to agency-level IT will become increasingly untenable with the explosion of data-consuming devices utilized daily by federal workers. Just the prospect of lost productivity when benchmarked against private-sector measures should be enough to spur action toward developing realistic approaches to strategically leverage IoT capabilities to address specific missions and goals.

To understand the potential obstacles on the path to effective government IoT adoption, consider how senior IT leaders and stakeholders might overcome the following:

1) Dynamic and Expanding Threat Surfaces: User-introduced and unmanaged solutions will literally "walk" on- and off-premise on a daily/hourly basis

- Unequal privacy controls create personal information asymmetry between government users and networks vs. private-sector and citizen users
- Network entry points proliferate, which can lead to data theft or manipulation by adversaries or inadvertent usage

2) Talent Acquisition and Development: The future federal workforce expects access to new technologies and the flexibility to use them on site and at home

- Military and intelligence community employees need proficiency with emerging network-access and machine-interface technologies devices such as haptic-feedback/input wearables
- A distributed and remote workforce features individuals with their own individual network of devices that must be able to sort and manage two-track access to work and personal networks

3) Lack of Common Standards: Incompatible data degrades federal efficiency while harming external compatibility necessary to Big Data management

- Federal agencies lose value of acquisition "scale," leaving "morsels vs. meals" for programs of record lacking a holistic approach
- Strategy choices must be made about when common standards are not yet available, such as employing aggregated technology approaches that may have higher latency while offering a viable work-around

IV. Understanding the IoT Opportunity

To maximize the opportunity represented by IoT adoption, industry must be a true partner for its government customers, offering more than simple "dashboarding." This value will come from companies anticipating the next wave of federal mission needs that reflect the technological aspirations of 2016 and beyond. It will also come from introspection. Contractors, as well, will be caught between past and future in establishing internal IoT strategies.

IoT Fundamentals for Federal Contractors:

- *Identify selective opportunities to utilize IoT technologies to support near-term federal mission requirements*
- *Explore leap-ahead sensor and Big Data capabilities derived from interconnected technologies not utilized in the federal market*
- *Support federal technology governance and implementation stakeholders in developing strategies for long-term adoption and IoT integration*
- *Develop internal ROI models and data management policies for IoT services and solutions*

V. Conclusion

Within the public sector, IoT represents the biggest digital challenge of the next decade – impacted federal spending alone could be more than $57 billion in 2025. Success hinges on near-term, collaborative engagement to explore near-term solutions and long-term strategies. As part of this process, all stakeholders need to challenge the conventional, "technology-first," definitions of IoT. Doing so will aid contractors and mission partners alike in visualizing the new solutions and opportunities associated with a connected world vs. the risk of adoption. Every second, new digital connections are being formed between once-unconnected devices. While this connectivity is technological, a successful future for federal IoT starts by understanding the digital phenomenon that is much more than the sum of its parts.

Endnotes

1 http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html

2 http://www.gartner.com/it-glossary/internet-of-things/

3 http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

4 http://www.ibm.com/blogs/think/2015/12/15/cognitive-iot-making-the-internet-of-things-deliver-for-all-of-us/

5 Customer Defs:
- **Defense/Intel**: Includes DoD, National Intelligence Program (NIP), and Military Intelligence Program (MIP) agencies
- **Public Safety**: Includes DHS
- **Civilian**: Includes all non-DHS civilian agencies

6 Application Defs:
- **Enterprise/Infrastructure**: Spending on the IT enterprise and federal physical infrastructure impacted by IoT capabilities
- **Citizen Services**: Includes applications focused on health care delivery and management, tax administration, financial services (e.g., payments and accounting), logistics management, and data storage/analysis
- **C4ISR**: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities include sensor development, sensor connectivity, data processing and dissemination, and C4ISR R&D
- **Cyber**: Includes cyber security spending that could be impacted by the need to protect IoT networks

About the Authors

Jason Layman is a Principal at Avascent and a leader in the firm's ICT and High Tech Services advisory practice. He consults on a wide range of issues, from expanding core market positions, evaluating and penetrating adjacencies and managing a healthy growth portfolio. Jason has expertise and experience in the areas of government / commercial technology transition, IR&D and BD investment alignment, portfolio management for providers of integrated Enterprise & Mission IT and Services solutions. He has driven strategic and tactical business development activities for major primes, including buy-side and sell-side acquisition support, and provides subject matter expertise to teams at market-leading technology primes considering adjacent and new market expansion. He holds an M.A. from Georgetown University and a B.A., from Davidson College, and is an active member of AFCEA International and PSC. For more information, contact: jlayman@avascent.com.

Jake Silverman is an Associate at Avascent, where he supports defense and aerospace clients through project management. In his 50+ projects with the firm, Jake has worked across the federal markets, with particular interest in projects related to space, satellite communications, information technology, and international defense markets. His functional experience includes new market entry strategy, capture support, competitive intelligence, international expansion strategy, and M&A due diligence. Jake graduated Phi Beta Kappa from the University of Pennsylvania with a B.A. in political science and minor in Modern Middle Eastern studies. For more information, contact: jsilverman@avascent.com.

About Avascent

Avascent is the leading strategy and management consulting firm serving clients operating in government-driven markets. Working with corporate leaders and financial investors, Avascent delivers sophisticated, fact-based solutions in the areas of strategic growth, value capture, and mergers and acquisition support. With deep sector expertise, analytically rigorous consulting methodologies, and a uniquely flexible service model, Avascent provides clients with the insights and advice they need to succeed in dynamic customer environments.

AVASCENT

US Office
1615 L Street NW, Suite 1200
Washington, DC 20036
Tel: +1 (202) 452 6990

Paris Office
59, rue des Petits Champs
75001 Paris
Tel: +33 (0)1 73 77 56 19

London Office
Portland House, Bressenden Place
London SW1E 5RS
Tel: +44 (0) 20 8282 6357

www.avascent.com