The Challenge of the Internet of Things

Posted At : November 11, 2014 7:16 AM | Posted By : Alex Rossino
Related Categories: Department of Defense, Technology Trends, Federal, Big Data/Analytics, Internet of Things, Emerging Technologies

You may have noticed recently that the media has grown weary of touting cloud computing and big data as the next big things. Those are yesterday's stories in the short attention span of reporters and technology prognosticators. Today's subject caught in the hype cycle is the so-called Internet of Things (IoT). The IoT hype envisions a world in which everything that can be attached to a network is. Choose any "thing," from a household appliance to your heartbeat, and if a sensor can be installed it will be connected to the internet for more efficient monitoring and use. Smart lights will turn on when you come home, a health care provider will contact you when the devices monitoring your vital signs set off an alert, etc. The world will be one of ubiquitous contact, communication, and computing.

Despite how the future is envisioned, the world of federal information technology is likely to remain in the land of yesterday's technology for far longer than any other sector of the U.S. economy. One need look only at agency struggles with cloud to conclude that the government Internet of Things will evolve slowly and painfully. What is more, even with the IoT advancing at a glacial pace it will likely overwhelm the ability of agency IT shops to handle the influx of data. Out of necessity the keys to enabling the IoT in federal IT will be automation and semantic networks. The number of devices and sensors and data will simply be too great for human beings to track and manage. Instead software will be needed to manage the data generated by IoT devices. Sitting at the heart of the IoT is a big data challenge and agencies haven't responded well to that challenge yet have they?

Consider the following. September brought revelations from the Council of the Inspectors General on Integrity and Efficiency about irregularities in the management of cloud contracts at multiple federal agencies. Among the various inspector general findings was a lack of understanding at the agencies when a cloud-based service had even been used. We're not talking about a large number of contracts and services here either. The number is small. Even so, The IGs found that poor management of these contracts and, by extension, the data that agencies have shared with cloud vendors, raised risk considerably. At issue here is a small data challenge. Take that challenge and multiply its difficulty many times to approach the complexity of the Internet of Things and this is the extent of the test agencies are facing.

Concerning the Internet of Things itself, agencies are to a certain extent already struggling with it. The proliferation of mobile devices has dramatically increased the size of agency networks and the surface vulnerable to cyber-attacks. Similarly, the increased number of end-point devices is placing bandwidth demands on networks that require technology upgrades to handle. This evolution is one of the reasons, for example, that the Department of Defense is working on the concept of the Internet Protocol-based Joint Information Environment. Imagine the burden that adding millions of sensors will place on agency networks. Imagine the vulnerabilities!

The coming Internet of Things is today the Internet of "some" Things. Solving the challenges of today around bandwidth, security, data management, governance, storage, and analytics will establish the framework for solving the challenges of tomorrow as the IoT evolves organically into the tsunami of data and devices that it is forecast to be. Within this context agencies will need vendors more than ever to help them manage. Those who can offer smart, scalable solutions that promise management benefits and integrated analytics with dashboards will probably find their products in demand. The outsourcing of agency data to cloud providers with self-healing networks should also prove lucrative in the years to come as the cost of implementing these kinds of networks in-house could be prohibitive to a federal government with skyrocketing debt service payments and social safety net obligations.