New JIE Requirements May Help the “Internet of Things” at the DoD

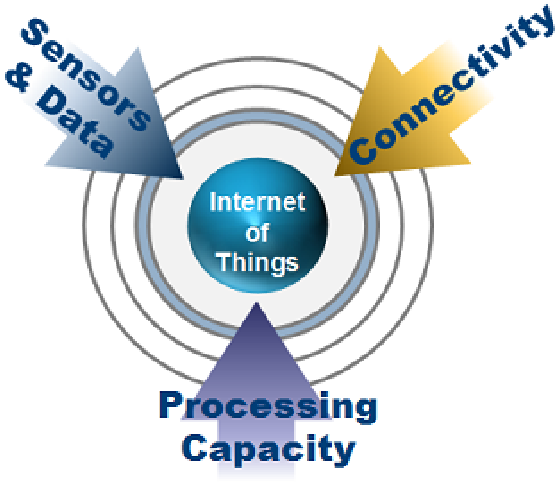
Posted At : January 22, 2015 2:59 PM | Posted By : John Slye

Related Categories: Department of Defense, Joint Information Environment (JIE), Innovation, DISA, Information Security, Air Force, Big Data/Analytics, Army, Internet of Things, Emerging Technologies, Navy, National Defense Authorization Act

The “Internet of Things” (IoT) is a pretty common phrase these days, with the rapid-expanding interconnectivity of devices and sensors sending information across communications networks, all to achieve greater capabilities, effectiveness, efficiency, and flexibility. The Department of Defense (DoD) clearly links the growth of emerging, interconnected technologies to the sustained superiority of U.S. defense capabilities, on and off the battlefield, so you could say that the IoT impacts defense IT at all levels.

The key to leveraging the IoT is in harnessing and integrating three key areas:

- Information – Data from devices and sensors, (e.g. phone, camera, appliance, vehicle, GPS, etc.) and information from applications and systems, (e.g. social media, eCommerce, industrial systems, etc.) provide the content input.
- Connectivity – Network connections via various wireless capabilities and communications backbones provide the transport links for aggregation and distribution. This facilitates the environment where data meets the power to use that data.
- Processing – The computational capacity and capabilities to make the data content useful. This may reside at the device and/or back end and ranges in complexity, (e.g. data analytics, etc.)



DoD Implications

The use of integrated networks to connect data with processing capacity to affect outcomes is far from a new idea at the DoD – it gave us much of the warfighting capabilities we have today. But technological evolution has resulted in a growing IoT mentality that goes beyond combat operations. One example is the establishment of the Air Force Installation Service Management Command (AFISMC) to coordinate management and maintenance of resources across Air Force bases and facilities. According to Air Force CTO Frank Konieczny, potential uses of IoT include facilities and vehicle management, logistics and transportation, integrated security, and robotics.

But pervasive connectivity is also creating security ramifications. In the wake of a network security incident last year, the Navy launched Task Force Cyber Awakening (TFCA) in an effort to protect hardware and software Navy-wide as IoT engulfs everything from weapons systems to shipboard PA systems.

Importance of the JIE

The drive to leverage sensor technologies and data analytics that these technologies enable is a driving force behind the DoD’s Joint Information Environment (JIE) network modernization efforts, so the pace of sensor-based innovation is tied to the success of JIE efforts. Adding potentially tens of thousands of diverse Internet-connected objects to a network that then need to be managed and secured will require proactive IT governance policies to ensure effectiveness, and some provisions in recent law apply.

The FY 2015 National Defense Authorization Act (NDAA), passed just last month, requires the DoD CIO to develop processes and metrics within the next six months for measuring the operational effectiveness and efficiency of the JIE. Further, Congress is having the CIO identify a baseline architecture for the JIE and any information technology programs or other investments that support that architecture.

These requirements may stem, in part, from a desire to help formalize and oversee JIE as an investment program, but the resulting baseline architecture will help pave the way to further implement greater IoT capabilities. The data from sensor-based devices will only continue to grow, but to maximize its utility the DoD will need a successful JIE to connect and carry the information.

---
*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*