IoT: a strategic approach to logistics

A focus on innovation to meet the mission
Connected Logistics Modernize Agency Operations

The complex and varied work of federal agencies creates logistics challenges that can limit agencies’ efficiency and effectiveness. The sheer scope of Federal government logistics is staggering. The Department of Defense (DoD) alone conducts a dollar volume of business more than double that of Walmart, the world’s largest company, and operating the DoD supply chains cost nearly $98 billion a year.1

Managing equipment and supplies at such a scale requires disciplined logistics management. However, a Reuters investigation concluded that the Pentagon faces significant challenges in keeping track of its vast stores of weapons, ammunition, and other supplies. As a result, it continues to spend money on duplicate supplies it doesn’t need and on storing others long out of date.2 Two years later, the Government Accountability Office (GAO) found serious weaknesses in the management of the DoD’s supply chain, particularly in inventory management, materiel distribution, and asset visibility.3

Pentagon logistics managers themselves acknowledge the problem. Many believe the DoD’s logistics challenges have a serious impact on the readiness of U.S. forces. In a Government Business Council survey of defense managers, 86% of respondents say defense logistics challenges have at least some impact on U.S. readiness, and 25% say the impact is severe. The survey also found that Defense logistics offices face mounting risk in managing supply chains and that Defense agencies lack the ability to derive actionable insights from supply chain data.4

It’s not just the DoD that struggles with logistics management; the Federal Emergency Management Agency (FEMA) and other agencies have faced similar challenges in managing emergency response. For example, following Hurricane Katrina, one of the deadliest storms in U.S. history, FEMA was hampered by the magnitude of the event, the loss of power, collapse of the telecommunications infrastructure, and the lack of integration between federal and state systems.5

Storing and moving perishable supplies also present problems. When the assets include food or emergency response supplies such as blood and medications, agencies must ensure that environmental conditions remain within prescribed limits. Failure to adequately monitor the condition of assets can lead to loss and spoilage, which in turn hamper agency effectiveness and create the additional expense of replacing items. In combat and emergency response scenarios, where every minute counts, efforts can be severely hindered when agencies lack visibility into the location and quality of potentially lifesaving equipment and supplies. Even when it’s not an emergency, agencies managing inventories of billions of items can find it difficult to keep track of high-value assets.

The good news is that innovative logistics solutions are available to change the way agencies function. The Internet of Things (IoT), which is already revolutionizing business and industry, can help transform the federal government’s ability to track and manage a variety of goods to which they previously had little to no visibility regarding utilization, location, and condition. IoT logistics solutions give organizations the power to locate things quickly and globally, and share the information with others to support mission-critical operations.

Visibility, Productivity, Efficiency

An estimated 50 billion “things” – ranging from sensors in cars and traffic lights to utility meters and household appliances – will be sharing data over the Internet by 2020.6 Most people are already taking advantage of IoT. In 2016, the average American has 3.64 connected devices,7 a number expected to grow substantially as households add connected TVs, vehicles, and appliances.

While government organizations are often cautious adopters, the promise of operational improvements has led growing numbers to begin making use of IoT solutions, and industry analyst Gartner, Inc. predicts that by 2020 government will be the nation’s third largest IoT user.8 Smart solutions, which involve the use of sensors to facilitate data-based decision-making, can help agencies increase the visibility of assets and take command of their supply chain and operations to mitigate risk, proactively improve quality control, and better fulfill their missions.

IoT has the potential to streamline operations, cut process time, and significantly reduce expenses. At the Department of Defense alone, experts estimate that tracking and remote monitoring of equipment within the next decade could lead to a 3 to 5% productivity gain, potentially generating an economic benefit of $15.6 billion to $27 billion per year.9

Improving Processes

Forward-thinking agencies are modernizing their operations and taking advantage of the same type of IoT technology that has created positive outcomes for global businesses like Maersk, the world’s largest container ship and supply vessel operator. The shipping giant formerly had to manually check the condition of every shipment of perishable goods, an unwieldy and expensive process. Maersk equipped 280,000 of its refrigerated containers with a remote container device with a 3G High Temperature SIM card for cellular connectivity, a GPS unit, a ZigBee radio and antenna, and multiple interfaces that connected to the container’s controller. Now it can track and monitor the condition of shipments at almost any part of their journey along the supply chain in near-real time to ensure ideal conditions.
Companies are also using IoT to manage fleet vehicles and other valuable equipment. As global emergency response specialist B&P Enterprises grew, it required a more efficient way to track its 600 vehicles and specialized construction equipment. When a railroad or any other customer called for assistance after an accident, B&P had to depend on its dispatchers knowing where the necessary equipment was located. The company saw immediate results and a swift return on its investment after it introduced a comprehensive asset tracking and fleet management solution. Response time was improved since dispatchers could see the location of all the company’s equipment. Another advantage was gaining the ability to track the location, speed, and mechanical condition of all its vehicles, which led to annual insurance savings of $86,000 and an 80% reduction in Department of Transportation violations.

In addition to creating efficiencies and reducing costs, IoT can help agencies save lives. Consider the impact that smart solutions could have in a Humanitarian Assistance Disaster Response (HADR) scenario. During a military campaign or after a natural disaster, troops and other responders have to be able to identify and locate critical pieces of cargo at each stage in an operation. Knowing the exact location of each asset—at the container, pallet, or individual item level—optimizes receipt, staging, onward movement, and integration (RSOI), so citizens can get the help they need more quickly.

By maximizing asset visibility for location and condition, whether the asset is in storage or in transit, agencies can now prevent delays in responding to events that require critical assets like human organs, blood, medication, and other medical supplies to fulfill a mission. IoT-enabled solutions monitor perishable cargo for temperature, humidity, and other environmental factors.

Smart cargo solutions and asset tracking can give emergency service personnel real-time updates on shipment arrival times. Additionally, such solutions can be used even in remote areas and regions left without power after a disaster, thanks to cellular, satellite-based, and custom mesh communications platforms.

**Condition-based Maintenance Maximizes Resources**

Some agencies have been using connected sensors, which are at the heart of IoT technology, for decades. The U.S. Geological Survey (USGS), the Army Corps of Engineers, and the National Oceanic and Atmospheric Administration (NOAA), for example, collect data from sensors to support coastal storm damage reduction, water supply, the environment, and emergency management efforts. Some of the technology, however, is decades-old, and produces minimal data. Today’s IoT technology enables agencies to integrate existing sensors and collect more sophisticated data from new sensors that are designed to interact easily with other technology, from even the most remote locations, worldwide.

A number of other federal agencies have begun using connected devices that increase productivity and efficiency by optimizing asset tracking and management in the field, giving them immediate visibility into the location and condition of important property. Agencies can achieve cost reductions by avoiding searching for assets or repurchasing items they can’t locate. Experts estimate that using data to predict and prevent breakdowns of vehicles and other equipment could reduce downtime by 50 percent.

Following are a few ways innovative agencies are using IoT solutions to cut expenses, increase security, and comply with federal mandates:

- Real-time data supports condition-based maintenance, enabling agencies like the Federal Bureau of Prisons to prioritize and optimize resources. The bureau’s fleet tracking system helps keep its assets in working condition and bolsters security by monitoring location, direction, speed, and other variables.
- The U.S. Census Bureau transmits critical survey work performed by 20,000 census takers in the field with an intelligent IoT management platform that securely captures and delivers census statistics on-the-go. As a result, the agency has increased census workers’ flexibility and significantly decreased mobile data charges.
- The General Services Administration (GSA) has installed GPS tracking to improve the performance of government fleet operations, enhance driver safety, cut costs, and enable compliance with Executive Order 13693 to measure, report, and decrease greenhouse gas emissions. The solution could save as much as $11 billion over the next decade.
- The U.S. Postal Service streamlined operations and enhanced consumer satisfaction with a wireless location-based tracking solution that generates automatic text alerts and enables consumers to text a tracking number to check a package’s location at any point in its journey.

**IoT Solution Considerations**

To gain real value from IoT solutions requires effective communication among all elements of the architecture. With an integrated, end-to-end platform (see figure 1) it is possible to deploy applications faster, process and analyze data at lightning speeds, and act on events as they occur.

As shown in figure 1, everything from actual hardware to backend systems and databases needs to be designed to work together as one, and the architecture must be flexible so agencies can build on the IoT platforms. The following steps are important when designing and developing IoT solutions:

- Create a network and service delivery platform that links devices and/or sensors over a wireless network. A global
1. Endpoint layer: Ranging from low-powered, low-bandwidth devices (without operating systems (OS)) to rich, OS-enabled devices, endpoint security solutions help authenticate and account for IoT endpoints connected to the enterprise network, and protect the data/usability of the devices themselves.

2. Connectivity layer: This helps secure data in transit from the endpoint to backend application/infrastructure for highly secure transmission of information over wireless and wireline connectivity types to keep enterprise data private and isolated, and away from the open Internet throughout the IoT ecosystem.

3. Data/application layer: Wherever the IoT application sits (public cloud, private cloud, on premises and/or in a data center), security solutions are deployed to provide specific policies and controls to protect stored data and data traffic, as well as the applications themselves.

4. Threat Management layer: Involves the collection and examination of data across all layers (endpoint, network, and data/application), in order to identify, isolate, and manage threats via a threat management platform. This platform unifies the various data streams of traffic traversing the different networks, which includes data collected from security functions, third-party and customer security information, and event management (SIEM) and government signatures. Using a centralized and comprehensive data “lake”, combined with a Big Data architecture, helps to maximize visibility into the threat landscape, and thereby supports optimal threat detection and response.

**Making the Right Connections**

Federal agencies require sophisticated, cloud-based platforms to launch, manage, and rapidly scale for a connected-device deployment. Decision-makers need to look at the agency’s current systems to determine how IoT solutions could work and whether system upgrades are required. With each IT expenditure, consider how IoT solutions could improve operations to support the agency mission. While IoT may be able to enhance or connect to installed systems, it may not always make sense to build on top of antiquated or legacy infrastructure. Agencies should invest in systems to reduce operations and maintenance (O&M) expenses over the long term, recognizing the value of new assets and the potential return on investment.

Getting the most from IoT requires a network with breadth, depth, reach, and reliability. Look for a network provider whose security approach meets the requirements described above, provides connectivity in each medium required (Cellular, Wi-Fi, Satellite, Ethernet, etc.), and be sure the provider understands existing Program of Record (POR) systems, e.g., Global Combat Support System and Global Command and Control System, and that its data and analysis platforms will integrate with them.

Choose a top-tier provider with the services and platforms that cover the entire technology value chain, which would include cloud-based, fully managed time-series data storage service for network-connected machine-to-machine (M2M) devices and other IoT solutions. Unless agencies have a robust and mature IT organization, including IoT technical support, they will need a provider that also offers consulting to help decide which devices and objects need to be

---

*Figure 1. Integrated end-to-end IoT platform.*

SIM Management platform will provide a single view into the network connections to help agencies monitor, understand, and control the wireless network.

- Certify devices on service provider’s network for compatibility the moment the devices are activated. Additionally, hardware configurations from third-party manufacturers should be optimized for the service provider’s network, so the right device is matched to the agency needs (based on usage, and accounting for performance characteristics and factors like form, size, antenna requirements and battery life, cost, and expected lifecycle).
- Provide preconfigured and customizable software applications that agencies can implement quickly and cost-effectively. Developing IoT applications is challenging. The majority of developers (53.7%) found the process of developing IoT applications somewhat challenging, while another 9% indicated the process has been very challenging. IoT platforms and services must accommodate all development approaches (e.g., Java®, Python®, Adobe® Air®, Silverlight®, C and C++), support robust software development kits, and third-party application development platform access, and have a broad catalogue of APIs.
- Cloud-based data storage should offer a fully managed time-series data storage service for network-connected devices and provide easy-to-use tools and analytics.
- Secure potential points of compromise with a layered approach to security that delivers protection at the device, network, data and application layers, and provides information loss prevention, intrusion detection, machine controls, and enterprise mobile management. This includes:
  1. **Endpoint layer**: Ranging from low-powered, low-bandwidth devices (without operating systems (OS)) to rich, OS-enabled devices, endpoint security solutions help authenticate and account for IoT endpoints connected to the enterprise network, and protect the data/usability of the devices themselves.
  2. **Connectivity layer**: This helps secure data in transit from the endpoint to backend application/infrastructure for highly secure transmission of information over wireless and wireline connectivity types to keep enterprise data private and isolated, and away from the open Internet throughout the IoT ecosystem.
connected and how to get the best analytical information from them. Look for a one-stop solution for network provisioning, device activation, customer support, billing options, performance audits, IT integration services and more.

**The Right Information Can Change the World**

Just as personal computers, cell phones, the Internet, and digital media redefined the way people and companies connect with one another, IoT may change the world in ways no one has yet dreamed. Many believe that IoT will facilitate a new era of innovation, with the potential to transform industry, government, and the way many people and enterprises live, work, and govern.\(^\text{15}\)

Today’s decisions on IoT deployments have the power to shape an agency’s effectiveness for years to come. Following the path outlined in this paper provides an opportunity to significantly augment the value of an agency’s assets, improve productivity and efficiency, and enable compliance with federal mandates such as energy sustainability. Taking advantage of the promise of IoT could also advance the agency’s public image and standing among other government programs. IoT solutions provide agencies the opportunity to fulfill their missions better and more cost-effectively, in ways never before thought possible.

---

**About Global Business – Public Sector Solutions**

Global Business – Public Sector Solutions, a business unit of AT&T Corp., blends unmatched network resources and IT professional services expertise with innovation from AT&T Labs and industry-leading technology providers to deliver IT solutions spanning cyber security, networking, mobility, mission support and applications.

AT&T

Global Business – Public Sector Solutions

1900 Gallows Road

Vienna, VA 22182

att.com/gov

---

**Works Cited**

14. IDC. The Developer’s IoT Playbook: What to Expect and Where to Turn to Fast-Track Your IoT Initiatives, 2015