Federal Cybersecurity Market Forecast –Sustained Growth Continues

Posted At : November 20, 2014 3:00 PM | Posted By : John Slye

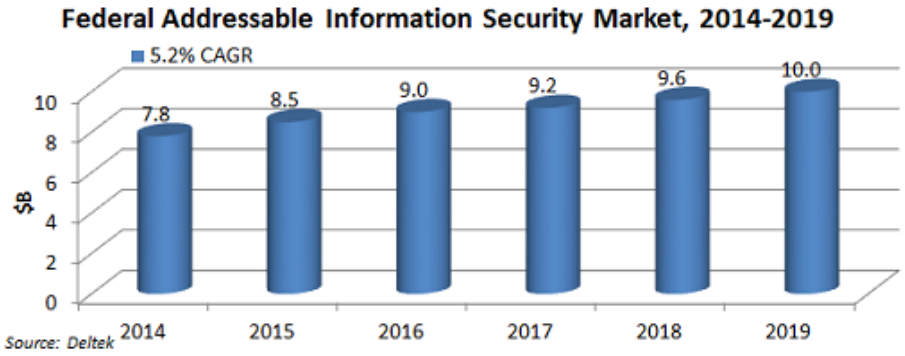
Related Categories: Critical Infrastructure Protection, Department of Defense, Department of Homeland Security, Technology Trends, Information Security, IT Workforce, Forecasts & Spending, Cybersecurity

The federal cybersecurity market continues to grow and we have just completed analysis that shows how much. Increasing threats, the rapid pace of technological change, and an increasing reliance on mobility, cloud computing, big data, and information sharing make information security critical for federal agencies. To address these challenges, agencies continue to invest in industry tools, technologies and personnel services and this will drive growth in the market segment over the next several years.

Taking a comprehensive perspective on the federal cybersecurity market, we see four major driving areas that continue to create demand for government-wide and agency budget investments:

- **Threat Drivers** - Rapid rise in complex, diverse, persistent and morphing threats to networks, devices, data and other infrastructure.
- **Policy Drivers** - Executive branch policies address wide areas of cyber- across government and beyond. Stagnant legislation reflects diversity of opinion. Compliance policy bolsters spending on existing frameworks. RFP language both driving and requiring security.
- **People Drivers** - Challenge to find enough qualified cybersecurity professionals. Initiatives to cultivate internal government talent and "inherently governmental" roles will limit contractor addressability, but agencies that supplement by contracting will drive spending.
- **Technology Drivers** - Threats and vulnerabilities drive direct technical remedies while new, disruptive technologies require security for full adoption.

Given these drivers, Deltek forecasts the demand for vendor-furnished information security products and services by the U.S. federal government will increase from $7.8 billion in FY 2014 to $10.0 billion in 2019 at a compound annual growth rate (CAGR) of 5.2%. (See chart below.)



Key Findings

There are several conclusions that we came to when reflecting on what we are observing across the federal information security environment and how the drivers above are impacting the market both now and going forward. Here are some of our key findings:

- The continued rise in cyber incidents underscores what is at stake.
  - Threats span all areas of cyber – from within and from without.
  - Threat concerns impact all levels of the federal IT environment.
  - Persistent and diverse threats are driving risk-based approaches.
- Policies and priorities are slow to evolve into effective security approaches.
  - The drive for security permeates multiple layers of federal policy, but there is a disconnect between compliance policies like FISMA and actual security, as revealed by the volume and type of security incidents.
  - Security considerations impact the broader tech and acquisition landscape.
- Security efforts and posture are currently dependent on the availability and proficiency of skilled personnel.
  - Staffing levels and skill sets vary across government, driving sustained demand for industry support.
- Technologies are seen as both security "gap-filler" and "gap-creator."
  - One year into CDM tools BPA only marginal improvements have been seen.
- Strong processes are needed to link technologies, approaches and personnel skill sets to maximize security posture.

Efforts among agencies to increase effectiveness, efficiency and economy like the joint DHS-GSA Continuous Diagnostics and Monitoring (CDM) program BPA are having some impact on how agencies are approaching cybersecurity and setting their spending priorities within their security budgets. Although the process of arriving at accurate and complete IT asset inventories that need to be secured and monitored is taking time, somewhat elongating the journey, we remain bullish that the priority of securing and protecting federal data and infrastructure will continue to drive significant market opportunity over the next five years.

Get more of our perspective in our latest report: ***Federal Information Security Market, FY 2014-2019***.

---

*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**.*