The Soter Group

Perspectives – Unclassified 2014 Federal Cyber Security Spending Update

Reported fiscal year (FY) 2014 unclassified Federal cyber security spending is up 23% to $12.7 billion. Federal Civilian spending increases for second consecutive year – adds 16% over FY13 levels.

The rollercoaster ride of unclassified Federal cyber security spending continued in FY14 as reported spending grew to $12.7 billion – an increase of 23% from $10.3 billion in FY13. However, this total remains below FY11 and FY12 levels of $13.3 and $14.6 billion, respectively. While these all indicate that there is a large Federal market for cyber security activities, these significant and rapid shifts in reported spending may leave the contractor community with more questions rather than answers.

	FY09	FY10	FY11	FY12	FY13	FY14	FY14 v. FY13, % Δ
Total Unclassified Federal Cyber Security Spending	$6.8	$12.0	$13.3	$14.6	$10.3	$12.7	*+23%*
Of Which: DoD	*$4.2*	*$9.5*	*$10.1*	*$12.1*	*$7.1*	*$9.0*	*+26%*
Of Which: Federal Civilian	*$2.6*	*$2.6*	*$3.2*	*$2.6*	*$3.2*	*$3.8*	*+16%*

(in $ billions)

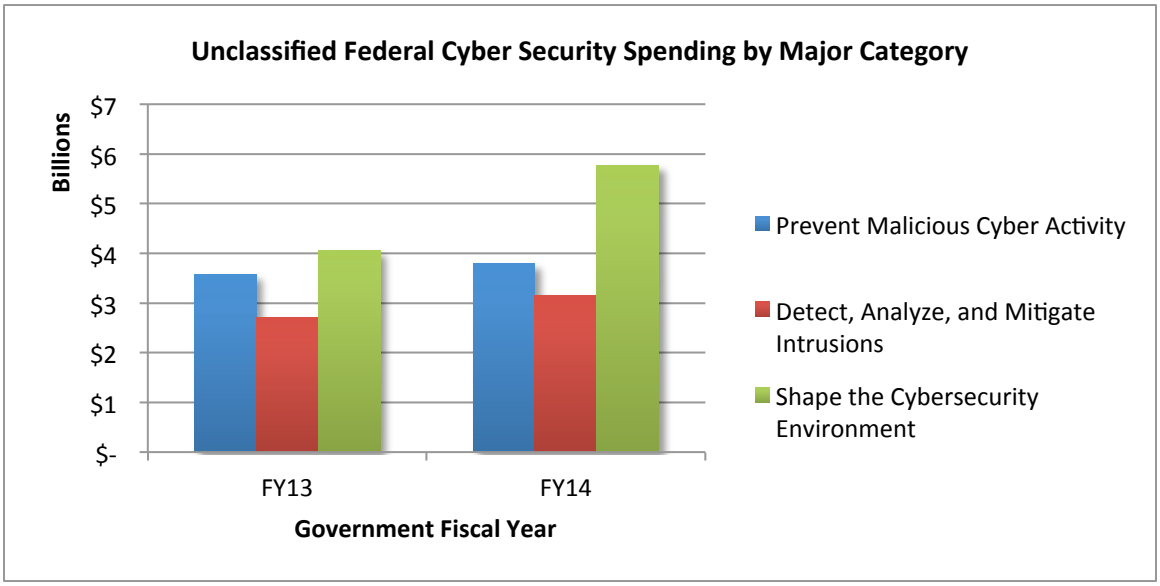
What does this growth in spending really mean? What portion of this extra $2+ billion in FY14 spending flowed to contractors? Or was it primarily used to pay government employees' salaries and benefits? Did it have a negligible effect on the contractor-addressable market? What should the private sector expect in the current (FY15) and coming fiscal years (FY16) given the President's budget requests of $13 and $14 billion, respectively?

The Office of Management and Budget (OMB) changed the cyber security taxonomy in FY14 and created three primary categories: (1) Prevent Malicious Cyber Activity; (2) Detect, Analyze, and Mitigate Intrusions; and (3) Shape the Cybersecurity Environment. While this prohibits an apples-to-apples comparison with pre-FY14 spending reports, this segmentation could provide some insight into the drivers behind volatile spending levels.

Between FY13 and FY14, activities related to the Shape the Cybersecurity Environment category received an increase in funding of over $1.7 billion – or 42% growth, year-over-year. This category includes activities such as workforce development, security training, standards development, and research and development (R&D). While Federal cyber security and information assurance-related R&D was estimated to have increased nearly 11% between FY13 and FY14 – or approximately $70 million, this accounts for only a small portion of the $1.7 billion jump.

The large shift in reported spending is partially due to workforce development and training activities but primarily attributable to reclassification of personnel into cyber security-oriented positions. Spending on personnel – both government and contractor – has historically been the largest category of Federal cyber security spending; for example, in FY12, cyber security personnel expenditures totaled $13.2

billion, or approximately 90% of the $14.6 billion total. Any large changes in spending are undoubtedly associated with this area of spending.



Does this mean the Federal cyber security market is stagnant or unreliable given the annual exercise of reallocating personnel expenditures and massive swings in cyber security "spending?" No. Cyber security is certainly not a fad. The threat is very real and will persist, and the Federal government is and will continue to have capability gaps and deficiencies to satisfy. The "arbitrary" labeling of spending as cyber security, IT, health IT, or cloud computing does not really matter; it is the real substance of the product, service, or solution that is being delivered to achieve a mission that matters.

As a Federal contractor, there are several key questions to focus on: Does government spending on cyber security products and services and future government needs and requirements align with your core capabilities? If so, do you know which government customers have both the money and the need? And lastly, do you have a means to deliver, deploy, and implement that product, service, or solution?

About The Soter Group

The Soter Group provides services to both the Federal government and the commercial entities that support it. Our Commercial Services Division provides market research and assessments, competitive assessments, and strategic advisory services to commercial clients seeking to enter or grow in the Federal government security market. Justin Taft, President & CEO, and Peter Wong, Director of Market Research, authored these perspectives. The Soter Group welcomes the opportunity for our research to be cited in third-party reports. To learn more, please visit www.TheSoterGroup.com and/or email info@TheSoterGroup.com. To access and read our other reports, please visit: The Soter Group Market Reports.

Report March 2015: Perspectives – Unclassified 2014 Federal Cyber Security Spending