

The Soter Group

Perspectives – Unclassified Federal Government Cyber Security Spending

Reported fiscal year (FY) 2015 unclassified Federal government cyber security spending is up 3% year-over-year to \$13.1 billion. The President's Budget Request for FY17 includes \$19 billion in funding for cyber security activities.

Unclassified Federal government cyber security spending showed modest growth in FY15 – increasing 3% to \$13.1 billion versus the previous full fiscal year. FY15 also marked the first fiscal year that Federal civilian cyber security spending eclipsed \$4 billion. While cyber security spending has oscillated around roughly \$12 and \$13 billion over the last several years, the FY17 budget request indicates the Federal cyber security market may be reaching a new inflection point – perhaps akin to the inflection point between FY09 and FY10 precipitated by the Comprehensive National Cybersecurity Initiative (CNCI). The \$19 billion budget request to support cyber security activities marks a significant departure from the spending pattern of the post-CNCI era.

	FY09	FY10	FY11	FY12	FY13	FY14	FY15	FY16 (Enacted)	FY17 (Request)	FY15 v. FY14, % Δ
Total Unclassified Federal Cyber Security Spending	\$6.8	\$12.0	\$13.3	\$14.6	\$10.3	\$12.7	\$13.1	\$14.1	\$19.0	+3%
<i>Of Which: Dept. of Defense (DoD)</i>	\$4.2	\$9.5	\$10.1	\$12.1	\$7.1	\$9.0	\$9.1	TBD	TBD	+2%
<i>Of Which: Federal Civilian</i>	\$2.6	\$2.6	\$3.2	\$2.6	\$3.2	\$3.8	\$4.0	TBD	TBD	+7%

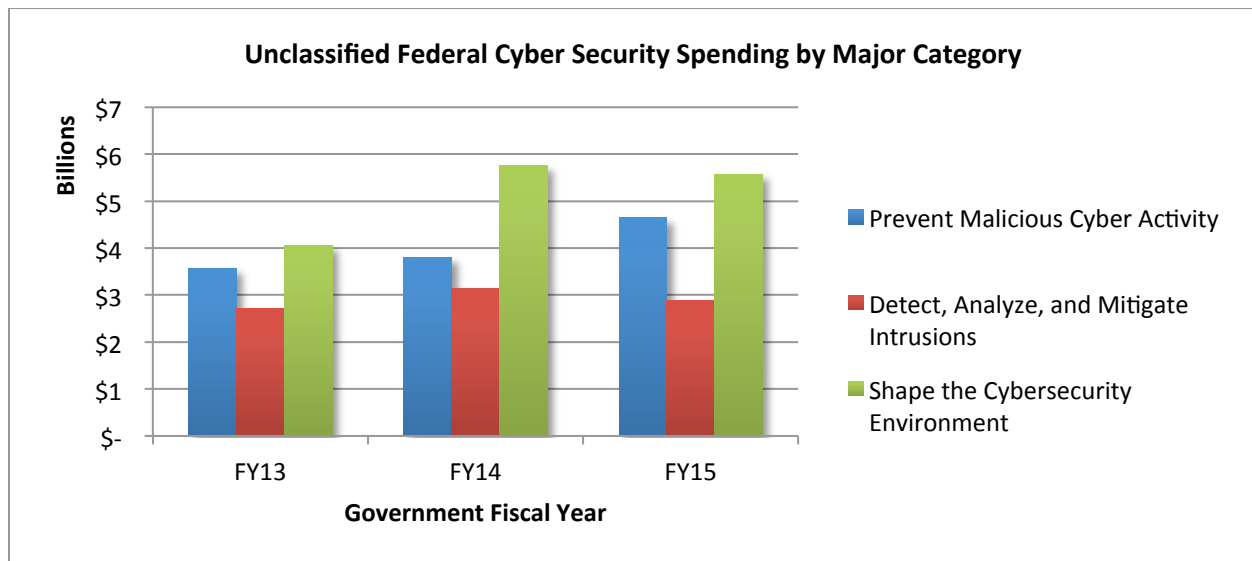
(in \$ billions)

The jump in anticipated cyber security spending may sound promising to both cyber security product vendors and service providers as well as traditionally cash-strapped government program managers, but there remains a significant amount of uncertainty. How much of the \$5 billion increase over current year levels is net new money? How much of the increase is a result of reorganization and reprogramming of funds – similar to what occurred nearly a decade ago? Part of this increase in funding stems from a proposed \$3.1 billion IT modernization fund – which is still in flux due to political differences. Additionally, assuming it is included in the appropriations, the proportion of these IT modernization funds that would apply to cyber security versus non-cyber security activities would depend on the legacy IT systems and programs that are prioritized for modernization.

Whether the large increase in funding is realized or not, there are other important trends that are indicative of Federal government cyber security priorities and initiatives. For the past several years, the Office of Management and Budget (OMB) has been using three primary categories for characterizing cyber security spending: (1) Prevent Malicious Cyber Activity; (2) Detect, Analyze, and Mitigate Intrusions; and (3) Shape the Cybersecurity Environment.

The Soter Group

FY15 showed continued investment in Shape the Cybersecurity Environment, which has a large focus on workforce development and training as well as cyber security research and development. This category accounted for 43% of total spending, or approximately \$5.6 billion. The primary area of growth, however, was Prevent Malicious Cyber Activity, which increased 22% year-over-year to \$4.6 billion this past fiscal year. This growth aligns with several major, on-going government cyber security initiatives, such as large network sensor programs and the Continuous Diagnostics and Mitigation (CDM) program.



It continues to be a dynamic period for the Federal cyber security market, from all angles – budget, policy, technology, and threat environment included. Much of this can be attributed to increased understanding of the threat and the cyber security problem across government stakeholders; increased commitment, including budgetary commitment, from the White House, Congress, and department leadership to address these cyber security concerns; and increased establishment and formalization of cyber security programs and organizations – and associated support contracts. The impending transition to the next administration is already at the top of everyone’s minds, and only time will tell whether this cyber security momentum and renewed sense of urgency persists.

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 June 2016: Perspectives – Unclassified Federal Government Cyber Security Spending