OMB Reports $10.3 Billion on Cybersecurity in FY 2013

Posted At : May 19, 2014 12:37 PM | Posted By : John Slye

Related Categories: Department of Justice, Department of Agriculture, Department of Homeland Security, Homeland Security, Office of Management and Budget, Health and Human Services, National Aeronautics and Space Administration, Air Force, Veterans Affairs, Treasury, Navy, Department of State, Department of Defense, Technology Trends, Information Security, Forecasts & Spending, Army, Department of Energy, Transportation, Cybersecurity, Department of Commerce, Department of Transportation

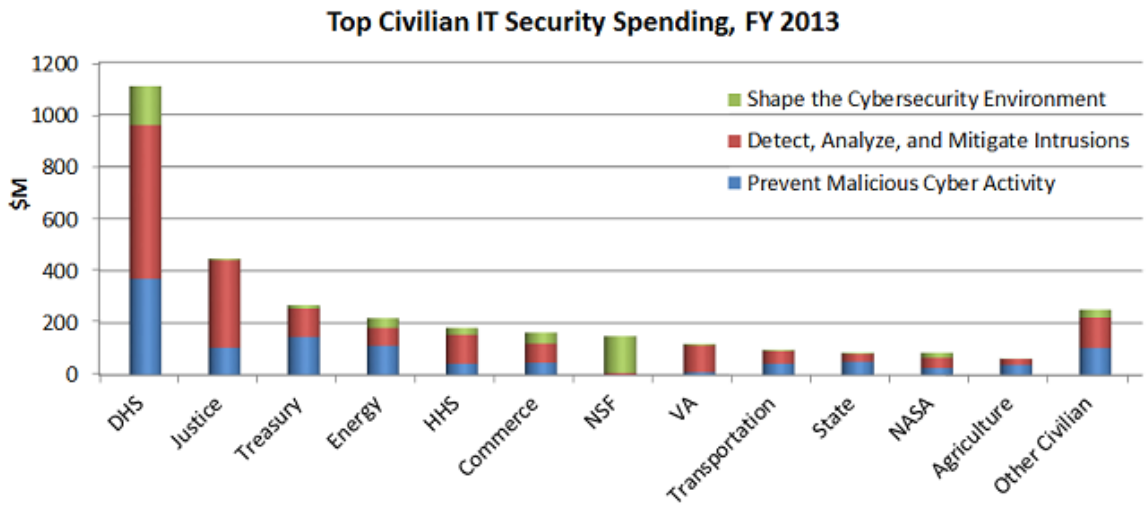
While no area of federal IT spending is "off the table" when it comes to scrutiny for efficiency, economy and return on investment, agency spending on information security continues to be an area for focused spending. The latest report out of the Office of Management and Budget (OMB) on Federal Information Security Management Act (FISMA) efforts shows that agencies spent $10.3 billion in FY 2013.

The latest **FY 2013 FISMA report** to Congress provides OMB's FY 2013 assessment on what agencies have achieved in FISMA-related information security in the previous fiscal year. Last week, I looked at the number of **reported federal cybersecurity incidents** and noticed that they were up 25% in FY 2013 across a broad range of categories from policy violations to malware. This week, I'll look at the spending data reported by OMB within the FISMA report.

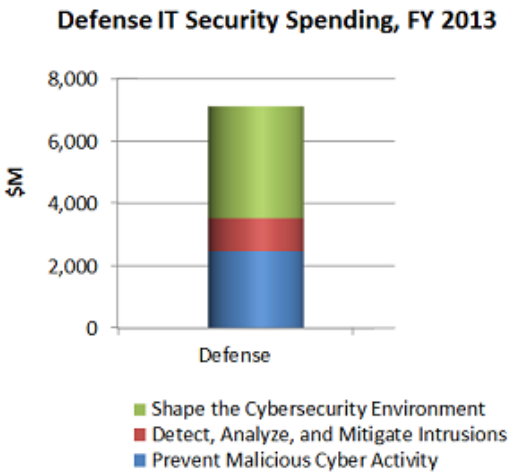
OMB requires executive branch agencies to report information security spending data on an annual basis. For FY 2013, agencies reported spending information in the following three areas:

- **Prevent Malicious Cyber Activity** – monitoring government systems and networks and protecting the data within from both external and internal threats. Such categories include trusted internet connection (TICs); intrusion prevention systems; user identity management and authentication; supply chain monitoring; network and data protection; counterintelligence; and insider threat mitigation activities.
- **Detect, Analyze, and Mitigate Intrusions** – systems and processes used to detect security incidents, analyze the threat, and attempt to mitigate possible vulnerabilities. These categories include Computer Emergency Readiness Teams (CERTs); federal incident response centers; cyber threat analysis; law enforcement; cyber continuity of operations (COOP); incident response and remediation; forensics and damage assessment; continuous monitoring and IT security tools; and annual FISMA testing.
- **Shaping the Cybersecurity Environment** – improve the efficacy of current and future information security efforts, including building a strong information security workforce and supporting broader IT security efforts. These categories include the National Strategy for Trusted Identities in Cyberspace (NSTIC); workforce development; employee security training; Standards development and propagation; international cooperation activities; and information security and assurance research and development.

The federal cybersecurity spend in the classified areas of the civilian and defense segments are not reported, but OMB provided the reported spending for the executive departments and agencies by the three categories above. I have put the data into a chart for ease of comparison, but separated out DoD with its reported $17.1 billion in spending due to scale.



Together, the **civilian departments and agencies account for just over 31% of the total federal spend** last fiscal year and the top twelve civilian organizations account for 29%. DHS's reported $1.1 billion in spending accounts for just 11% of the overall $10.3 billion in spending, but **DHS represents nearly 35% of the overall civilian agency spending** in FY 2013. DHS spent 33% of its dollars in the Prevent Malicious Cyber Activity category, an aspect that it shares only with Treasury and Energy among the largest departments.



The $17.1 billing in **Defense Department spending accounts for nearly 70% of the total reported $10.3 billion** in cybersecurity spending in FY 2013. Half of the DoD spend is in the area of shaping the environment, which sets it apart from the ratios of most civilian agencies with the exception of the National Science Foundation (NSF) above. Another contrast is that the DoD spent just 15% of its FY 2013 dollars in the Detect, Analyze, and Mitigate category where many civilian agencies often spend the most.

Each year the information that OMB includes and highlights in the FISMA report varies, sometimes widely. The inclusion of spending data by the above three categories is different from the cost categories included in previous FISMA reports (e.g. personnel costs, etc., which OMB did *not* include this year.)

---
*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@GovWinSIye**.*