MARCH 20, 2017

OMB Claims Federal Progress on FISMA in 2016 But Much Work Remains

by Christian F. Henel

Earlier this week, the White House Office of Management and Budget ("OMB") issued its 2016 Federal Information Security Modernization Act ("FISMA") Annual Report. FISMA (last amended 2014) charges OMB with tracking the extent to which federal agencies are complying with FISMA's core objective to secure the availability, confidentiality, and integrity of federal information.

This year's FISMA Report had a number of key takeaways. First, OMB found that federal agencies continue to be the target of sophisticated and destructive cyber-attacks. According to the Report, over 30,899 cyber incidents in 2016 led to the compromise of information or system functionality within federal information systems. Of those, sixteen met the threshold for a "major incident," which OMB defines as "a designation that triggers mandatory steps for agencies including reporting certain information to Congress." The agencies sustaining major incidents were the U.S. Patent and Trademark Office, Departments of Health and Human Services, Housing and Urban Development, Treasury, and the Federal Deposit Insurance Corporation. Almost all involved the compromise of Personal Identifiable Information ("PII") or Federal Taxpayer Information ("FTI").

Second, the Report disclosed that many agencies made progress in developing their information security defense capabilities, with several exceeding their 2015 participation levels in the areas of Information Security Continuous Monitoring ("ISCM"), Identity, Credential and Access Management ("ICAM"), and Anti-Phishing and Malware Defense – by far the most significant increase of the three categories. In addition, OMB found that the vast majority of federal agencies developed and implemented policies and training around privacy requirements and accountability.

Third, the government's overall progress in developing information security capabilities remains somewhat immature. The phrase "immature" is not our term – OMB commissioned a council of agency Inspectors General ("IG") to assign the federal government one of five levels of "maturity" for each of five cybersecurity framework function areas (identify, protect, detect, respond and recover). The IGs issued a government-wide score of 2 out of 5:

aaa

The Report also includes individualized reports for each federal agency.

Finally, the Report touched on information security spending by fiscal agencies. DHS topped the list at nearly $1.3 Billion and the median spend was just over $81 million. Our read of the numbers suggest that contractors can expect to see the highest priority emphasis on cybersecurity and cybersecurity compliance within DoD, NASA, DHS, HHS, DOT, DOS and the VA. To close with a word of caution – regardless of how much (or how little) an agency appears to have committed to cybersecurity, contractors can expect agencies accountable to the President and Congress to hold contractors strictly responsible for information and data lost "on their watch."