KILPATRICK TOWNSEND

May 17, 2017

“No Ransom, No Cry” – Trump’s Latest Executive Order on Cybersecurity and Preventing the Next “WannaCry” Virus

On Thursday, May 11, 2017, President Trump signed a new Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The new Order came out just one day before last week’s “WannaCry” ransomware attack wreaked coordinated havoc across information systems – and in particular, government systems – in over 100 countries.

Although the new Order has no direct relationship with WannaCry, its clear intent is to bolster the U.S.’s cyber defense capabilities to protect federal networks and data from future cyber attacks.

The Order covers several topical areas from broad cybersecurity priorities (including a section on critical infrastructure that builds upon President Obama’s E.O. 13636) to specific strategies and procedures. But two takeaways matter most for government contractors.

First, the Government’s overall cybersecurity strategy is about to undergo a top-down review. Observing that the executive branch “has for too long accepted antiquated and difficult-to-defend IT,” the Order requires that each agency head employ NIST’s Framework for Improving Critical Infrastructure Cybersecurity and provide a risk management report within 90 days of the date of the Order (a) documenting the agencies current risk mitigation and acceptance choices (and the reasoning behind those choices) and (b) the agency’s plan to implement the OMB framework going forward. The Order tasks OMB and the Secretary of Homeland Security with evaluating the agency reports and advising the executive branch on cybersecurity risks and strategy within 60 days of receiving the reports. The Order also charges the executive branch with developing defense and response strategies to multiple types of common vulnerabilities and attack scenarios, such as automated distributed attacks (like WannaCry) and attacks that threaten widespread power outages and other crucial infrastructure failures.

Second, the Order may drastically change the architecture of Government networks and Government priorities in acquiring IT services. Seeking to “build and maintain a modern, secure, and more resilient executive branch IT architecture,” the Order requires Agency heads to “show preference” for “shared IT services,” such as shared cloud-based solutions. The Order tasks OMB, the Secretary of Homeland Security, and the Administrator of GSA, in consultation with the Department of Commerce in preparing a report on the feasibility of adopting more consolidated network architectures and shared (e.g., cloud-based) services. This part of the Order calling for uniformity and shared IT solutions departs significantly from the current IT landscape, where an individual agency determines its needs for cloud and shared IT services. An agency seeking cloud-based solutions could procure

those services from contractors and subcontractors certified through GSA's FedRamp program. Alternatively, agencies could avoid the cloud and build within their or the contractor's existing local networks. Moving all (or most) agency IT services to the cloud would likely result in (a) significant regulatory changes as agencies update their information security clauses; and (b) a significant market shift to cloud service providers as Agencies increase cloud-based IT acquisitions. Given the highly sensitive nature of some Government data, we would also expect increased demand for higher-baseline FedRamp capabilities (e.g. FedRamp Moderate and FedRamp High).

Although these changes may signify new opportunities for federal contractors, we recommend treading carefully – changes as significant as moving most federal IT infrastructure to the cloud *en masse* could have unintended consequences from both a cost and risk standpoint. We will continue to monitor new developments and update this post as we learn more.