United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

April 7, 2016

The Honorable Shaun Donovan
Director
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Director Donovan: Shaun

As you well know, federal agencies are under a constant yet evolving threat from cyber attackers. From what I understand, however, flaws in the federal acquisition process can limit the tools agency network defenders can obtain. I write today to better understand what the Office of Management and Budget is doing to address this issue, as well as to ascertain what can be done to make it easier for federal agencies to take advantage of the most effective cyber defense tools available.

My staff and I recently met with a number of small businesses to discuss innovation in cybersecurity. Our discussions made it clear that, because the techniques our adversaries use against us online are always evolving, deploying innovative products and services is critical to staying ahead of the threats we face online. The small businesses we met with advised us that financial institutions, power companies, retailers, and other private critical infrastructure owners are able to quickly reap the benefits of the many new and innovative cyber defense products put on the market each year. Yet it was not clear to them that federal agencies are similarly able to rapidly acquire new and innovative cybersecurity solutions.

Several federal initiatives could potentially help in this matter. First, as part of the Federal Acquisition Streamlining Act of 1994, Congress granted agencies the ability to use simplified procedures for small purchases of supplies and services. It can currently be used for purchases totaling $150,000 or less. The simplified process allows for purchases of items like desktops and routers, but it is currently unclear how agencies use this authority to get advanced cyber defense tools into the hands of their network defenders.

Second, Congress has afforded agencies the authority to limit competition, and thereby speed up the acquisition process, when there is an urgent need or when the open, public nature of the traditional procurement process would compromise national security. Specifically, the Competition in Contracting Act of 1984 (implemented through the Federal Acquisition Regulation, Subpart 6.3) identifies exceptions to the competitive federal acquisition process, including for both urgent need and matters of national security. It is my understanding, however, that many agencies do not take advantage of these provisions to acquire advanced cyber tools.

Third, the General Services Administration (GSA) manages a supply schedule for information technology equipment, software, and certain services called Schedule 70, in which GSA does much of the vetting of vendors to save agencies time. This schedule is easier to navigate than the traditional process, gives companies selling their products better access to more agencies, and reduces paperwork. One challenge for startups seeking to use Schedule 70, however, is that companies are required to demonstrate two years' worth of past performance. The new "Startup Springboard," announced this week by

Administrator Roth[1] will likely address this concern, but agencies need detailed guidance to leverage this change and we need to measure its impact.

Fourth, the Continuous Diagnostics and Mitigation (CDM) program at the Department of Homeland Security allows agencies to partner with DHS to deploy cybersecurity tools and services while saving taxpayer dollars by leveraging government-wide buying power and buying in bulk. CDM is starting to deliver tools and services to agencies, but because of the complexity of the contracting process, it may not be able to offer new tools fast enough to keep up with the threat.

Finally, Congress has granted many agencies what is known as "other transaction authority," which allows agencies to enter into agreements that are not subject to traditional contracting laws and regulations. This authority can help agencies fulfill their missions by attracting companies that have not previously done business with the government and which might find traditional contracting rules prohibitively complex or onerous. For example, the Department of Homeland Security recently used it to work with a cybersecurity start-up in California.[2] But the Government Accountability Office recently found that agencies are not making frequent use of "other transaction authority" for several reasons, including agency implementation rules that may be too burdensome.[3]

To better understand what OMB is doing to shepherd the use of innovative and emerging cybersecurity tools at Federal agencies, I am writing to ask you answer the following questions within 30 calendar days.

1. What are agencies doing to acquire innovative cyber solutions developed by start-ups and other companies that have not traditionally done business with the government? How successful have agencies been in doing so? Are any agencies piloting innovative procurement processes for rapid acquisition of cybersecurity tools?

2. What action has OMB taken, or is planning to take, to guide agencies in the rapid procurement of new and emerging cybersecurity tools?

    a. In particular, what will OMB do to promote the appropriate use of the five acquisition tools listed above to acquire cybersecurity products and services?

    b. How will each of these efforts need to be updated or addressed to better accommodate the quick purchase of such tools?

    c. Are there any other avenues agencies can use to access new commercial cyber tools in a rapid manner?

    d. Has OMB assessed the challenges start-ups face in doing business with the government? If so, what will OMB do to address these challenges?

---

[1] Denise Turner Roth, "*GSA Making it Easier for Suppliers to Do Business with the Government,*" GSA Blog, April 6, 2016.
[2] Mohana Ravindranath, "*DHS Silicon Valley Office Awards First Contract to Internet of Things Startup,*" NextGov, Feb. 23, 2016.
[3] "*GAO-16-209, Federal Acquisitions: Use of 'Other Transaction' Agreements Limited and Mostly for Research and Development Activities,*" Government Accountability Office, Jan. 7, 2016.

e. How is OMB ensuring that contracting officers at agencies are knowledgeable and comfortable with the use of the five acquisition tools discussed above, as well as any other ways of rapidly acquiring cyber tools, in an appropriate way?

f. What is OMB doing to ensure that best practices in this area of acquisition are being shared between defense, intelligence, and civilian agencies?

3. When and how should Part 6.3 of the Federal Acquisition Regulation be applied in the acquisition of cybersecurity products?

4. Venture capital firms play an important role in bringing new and innovative cybersecurity tools to market. To what extent should venture capital firms be encouraged to pursue channels like Schedule 70 contracts from GSA to enable the firms to offer products and services of the companies they represent? How would the Schedule 70 program need to change to better accommodate the start-up nature of venture capital firms and the companies they support?

5. How can new and emerging products and services be considered and integrated into the CDM program?

6. The Chief Information Officers Council and the Chief Acquisition Officers Council are the primary bodies of the federal government where agencies collaborate and share best practices on information technology management and procurement activities. How will OMB work with these bodies to find solutions that facilitate the rapid acquisition of cybersecurity solutions?

7. Many agencies, including the research and development arms of the Department of Defense and the Department of Homeland Security, play important roles in fostering cybersecurity innovation and bringing new tools into government. What are OMB and other agencies doing to promote research and development efforts related to the acquisition of new cybersecurity tools and services to industry and the federal government? How are agency cyber research and development efforts of coordinated?

Thank you for your attention to this important issue. I appreciate your continued leadership on acquisition issues and on getting the most value out of our taxpayers' dollars. I look forward to your response.

With best personal regards, I am

Sincerely yours,

Thank you, Shaun! Tom

Thomas R. Carper
Ranking Member

CC: Secretary of Homeland Security, Jeh Johnson; Administrator of the U.S. General Services Administration, Denise Turner Roth.