Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity Vendors Must Be Careful With New GSA Option

Law360, New York (September 2, 2016, 12:24 PM ET) --

Alexander Major

Machiavelli — yes, that Machiavelli — knew a thing or two about working with a powerful government. In his most well-known writings, Machiavelli opined on both the application of power and importance of intellect when addressing that power. To be sure, in his 1521 treatise "The Art of War," the tactician warns forces facing a government to be wary if all is not as it seems:

If the [government] puts some booty before you, you ought to believe that within it there is a hook and that it conceals some trick … you should never believe that the [government] does not know how to carry on his affairs."

Against this ominous paraphrase, let's take a look at the cyber battlefield. On Aug. 17, 2016, the General Services Administration revealed what may well qualify as one of Machiavelli's booty-encrusted hooks — a solicitation for four new special item numbers (SINs) intended to give federal agencies a new way to buy cybersecurity services called, collectively, Highly Adaptive Cybersecurity Services, or HACS. (I can only assume the acronym is intentional.) Although intended to have been included in the GSA's Multiple Award Schedule 70 (IT Schedule 70) solicitation by Sept. 1, these services are expected to be included in the upcoming refresh and include:

- Penetration Testing under SIN 132-45A
- Incident Response under SIN 132-45B
- Cyber Hunt under SIN 132-45C
- Risk and Vulnerability Assessment under SIN 132-45D

The GSA anticipates the inclusion of these new SINs will improve the way government customers can acquire cybersecurity services through IT Schedule 70, while allowing industry the opportunity to differentiate their cybersecurity services from other IT-related services. Moreover, the new SINs will be subject to "cooperative purchasing" — meaning that state, local and tribal governments can also order these services.

While all of this sounds like an amazing opportunity for cybersecurity vendors, they should, as explained below, proceed with caution.

The Biggest Issues: Indemnification, Control and Standards

The primary concern vendors should have in responding to this solicitation is whether the government

truly understands what it is buying. While the government needs the services these SINs are supposed to provide, the government has to understand that cyber services alone do not beget security. Vendors all recognize that "pen testing," threat monitoring ("cyber hunt"), and risk and vulnerability assessments (SINs 132-45A, 132-45C and 132-45D) are waypoints on the road to security, but they are not the final destination. And while the GSA and the purchasing agency information technology staff or contracting officer may understand that, vendors must recognize that in a year, when something has gone awry leading to a cyber incident or breach, the GSA Office of Inspector General and the U.S. Department of Justice may not share that understanding. The enforcers will look at the paper trail and to the promises expressly stated or inferred by the vendor during negotiations. So what should a cautious company do?

- Make sure that indemnification provisions are clearly stated throughout negotiations with the government, from its initial offer to the final draft of the best and final offer letter. If the GSA suggests that such a clause is "not needed" or "generally understood," thank them for that assurance ... and leave it in.

- In order to "command and control" an incident, as required under SIN 132-45B, incident response vendors should ensure that they are granted the appropriate level of authority needed to properly respond to any sort of response a cyber incident may bring, including the lateral mobility necessary to chase down new systems not originally in scope should the evidence so direct.

- Further, incident response vendors will need to prepare for varying response requirements directed by the agencies. Due diligence is required to ensure that the vendor (1) understands and (2) is capable of meeting the processes demanded by the GSA, the U.S. Department of Labor, the U.S. Department of Education, the state of Florida, the territory of Puerto Rico, etc.

Identifying and negotiating clear lines of authority and communication are vital in setting expectations and avoiding contractual conflicts before, during or after any sort of cyber incident. The fog and confusion of a breach is no time to try to work out or modify contractual terms or understandings.

Then There's the Oral Technical Evaluations

A key element of the SINs' inclusion in the new IT 70 solicitation will be a new evaluation factor: an oral technical evaluation. That's right — vendors will need to pass an oral examination before contract award. Here's how that process will work:

- The GSA will invite prospective vendors to an interview (in person or virtually) with purportedly tech-savvy GSA evaluators.

- Each vendor will be given a series of questions and a scenario, uniform by SIN, and will have 40 minutes to respond to each SIN-related round of questions/scenarios.
    - Vendors presently offering penetration testing, incident response, cyber hunt, and risk and vulnerability assessment under existing SINs will need to transfer to these new SINs and will also be subject to this oral evaluation factor.

- The vendor's answers will be judged by the panel, leading to an overall pass/fail score.

- A vendor that fails the oral evaluation will have only one opportunity to provide clarifications to its interview within "24 hours from the time of the notice of possibly not meeting the passing criteria of the fail rating from the [technical evaluation board]."
    - The draft solicitation is unclear as to exactly how those 24-hour vendor clarifications are to be given.

- No recording devices will be permitted in the oral evaluation. The only official record of the oral evaluation will be the notes taken by evaluators on the vendor's responses and, as the GSA assured in an Aug. 24 Q&A addressing the new SINs, will become a part of the vendor's contract file and incorporated into the GSA pre-negotiation memorandum.

If not readily apparent on its face, vendors considering offering penetration testing, incident response, cyber hunt, and risk and vulnerability assessment through IT 70 need to approach the oral evaluation factor with caution:

- Take nothing for granted. The GSA does not intend to limit the number of vendors offering these services, but vendors who fail to pass the oral evaluation may have a difficult time protesting their exclusion.

- Vendors should take notes — not only of the questions and responses, but also regarding the attitude and demeanor of the evaluators.

- In these oral technical evaluations, ensure that no off-the-cuff promises or guarantees are made. None. Anything said (or inferred/construed/suggested) could be used as the basis for a future False Claims Act violation brought against the unwary vendor if a purchasing government agency is affected by a "zero day" exploit. (A zero day exploit is a cyberattack that occurs on the same day a weakness is discovered in software and before a fix becomes available from its creator.)

While cybersecurity vendors fully understand the dynamic and asymmetric nature of the cyberthreat, they should not for a moment believe that the government thinks likewise. If the government paid a vendor to do something one way, and something went sideways, it will be the vendor's back that will be up against the wall.

Not Subject to Mandatory Transactional Data Reporting Rule

Importantly, these new SINs will not be subject to the new transactional data reporting (TDR) rule. For the uninitiated, the TDR rule requires GSA schedule holders to submit 11 transactional data elements to the GSA on a monthly basis in exchange for the GSA's elimination of the often confusing commercial sales practice (CSP) disclosures and the challenging price reduction clause (PRC) basis of award tracking customer requirement. While the TDR rule is applicable to some of the IT-70 SINs (132-8, 132-32, 132-33, 132-34, 132-54 and 132-55), the HACS SINs are not included. However, if a vendor chooses to include the new HACS SINs alongside TDR rule SINs, then the TDR rule will apply to all SINs being offered. For a basic overview of the TDR rule, take a look at the explanation provided by the Coalition for Government Procurement here.

Accordingly, vendors offering HACS independently will be subject to the requirements of the CSP and the controls established by the PRC. Experienced vendors in venerable industries know that these GSA contractual requirements can serve as the gateway to trap-laden litigation, and yet many still fall victim.

Cybersecurity is an extremely "young" and dynamic industry; cyber vendors wanting to avoid a False Claims Act violation need to spend time carefully evaluating the following:

- the disclosure of commercial sales practices and special discounting;
- identification of the appropriate "basis of award customer(s)" and
- how often each may change in the usual course of business.

The opportunities provided to cybersecurity vendors under the new HACS SINs cannot be understated. A GSA Schedule can be a fine vehicle for any company wishing to place services in easy reach of hundreds of scared and eager federal purchasers. But cybersecurity is a unique beast that may not be wholly understood by its purchasers. It is up to vendors to explain the strengths and limitations of their products and to educate their customers as to what they can realistically expect. Do so clearly, with caution and with wisdom. This is a new world and, as Machiavelli noted centuries ago: "There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things."

—By Alexander Major, McCarter & English LLP

Alexander Major is a partner in McCarter & English's Washington, D.C., office and co-leader of the firm's government contracts and export controls practice group.