IT for Goverment

Four tips for security contracting

By Eddie Franklin

Government entities have a tremendous appetite for IT and the budget to back it up. Before jumping into a government contract, here are four things to consider:

1. **Government contracts have an extended DSO cycle:** On average, DSO on Government A/R is more than 45 days; but there are several ways to hedge against this, such as securing extended terms from suppliers and making payments for work in phases. Before bidding, do the math to ensure a government opportunity does not turn into financial hardship.

2. **Government entities are cost-conscious:** Government entities are focused on doing more with less. Federal and state government procurement staff have tight controls and high visibility of costs, but may not recognize added-value. Resellers need to keep bids competitive yet simple, carefully outlining any extra value and monetizing elements when possible. Always be respectful of government customers — they are spending taxpayer dollars, and the contractor's acknowledgement of this is very important.

3. **Have a clearly defined statement of work:** The rules of engagement must be crystal clear and both parties should measure progress and success the same way. Resellers should take time to ask detailed questions, which shows they are trying to avoid mistakes. It is also important to acknowledge when customer expectations supersede requirements outlined in the statement of work.

4. **Stay focused on the outcome:** Every project should have clearly defined goals; and it is the contractor's job to help the agency or department achieve them. Develop firm checkpoints to keep the project on track. When something goes wrong, communicate the problem quickly and professionally, documenting the details and clearly defining an action plan to overcome the obstacle. ▮

A 22-year channel veteran, Eddie Franklin leads SYNNEX Corp.'s public sector initiatives through GOVSolv and PROHEALTHSolv. SYNNEX is a distributor of IT products and services, servicing resellers and OEMs around the world. Request more info about the company at www.securityinfowatch.com/10215269.

Opportunities Abound

Understanding government security threats, solutions and the role of dealers and integrators

By Phrantceena Halres

Federal spending is rising, which means more opportunity for government contractors, and particularly with small business. Whether your goal is to contract directly with the government or carve out a specific role as a subcontractor in the homeland security and critical infrastructure sectors, as dealers and integrators, you have to make sure you know your own company inside and out, and understand exactly what it is you have to offer. It is also of vital importance to define your role — not just for the part you play in the project, but to always be cognizant of the overall protection of this nation.

Government projects are getting a boost through more and more economic development programs, while many private-sector plans remain status quo; thus, the playing field for finding new work has changed. As federally funded projects ramp up, security firms with little to no experience in public sector work are eyeing opportunities to get on the bandwagon.

Landing public contracts can be a challenge for the uninitiated; however, with a little homework and some smart decisions, they can get in and find it very valuable.

The size of U.S. government contracting is staggering — to the tune of more than a half-trillion dollars. Following the national trend toward outsourcing business functions, the White House continues to prod the government to outsource more work. The rising defense and DHS budgets also add to contracting opportunities. For decades, small security businesses and entrepreneurs were often shut out of these marketplaces because government favored larger contractors with longer track records. That has changed — new laws have allowed Congress to create broader opportunities for small companies, specifically security-related ones.

The government is also bundling security contracts, where government departments are consolidating several small contracts into larger ones. Bundled contracts are ideal for small security companies because these smaller firms can take advantage of larger government needs by sectoring out specialized requirements.

New Threats and Innovative Solutions

The threat environment we see today is drastically different from what existed just a year ago. And a year from now, I expect

to say the same thing. Those behind the threats are evolving; the motivation behind attacks is more difficult to anticipate and predict. So, it is not enough to have a security strategy in place today; it's about deploying a long-term security solution that has the scalability and flexibility to adapt to this ever-evolving threat environment.

As the world becomes increasingly connected, the opportunities for innovation are limitless. Cyber technology — especially virtualization and "Big Data" brought to life through cloud computing — has freed businesses to explore new opportunities that simply weren't possible a few years ago.

Simultaneously, the risk and complexities associated with these opportunities are vast. With so much business-critical data at stake, the need to protect those assets is more important than ever. The motivations of web-based security threats vary significantly. Foreign governments, political protesters and known and emerging hacking groups are among the sources of daily government attacks executed on a global scale.

With the evolving cast of adversaries, many companies are straddling two security concepts — IT security innovation and physical security at the same time. Building a security solution that protects both traditional infrastructure and cloud-based infrastructure can be difficult, but it is the ultimate answer, and security firms that embrace this paradigm will succeed. This involves, for example, enabling governments and companies to maintain a secure origin onsite without risking compromise of origin servers.

As the security industry looks for the best way to embrace this new type of national security, it befits us to consider actions that will provide sustainable results. Regional workforce and entrepreneurial development is an ideal result because it is a long-term plan to remedy the situation, both economically and politically.

Best Practices for Your Firm

The security industry should be training on a non-stop basis for the "unknown or attack." Every scenario should be evaluated and audited on a continuous cycle from internal and external stakeholders. Nothing should be taken for granted, and constant watch should ensure complacency doesn't become an issue.

Along with training and evaluation, the security industry needs to set rigorous standards for recruiting, especially when considering the role of securing infrastructures and the nation. This standard should far exceed the minimum standards set for normal security requirements. Additionally, we need to raise security workforce performance standards through experience-based training and continuous education, as well as streamline workforce recruitment, convergence and retention measures by working closely with the security professionals responsible for hiring these officers.

Employ a higher pay-scale to attract higher caliber personnel, and promote a robust safety culture through safety-conscious work environment initiatives, human performance improvements and heightened threat awareness training such as "Sixth Sense Protection" where facilitators teach trainees the ability to anticipate threats around them. High security standards for business operations comes from the industry and the regulators working together to implement solutions.

Building a security solution that protects both traditional infrastructure and cloud-based infrastructure can be difficult, but it is the ultimate answer, and security firms that embrace this paradigm will succeed.

Each of us has to take responsibility for what happens in our community and nation at large, and not just ask "what can I do better" — but take tactical action. As a dealer or integrator in the security industry, it is up to you to lead the charge. Use this opportunity raise awareness about safety and security measures at the individual level, and then practice and integrate these principles into the security we as security professionals provide. ▮

Phrantceena Halres is founder, chairman and CEO of Total Protection Services Global, a certified security services company focused exclusively on high threat/close proximity safety and security services for the protection of critical infrastructure assets in the corporate, government, nuclear, energy and personal protection sectors. Contact her at www.total-protections.com.