Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Q&A With Crowell's David Bodenheimer

Law360, New York (March 15, 2013, 1:54 PM ET) -- David Z. Bodenheimer is a partner with Crowell & Moring LLP's government contracts group in Washington, D.C. He heads the firm's Homeland Security practice and focuses his practice on cybersecurity, False Claims Act, government pricing, protests and related litigation. He joined the firm in 1988 after six years with the U.S. Navy Department.

Q: What is the most challenging case you have worked on and what made it challenging?

A: The Great Engine War litigation readily tops the list of my most challenging cases over the past 30 years. In this case, the Air Force brought a $299 million defective pricing claim against Pratt & Whitney based upon over 30 audit reports spanning a decade. The 33-day trial featured over 50 witnesses covering virtually every aspect of competitive source selections, government pricing requirements and Truth in Negotiations Act nuances.

As one of my more memorable highlights of the litigation, I cross-examined the former secretary of the Air Force, Verne Orr, who displayed a remarkable memory and great pride in the Air Force's competitive savings resulting from the Fighter Engine Competition. After Pratt won the initial trial decision, we had to fight through an agency request for reconsideration and Federal Circuit appeal, ultimately prevailing after eight years of robust litigation. Wynne v. United Technologies Corp., 463 F.3d 1261 (Fed. Cir. 2006), affirming 05-1 BCA ¶ 32,860 and 04-1 BCA ¶ 32,556.

Q: What aspects of your practice area are in need of reform and why?

A: In one of the most regulated industries in the world, the federal government contracting business has yet to tame the chaotic and unruly frontier for federal cybersecurity regulations and request for proposal requirements. In 2005, a Federal Acquisition Circular (FAC) stated that federal contractors must generally adhere to the "same security standards as Government employees," but left the detailed implementation to individual federal agencies. FAC 2005-06 (Sept. 30, 2005). The result has been a virtual Tower of Babel as each federal agency has been driven to create its own cybersecurity regulations, rules and RFP requirements, thus confronting federal contractors with a kaleidoscope of different information security programs, internal rules, and practices for each agency's information technology needs. The current agency-by-agency approach to cybersecurity rules places a huge burden on both agencies (reinventing the wheel) and contractors (coping with multiple security regimes). Just as the time for more effective cybersecurity is now, so is the time for greater uniformity and consistency in cybersecurity acquisition regulations and rules governing the federal government sector and its contractors.

Q: What is an important issue or case relevant to your practice area and why?

A: Cybersecurity is hot everywhere now. But nowhere is cybersecurity hotter than in the federal public sector, given that the U.S. government is the world's largest user, consumer and manager of data in the world. And this data includes some of the most advanced military technology, sensitive intelligence data and coveted trade secrets anywhere. With the rise of homeland security, I have been immersed in public sector cybersecurity, advising large and small government contractors on cyber law and privacy, testifying before Congress on cyber issues, teaching the Cyber Contracting Workshop for Thomson West Federal Publications, and publishing briefing papers and other articles on federal information security, cloud cybersecurity and cyber war.

I am delighted that the American Bar Association has made cybersecurity a top priority this year. The ABA is producing high-profile programs, preparing practical handbooks and pursuing other critical initiatives through the multiple sections and task forces, including ABA Science and Technology Section's Security, Privacy, and Information Law Division and the ABA Public Contract Law Section's Cybersecurity, Privacy, and Data Protection Committee, for which I serve as chair. We look forward to making real progress on raising awareness and providing practical guidance on cybersecurity to lawyers in both the public and private sectors at this critical juncture.

Q: Outside your own firm, name an attorney in your field who has impressed you and explain why?

A: In the cybersecurity arena, Jake Olcott (cybersecurity principal, Good Harbor Security Risk Management) is one of the foremost young guns in shaping cyber policy and practices. While serving as the staff director for the House Homeland Security Subcommittee on Emerging Threats and Cybersecurity, Jake had a major hand in some of the most significant congressional hearings and oversight on cybersecurity, critical infrastructure, and security breaches in the public sector. Later as counsel for the Senate Commerce Committee, he continued to be a driving force on cybersecurity issues on the Hill. I will continue to rely on his valuable cyber expertise and big-picture thinking as we push forward on the cyber front.

Q: What is a mistake you made early in your career and what did you learn from it?

A: In the early stages of my career with the Navy and later in private practice, I made the mistake too often of failing to tap the incredible expertise of some of the giants in the field of government contracts. Some, like Norm Lussier (formerly with the Navy, now with Defense Logistic Agency) trained me despite myself. Others — like Harvey Wilcox (Navy), Peter Murphy (Marine Corps) and Roger Boyd (Crowell & Moring) to name far too few — had unparalleled grasps of public sector contracting that would have made me twice the lawyer I am today. If I could do it again, I would tap into that exceptional procurement expertise and experience that would make me, and everyone around them, a better lawyer.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.