In a world of smart devices and digitally delivered services, cybersecurity is critical for individuals, businesses, and government. At the federal level, it is also clickbait for cyber-fraud.

President Joe Biden's May Executive Order on Improving the Nation's Cybersecurity acknowledged the country faces significant cyber threats to national and economic security and asserted that the government would partner with the private sector to combat those threats. That was the starting gun for a run on government contracts to protect systems that process data (information technology, or IT) and that monitor or control industrial equipment, assets, processes, and events (operational technology).

Biden's executive order directed government contractors to report cybersecurity breaches to the Cybersecurity and Infrastructure Security Agency, and it set goals for modernizing the government's approach to cybersecurity, with investments in technology and personnel. The major sections of the order require specialized knowledge and skill sets only government contractors can offer.

The Government Accountability Office reports that federal agencies invest over $100 billion annually in IT and cybersecurity, and that's likely to increase as government contractors assist in the movement towards cloud-based services, multi-factor authentication, data encryption, and other cybersecurity enhancements.

Recent cyberattacks have had substantial consequences. In May, Eastern European criminals hacked the Colonial Pipeline, shutting down fuel deliveries to the East Coast for days. In October, Microsoft accused Russia-based Nobelium of targeting hundreds of cloud service resellers and other technology service providers in the U.S. And this month, Cybersecurity and Infrastructure Security Agency warned that Iranian government-sponsored hackers are actively targeting a "broad range of victims" across the transportation and health care sectors, deploying ransomware and other threats against those victims.

Experts warn these cyber incidents are the tip of the iceberg. The Government Accountability Office has designated information security as a government-wide high-risk area because of “increasing cyber-based threats and the persistent nature of security vulnerabilities.”

In October, the Department of Justice announced a new Civil Cyber-Fraud Initiative whose primary weapon is the False Claims Act, an effective enforcement tool for recovering misspent government contract funds and deterring future misconduct. The False Claims Act helps keep government contractors honest. Commenting on the initiative, the Acting Assistant Attorney General noted the False Claims Act “was enacted during the Civil War to address fraud involving contractors selling defective goods to the Union Army. Since the Act was revitalized by Congress in 1986, the department has recovered more than $65 billion on behalf of the American taxpayers” and “procurement fraud remains one of the main areas of False Claims Act enforcement.”

Significantly, the act’s qui tam, or whistleblower provision, allows individuals to report fraud, sue on behalf of the government, and obtain substantial cash rewards. The acting assistant attorney general named three common cybersecurity failures as prime candidates for whistleblower reporting — government contractors: knowingly failing to comply with cybersecurity standards; misrepresenting security controls and practices; and failing to timely report suspected breaches.

“Whistleblowers with inside information have been critical to identifying and pursuing new and evolving fraud schemes that might otherwise remain undetected,” the Department of Justice official said. “They also bring considerable technical expertise to complex investigations. As they have in many other aspects of False Claims Act enforcement, we expect whistleblowers to play a significant role in bringing to light knowing failures and misconduct in the cyber arena.”

The False Claims Act has been an effective enforcement tool. It was used during the Obama Administration to right the wrongs committed by financial institutions that led to the mortgage crisis. The act helped government-insured mortgage insurance programs recover billions of dollars of misspent funds and save the Insurance Fund from collapse. In the same way, the False Claims Act can be used to recover the likely billions of dollars that will be misspent through IT and cybersecurity contracts.

As federal agencies implement cybersecurity contract rules, contractors should heed the words of Supreme Court Justice Oliver Wendell Holmes: “Men must turn square corners when they deal with the government,” regardless of whether those corners are real or virtual.

Renée Brooker, a partner at the Washington law firm Tycko & Zavareei LLP, represents whistleblowers. She was an assistant director at the U.S. Department of Justice in the national office that supervises False Claims Act whistleblower cases in all 94 federal trial courts. She wrote this for InsideSources.com.

Written By
Renée Brooker
