Whistleblower News Review

September 19, 2016

# Defense Contractor Cybersecurity Breaches Bring Wave of Cyber Whistleblower Opportunities

**By ML McLaren**

Failure to report cyberattacks among Department of Defense (DOD) contractors and subcontractors means big whistleblower opportunities for IT professionals and other defense contractor employees. Cyber hacking and cybersecurity breaches are widespread, and a whole new category of cyber whistleblower claims are cropping up around them under the federal False Claims Act.

## CYBERCRIME COULD COST U.S. COMPANIES $2 TRILLION BY 2019

Cybercrime cost U.S. companies approximately $500 billion in 2015. This number could quadruple to $2 trillion by 2019. Cyber hacks into the computer networks of private vendors that supply aircraft, ammunition, radar technology and specialized software to all areas of our U.S. defense agencies present a significant danger to national security and

> "We worry that many vendors will not immediately report any cyber security problems, especially successful attacks," said leading U.S. whistleblower attorney Brian Mahany. "That directly affects our national security and could be a violation of the federal False Claims Act for those who have a government contract and don't follow cybersecurity regulations."

members of our armed forces. Because of this, federal rules and regulations on cybersecurity continue to tighten.

The Department of Defense (DOD) enacted a set of strict cybersecurity and breach reporting regulations in August of last year following a string of cyberattacks on American businesses and government contracting agencies. One IRS hack exposed the personal financial information over 700,000 U.S. taxpayers. In June of last year, hackers accessed the databases of the Office of Personnel Management, exposing SF-86 questionnaire data that military intelligence officers use to get top secret



Continued on next page

Continued from previous page

clearance. The breach disclosed names, addresses, social security numbers, financial data, and other personal information.

## FEDERAL RULES REQUIRE STRICT CYBERSECURITY MEASURES AND PROMPT REPORTING OF BREACHES

The Defense Federal Acquisition Regulation Supplement (DFRAS) cybersecurity rule, titled Safeguarding Covered Defense Information and Cyber Incident Reporting, requires that those participating in any kind of defense department contract (1) have security measures in place on all computer systems, and (2) report all incidents of cyber hacking or security breaches to the Department of Justice within 72 hours of discovery.

Specifically, regulations require that contractors and their subcontractors employ "adequate security" commensurate with consequences and probability of loss, misuse or unauthorized access to, or modification of, information. Contractors are obligated to report any cyber incident that affects the covered contractor's information system, covered defense information or the contractor's ability to provide operationally critical support within 72 hours of discovery.

The Department of Defense enacted the regulations last year because "of the urgent need to protect covered defense information, to understand the full scope of cyberattacks against defense contractors, and to reduce the vulnerability of cloud computing attacks."

"Recent high profile breaches of federal information show the need to ensure that information security protections are clearly, effectively and consistently addressed in contracts," said a Department of Defense rep on enacting the rule. "Failure to implement this rule may cause harm to the government through the compromise of covered defense information or other government data, or the loss of operationally critical support capabilities, which could directly impact national security."

## COMPANIES CONTINUALLY FAIL TO REPORT CYBER HACKING INCIDENTS SAY WHISTLEBLOWERS

Despite these regulations, companies continue to fail to report incidents of cyber hacking or security breaches. One review of just a mere 90 days of data showed there were 199 instances of purported government leaks of information of which 41 could be verified. Over the same 90-day period, only 12 agencies reported a data breach. Of the remaining incidents that were not reported, six incidents were extremely sensitive in nature, containing the home addresses and family details of subjects potentially putting government employees at risk.

"We worry that many vendors will not immediately report any cyber security problems, especially successful attacks," said leading U.S. whistleblower attorney Brian Mahany. "That directly affects our national security and could be a violation of the federal False Claims Act for those who have a government contract and don't follow cybersecurity regulations."

## MILLIONS IN WHISTLEBLOWER AWARDS AVAILABLE TO IT PROFESSIONALS

Whether cyberattacks succeed or not in obtaining sensitive information, any breach in cybersecurity that is not reported could be in violation of the False Claims Act. This means a big opportunity for whistleblowers. The False Claims Act provides whistleblowers with between 15% and 30% of any government recovery arising from settlement or successful lawsuit against the wrongdoer. The potential for a million dollar plus whistleblower award under the False Claims Act is significant since many defense department contracts can range in the millions to tens of millions of dollars.

IT professionals, federal contract administrators and other defense contractor or


Continued on next page

Continued from previous page

subcontractor employees are in prime position to detect weaknesses in security measures or breaches in cybersecurity systems. To qualify for a whistleblower award, the whistleblower must have "original source" information about the failure to report a cybersecurity breach or failure to take the required security measures involving a federal program or contract.

Whistleblower awards may not be available for simple breach of contract claims, like reports that a software system contains bugs. But if a vendor's actions are fraudulent in reporting cybersecurity status or failing to report a breach in the system, a False Claims violation may be viable.

With defense contractors' demanding work and substantial involvement in information technology, the potential for failing to provide the required levels of security and resulting cyber breaches is high. Any deliberate attempt to ignore or bypass cybersecurity rules or failure to report a breach endangers our national security and the safety of members of our armed forces along with that of each American citizen. Cyber whistleblowers are key to ensuring that our nation is safe, playing a paramount role in protecting our nations information systems. ■