Have the Floodgates Opened?

Cisco Settles First-of-Its-Kind Cybersecurity False Claims Act Litigation

By Matthew E. Feinberg

On 31 July 2019, a False Claims Act (FCA) matter pending in federal court in New York was unsealed, revealing an USD 8.6 million settlement that may have far-reaching implications for government contractors. The litigation, United States, et al., ex rel. James Glenn vs Cisco Systems, Inc., was initiated in 2011 on behalf of the federal government and a number of state governments, after a Denmark-based employee of a Cisco affiliate was terminated, allegedly for reporting a flaw in one of Cisco's video surveillance products. **With the rapidly developing role of cybersecurity in federal procurements, government contractors should clearly understand their obligations, representations, and certifications to avoid FCA liability and ensure compliance.**

According to the unsealed complaint, in 2007, Cisco created a cloud-based IP video surveillance product, Cisco Video Surveillance Manager (VSM), using software it acquired from another company. The system allows customers to connect and manage multiple video surveillance cameras through a single centralised server, which can be accessed remotely. This means that the system could connect multiple camera systems

Matthew E. Feinberg

located around the country and store data and allocate video streams from one (or a small number) of principle locations. A system such as this was particularly attractive to federal government agencies and national and international organisations, which often have many physical offices or worksites around the country or around the world that must be monitored on an ongoing basis. For example, Cisco's VSM was used by all four branches of the US Military, at schools, at the Los Angeles International Airport, by the Metropolitan Police Department in Washington, DC, and by the New York City public transit system, among others.

In October 2008, James Glenn was a computer security expert working for one of Cisco's Danish distributors when he discovered and reported alleged flaws in the Cisco VSM system that, according to the complaint, would allow a person with only a 'moderate knowledge of software/network security' and the software programme to 'exploit the system in a number of ways, including: gaining access to all video feeds, . . . all user passwords, [and] . . . all stored data on the system, modifying or deleting video feeds, and gaining permanent 'administrator' (i.e., highest-level) access to the system (which would enable future abuse to go completely undetected)'. Glenn contended that these flaws would not only render the product worthless (and likely harmful) to customers, risking exposure of their critical security data, but it would 'violate the mandatory technical requirements imposed on any computer system sold to the Government…'.

The complaint further alleges that, rather than Cisco taking action to correct the vulnerabilities with the software in response to Glenn's report, Glenn was terminated by the Danish distributor. Indeed, Cisco continued to sell the product, without repair or correction and without notice to customers of the system's vulnerabilities, until it issued a security alert in 2013,

along with a solution to solve the security flaws. By then, Glenn had already filed his FCA case, and the FBI was already investigating.

Glenn's complaint offered a somewhat novel approach to FCA liability. Rather than targeting a specific certification requirement imposed on government contractors generally, the complaint relied on the **government's** obligations regarding procurements. Specifically, Glenn noted that the Federal Acquisition Regulations (FAR), including 48 C.F.R. § 11.102, mandate that government agencies meet certain information technology (IT)-based requirements, including, in Cisco's case, the Federal Information Processing Standards (FIPS). The FIPS, in turn, incorporates certain cybersecurity requirements with which the government must comply, including those found in National Institute of Standards and Technology (NIST) Special Publications 800-53. These requirements are then flowed down, either directly or by implication, to government contractors.

Glenn argued that Cisco, in billing the government for the purchase of the Cisco VSM, was required to ensure that its surveillance products were compliant with certain provisions of the NIST, which, relevant to the Cisco case, set minimum security standards. Because, based on Glenn's report, Cisco knew that the Cisco VSM did not meet these standards, it may have presented repeated false claims to the government over a five-year period, subjecting it to potential FCA liability.

The settlement appears to be, and is being publicised in the industry as, the first time there has been a pay-out, either through a judgment or settlement, in an FCA case brought due to a party's failure to meet cybersecurity standards. But it is undoubtedly not the last. Given the favourable outcome in the Cisco case, and the substantial monetary benefits available to successful whistle-blowers in FCA matters – Glenn will receive approximately USD 1.72 million for blowing the whistle on Cisco – we expect many more cybersecurity FCA complaints to be filed in the coming years. Therefore, it is critical that government contractors have a clear understanding of their obligations, representations, and certifications regarding cybersecurity requirements on federal contracts.

Matthew Feinberg is a Partner and Chair of PilieroMazza's False Claims Act and Litigation and Dispute Resolution practice groups.

XLNC member firm
PilieroMazza PLLC
Legal
Washington DC, USA
T: +1 202 857 1000
W: www.pilieromazza.com

Matthew E. Feinberg
E: mfeinberg@pilieromazza.com