Bloomberg Law®

bloombergbna.com

Data Security

Defying Kaspersky Ban Could Trigger Plethora of Punishments

By Daniel Seiden

Federal contractors that don't comply with the governmentwide ban on Kaspersky Lab software taking effect today could face a variety of possible punishments and legal headaches.

Complying with the ban in the fiscal 2018 National Defense Authorization Act (Public Law 115-91) is not only very difficult for contractors, but the failure to get their networks ''Kaspersky-free'' could expose them to terminations, suspensions, or false claims liability, attorneys say.

The government concluded that the Russia-based Kaspersky Lab, which had provided cybersecurity products to defend computer systems in federal agencies, could be used by the Russian government for cyber intrusion.

The cases would be highly fact specific, but the government could pursue ''general contract remedies such as remediation requirements, show cause or cure notices, or potentially termination for default as a last resort,'' said Craig Schwartz of Arnold & Porter LLP, Washington.

''Potential risks relating to the ban may be more likely to arise at lower-tier subcontractor or supplier levels,'' he said. ''A subcontractor/supplier may fail to comply with removal of the software by the deadline because of a lack of awareness of the serious risks of it failing to do so.''

''It is clear that based on the regulatory and legislative history that the government is taking this ban seriously,'' said Jeniffer De Jesus Roberts of Alston & Bird, Washington.

''Because of the national security implications, I think we'll see aggressive enforcement of this ban across all agencies of the government, and particularly in the defense and intel space,'' she told Bloomberg Government.

Kaspersky has appealed the ban at the U.S. Court of Appeals for the D.C. Circuit, arguing that it is unconstitutional. The ban was a reasonable action to protect the government's information systems, a district court ruled.

A Matter of When, Not If It is a ''huge understatement'' to say it is a challenge for prime contractors to make sure subcontractors and suppliers in their supply chain are compliant and ''Kaspersky-free,'' Roberts said.

Some small companies in a prime contractor's supply chain may not have the resources to make sure they are Kaspersky-free, and therefore a prime contractor's task in eliminating Kaspersky products is a daunting task, she said.

Prime contractors may threaten subcontractors with contract breach claims, seek indemnification for noncompliance, or demand they sign certifications about compliance, but these approaches may not have the desired effect, she said.

''Let's not forget that the Kaspersky products that are the subject of the ban were developed and intended to be used to prevent their destruction in the event of a breach or intrusion, and to run undetected in the background of other systems,'' she said. ''We are talking about uninstalling a system that wasn't meant to be removed.''

Dialogue with all levels of the supply chain is critical for prime contractors because they will need to inform the government—in order to satisfy reporting obligations under the Federal Acquisition Regulation (FAR)—when, and not if, a subcontractor discovers a Kaspersky product, she said.

Lack of awareness with ban requirements may be problematic for suppliers that are primarily commercial enterprises that don't derive a large portion of their revenue from government contracting, Schwartz said.

''Those entities might not have the internal controls, and compliance structures and functions, of more seasoned government contractors,'' he said.

Multiple Risks In addition to receiving a cure notice for failing to abide by the ban, a contracting agency may issue a contract termination for default notice and pursue other actions such as suspension, or issuing a notice of proposed debarment, Roberts said.

Debarment typically ends a company's contracting opportunities for no more than three years; suspensions do the same on a temporary basis.

A suspension or debarment official might find, in more extreme cases, that a noncompliant contractor isn't ''presently responsible'' under the FAR to perform a contract because Kaspersky software remained on their systems, or the contractor didn't make a prompt disclosure after discovering the software remained on their systems, Schwartz said.

''There may also be a remote risk of implied certification liability under the False Claims Act to the extent the contractor certified compliance with U.S. law generally or the Kaspersky ban specifically, although the contractor would have materiality defenses,'' he said.

To contact the reporter on this story: Daniel Seiden in Washington at dseiden@bgov.com

To contact the editors responsible for this story: Paul Hendrie at phendrie@bgov.com; John R. Kirkland at jkirkland@bgov.com