The FAR Takes Aim at Russia's Kaspersky Lab: What Every Contractor Must Know

Related People:
Franklin C. Turner

Government Contracts Alert

06.25.2018

At this point, even casual observers of the news likely have heard of Moscow-based Kaspersky Lab. In the wake of reported connections to the Kremlin and Russian intelligence entities, the cybersecurity company was famously banned as a source of supply to the United States Government by Section 1634 of the 2018 National Defense Authorization Act ("NDAA"). Effective October 1, 2018, the NDAA forbids every "department, agency, organization, or other element of the Federal Government" from using "any hardware, software, or services developed or provided, in whole or in part" by (i) Kaspersky and any corporate successors, (ii) any entities controlled by or under common control with Kaspersky and (iii) any entity in which Kaspersky has majority ownership.

In furtherance of the NDAA's statutory mandate, the FAR Council issued an Interim Rule on June 15, 2018 that – beginning July 16, 2018 – amends the FAR to implement the Kaspersky prohibitions. In particular, the Interim Rule:

- Creates FAR Subpart 4.20, which contains policies and procedures that administratively codify the NDAA's requirements; and
- Establishes a new contract clause, FAR 52.204-23, titled "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities."

The FAR clause, which must be incorporated into all solicitations and contracts and all subcontracts in support thereof, contains two essential terms with which every Federal Government contractor should become familiar: "covered entity" and "covered article." A "covered entity" is defined as Kaspersky Lab, any successor entity to Kaspersky Lab, any entity that shares control, is controlled by, or that controls Kaspersky Lab, and any entity in which Kaspersky Lab has a majority ownership. A "covered article," in turn, is defined as any hardware, software, or service that is developed or provided in whole or in part by a covered entity **or** which contains components using any hardware or software developed in whole or in part by a covered entity.

As its title foreshadows, the clause "prohibits Government use of any covered article" and similarly bans contractors from (1) providing any covered article that the Government will use on or after October 1, 2018, and (2) using any covered article on or after

October 1, 2018 in the development of data or deliverables first produced in the performance of the contract. In addition, contractors are required to report instances in which they either have identified a covered article that has been provided to the Government or have been advised as to the existence of a covered article by a subcontractor at any tier or any other source. The reporting requirements, which vary depending on the affected contract(s), are summarized as follows:

- **For non-DoD contracts**, the contractor must inform the contracting officer in writing within 1 business day from the date it identifies the covered article or is notified of its existence. Contractors holding non-DoD indefinite delivery contracts are required to notify both the contracting officer for the indefinite delivery contract and the contracting officer(s) for any affected order(s). In its notification, the contractor must identify the contract number, the order number(s) (if applicable), the supplier name, brand, model number, original equipment manufacturer number, manufacturer part number or wholesaler number, the item description and any readily available information about mitigation actions undertaken or recommended.
  - Within 10 business days of providing the initial notification, the contractor must report any further available information about mitigation actions undertaken or recommended. Additionally, the contract is required to describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.
- **For DoD contracts**, the contractor must include the foregoing data elements, to be provided in accordance with the same timelines, in a report to be filed at https://dibnet.dod.mil.

Compliance in Four Steps: Practical Guidance for Contractors

The Interim Rule was issued without the opportunity for public comment because of the Government's determination that "urgent and compelling reasons exist" for the imposition of the NDAA's requirements on federal contractors. Although the full prohibitions do not take effect until October 1, 2018, the FAR Council has explicitly advised contractors to "take steps immediately to meet this deadline." We agree that this is a prudent course of action, particularly given the sweeping nature of the new requirements. Accordingly, here are four key actions that we recommend contractors consider as the compliance deadline nears:

1. Immediately evaluate the products and services in your supply chain to ensure that your company is not providing products or services with any nexus to Kaspersky Lab. If and as any such product or service is discovered, it should be identified, isolated, and removed as soon as possible.
2. Establish internal policies and procedures to ensure compliance with the new reporting requirements. Remember, FAR 52.204-23 requires that the identification/notification of a covered article be reported to the Government within 1 business day of discovery. In addition to the multiple data elements and mitigation measures that must be reported, a detailed follow-up report must be filed within 10 business days.
3. Inform your existing and potential subcontractors of the new requirements by providing them with a copy of FAR 52.204-23 and by obtaining written assurances that they (a) understand what the clause mandates and (b) will comply with its requirements.
4. Modify your existing FAR flow-down templates to include FAR 52.204-23 for all subcontracts awarded on or after July 16, 2018.

At an indeterminate point in the future, the Government will issue a Final Rule that will likely modify at least some of the foregoing requirements. If your company would like to propose changes to the Interim Rule or otherwise engage with the Government regarding the requirements, it must submit comments by August 14, 2018. But for now, these are the new rules with which every contractor must comply. The bottom line – to borrow and Russianize a

timeless phrase from Nancy Reagan – is that federal contractors are now required to "Just Say *Nyet*" to Kaspersky.