Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Russian Exorcism Of US Gov't Contracts

By **Franklin Turner and Alexander Major** (July 12, 2018, 1:14 PM EDT)

Franklin Turner

Alexander Major

The Demon: What an excellent day for an exorcism.
Father Karras: You would like that?
The Demon: Intensely.

Honestly, it was challenging finding an all-audiences quote from William Peter Blatty's "The Exorcist," but we believe that this quote is exactly what federal contractors need to know. Today is indeed an excellent day for an information system exorcism and, unlike Father Karras, federal contractors know the name of that which they must purge: Kaspersky Lab.

As even casual observers of the news likely know by now, in the wake of reported connections to the Kremlin and Russian intelligence entities, the Moscow-based cybersecurity company has had a tumultuous year. It started with the company being removed from the General Services Administration list of approved vendors last July. Then, in the fall, Acting Homeland Security Secretary Elaine Duke issued a directive giving federal agencies a timeline to rid their networks of the software. Shortly thereafter, the company was famously banned as a source of supply to the United States government by Section 1634 of the 2018 National Defense Authorization Act, which 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 (1) Kaspersky and any corporate successors, (2) any entities controlled by or under common control with Kaspersky, and (3) any entity in which Kaspersky has majority ownership.

Now, in furtherance of the NDAA’s statutory mandate, beginning July 16, 2018, the Federal Acquisition Regulation is amended to implement the prohibitions targeting Kaspersky and providing federal contractors until Oct. 1, 2018, to tie their information systems to the bedposts, get out their cybersecurity holy water, avoid long staircases, and exorcise Kaspersky products and services from their systems. In particular, the new 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.”

In a staggering display of clarity, the FAR clause, which must be incorporated into all solicitations and contracts and all subcontracts in support thereof, contains two essential — and lucidly defined 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.

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 Oct. 1, 2018, and, (2) using any covered article on or after Oct. 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 identify 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.

Please excuse the pun, but all federal contractors that possess — or may possess — Kaspersky products will need to take heed of the reporting requirements, which will vary depending on the affected contract(s), are summarized as follows:

- For non-U.S. Department of Defense contracts, the contractor must inform the contracting officer in writing within one 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.
    - The contractor 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. (As with any reporting/disclosure obligation through the DIBNet portal, remember that a DOD-approved medium assurance certificate is required. As such, it is not something that should wait until last

minute as it will require payment, document collection and the provision of key information for the company.)

Casting Out the Unclean — Practical Guidance for Contractors

As the government's head was spinning 360 degrees from the "alleged" Russian tampering with its systems, the 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 Oc. 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 and exacting nature of the new requirements. Accordingly, here are key actions that we recommend contractors consider as the compliance deadline nears:

1. Examine your systems for any Kaspersky products. Document that effort in your information security plan — even if nothing is found — and update that plan to make clear to your employees that Kaspersky is not to be permitted on any system that touches federal information.

2. If Kaspersky products are identified, remove them and all vestigial programs from your systems. Document that effort and all efforts to "double check" the removal of any lagging programs or system modifications made by the product(s). If and as any such product or service is discovered, it should be identified, isolated, removed and replaced as soon as possible. Remember, don't just delete it — replace it!

3. If Kaspersky products were indeed being used in performance of a federal contract, after or incidental to a removal, perform an internal cyber investigation to ensure that there are none of the alluded-to "back doors" or vulnerabilities left behind. If you were relying on Kaspersky for system security — check to make sure your system's security isn't tainted — it will be well worth the effort.

4. Cleanse Kaspersky from your supply chain. Immediately perform a documented evaluation — with documentation — on 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.

5. Establish or update internal policies and procedures to ensure compliance with the new purchasing restrictions and reporting requirements. Remember, FAR 52.204-23 requires that the identification/notification of a covered article be reported to the government within one 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.

6. Modify your existing FAR flow-down templates to include FAR 52.204-23 for all subcontracts awarded on or after July 16, 2018.

7. Inform 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 (1) understand what the clause mandates and (2) will comply with its requirements.

8. Use this effort to ensure your information security policies are up to date and aligned with all the recent updates provided by the Department of Defense chief information officer and the modifications

of NIST Special Publication 800-171 and its related requirements (e.g., National Institute of Standards and Technology SP 800-171A, DOD Guidance for Reviewing System Security Plans; and the NIST SP 800-171 Security Requirements Not Yet Implemented).

9. Train your employees on the new requirements so they can assist the company on ensuring compliance.

10. Do not delay. Get this done immediately and engage counsel if any problems are found when complying with the rule.

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 Aug. 14, 2018. But for now, these are the new rules with which every contractor must comply. We suggest that to avoid the regulatory equivalent of being hit by projectile vomit to the face, federal contractors take immediate action to ensure that their systems — and the systems of their subcontractors and supply chain — are not using Kaspersky products. The power of the FAR compels you.

Franklin C. Turner and Alexander W. Major are partners at McCarter & English LLP.