PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 9 **NUMBER 6** **June 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:
Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341

Customer Service Website . . . . . http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call
Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)
ISSN: 2688-7290

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt).
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Originally published in: 2017

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

Editor-in-Chief, Editor & Board of Editors

Pratt's Government Contracting Law Report is published 12 times a year by Matthew Bender & Company, Inc. For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

Spy Games: Biden Administration Issues Executive Order Restricting Federal Use of Commercial Spyware

By Michael G. Gruden, Evan D. Wolff, Adelicia R. Cliffe and Jacob Harrison*

In this article, the authors discuss an executive order signed recently by President Biden that restricts federal agencies' use of commercial spyware.

President Biden has signed the Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security (EO),[1] restricting federal agencies' use of commercial spyware. The Biden Administration cited targeted attacks utilizing commercial spyware on U.S. officials and human rights abuses abroad as motivations for these restrictions.

USAGE RESTRICTIONS

The EO is not a blanket ban on commercial spyware, defined in the EO as "any end-to-end software suite that is furnished for commercial purposes, either directly or indirectly through a third party or subsidiary, that provides the user of the software suite the capability to gain remote access to a computer, without the consent of the user, administrator, or owner of the computer, in order to:

(i) Access, collect, exploit, extract, intercept, retrieve, or transmit content, including information stored on or transmitted through a computer connected to the internet;

(ii) Record the computer's audio calls or video calls or use the computer to record audio or video; or

(iii) Track the location of the computer."

The term "computer" includes smart devices or other high-speed data processing device performing logical, arithmetic, or storage functions, as well as any data storage facility or communications facility linked to such a device.

---

* Michael G. Gruden (mgruden@crowell.com), Evan D. Wolff (ewolff@crowell.com), Adelicia R. Cliffe (acliffe@crowell.com) and Jacob Harrison (jharrison@crowell.com) are attorneys with Crowell & Moring LLP.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.

Instead, the EO bars federal government agencies from using commercial spyware tools if they pose significant counterintelligence or security risks to the U.S. government, or significant risks of improper use by a foreign government or foreign person, including to target Americans or enable human rights abuses. Indirect use of such spyware (e.g. through a contractor or other third party) is also prohibited. The EO establishes risk factors indicative of prohibited commercial spyware, including:

- Past use of the spyware by a foreign entity against U.S. government personnel or devices;
- Past use of the spyware by a foreign entity against U.S. persons;
- The spyware was or is furnished by an entity that maintains, transfers, or uses data obtained from the commercial spyware without authorization from the licensed end-user or the U.S. government, or has disclosed or intends to disclose non-public information about the U.S. government or its activities without authorization from the U.S. government;
- The spyware was or is furnished by an entity under the direct or effective control of a foreign government or foreign person engaged in intelligence activities directed against the United States;
- A foreign actor uses the commercial spyware to limit freedoms of expression, peaceful assembly or association; or to enable other forms of human rights abuses or suppression of civil liberties; or
- The spyware is furnished to governments that have engaged in gross violations of human rights, whether such violations were aided by the spyware or not.

The above restrictions do not apply to the use of commercial spyware for purposes of testing, research, analysis, cybersecurity, or the development of countermeasures for counterintelligence or security risks, or for purposes of a criminal investigation arising out of the criminal sale or use of the spyware. Additionally, an agency may be able to obtain a waiver allowing it to temporarily bypass the EO's prohibitions, but only in "extraordinary circumstances."

AGENCY REPORTING REQUIREMENTS

The EO contains various agency reporting requirements. Some are specific to the Director of National Intelligence (DNI) while some apply to all federal agencies:

- Within 90 days of the EO, the DNI will issue a classified intelligence

assessment on foreign commercial spyware and foreign use of commercial spyware.

- Within 90 days of the DNI assessment, all federal agencies must review their use of commercial spyware and discontinue uses that violate the EO.
- If an agency elects to continue using commercial spyware, within one year of the EO it must report its continued use to the Assistant to the President for National Security Affairs (APNSA) and explain why its continued use does not violate the EO.

NEW COMMERCIAL SPYWARE PROCUREMENT PROCEDURES

Agencies seeking to procure commercial spyware "for any purpose other than for a criminal investigation arising out of the criminal sale or use of the spyware" must:

- Consider any relevant information provided by the DNI, and solicit such information from the DNI if necessary;
- Consider the risk factors listed above;
- Consider any controls the commercial spyware vendor has in place to detect and prevent potential security risks or misuse; and
- Notify APNSA within 45 days of procurement and provide a description of its intended purpose and use(s) for the commercial spyware.

Key Takeaways

While the EO signals that the federal government is approaching commercial spyware with caution, interested parties should note that the government has been careful not to rule out its usage altogether. The EO, for example, does not address the government's use of non-commercial (i.e. government-produced) spyware, or mention state or local government use of commercial spyware at all. The EO also allows federal agencies to procure and employ commercial spyware so long as the agency determines that the spyware does not pose a significant risk to national security or for improper use. Vendors of commercial spyware should pay close attention to the risk factors identified in the EO and consider implementing internal controls to address them.