PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 9 **NUMBER 5** **May 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.

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

MATTHEW BENDER

(2023–Pub.4938)

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.

Recent Government Contracts Cybersecurity Developments Demonstrate the Need for Enhanced Monitoring Now

By Dawn Stern and Thomas Daley*

In this article, the authors discuss a recent statement by a Department of Defense (DoD) official that DoD agencies will begin to include cybersecurity controls as an evaluation criterion in competitive procurements, as well as a number of bid protest decisions involving cybersecurity-related protest grounds.

The juxtaposition of a recent statement by a Department of Defense (DoD) official and a number of bid protest decisions involving cybersecurity-related protest grounds demonstrates the ever-increasing need for contractors to remain vigilant in their review of their cybersecurity infrastructure, policies, contract requirements, and certifications.

THE DEPARTMENT OF DEFENSE

During a September 2022 cybersecurity conference, Stacy Bostjanick (DoD's Chief Defense Industrial Base Cybersecurity, Deputy Chief Information Officer for Cybersecurity) stated that DoD contracting officers were being instructed to consider including compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171[1] as an evaluation criterion in upcoming procurements. Bostjanick suggested that the office of the DoD Chief Information Security Officer had provided contracting officers with sample solicitation language addressing evaluation of NIST SP 800-171 compliance.

Additionally, Bostjanick indicated that contracting officers will be taking a more aggressive approach to evaluating an officer's compliance with NIST SP 800-171. She said that non-compliance "could have implications for you moving forward and your position on a competitive procurement."

---

* Dawn Stern and Tom Daley are attorneys in DLA Piper's Government Contracts practice. They provide both litigation and counseling services on matters related to doing business with federal, state and local governments. As part of their practice, the authors advise clients on the cybersecurity obligations of government contractors. They may be contacted at dawn.stern@dlapiper.com and tom.daley@dlapiper.com, respectively.

[1] NIST SP 800-171 provides a list of 110 controls for protecting controlled unclassified information (CUI). Pursuant to Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, covered contractor information systems are subject to the requirements in NIST SP 800-171.

Thus, although the DoD's Cybersecurity Maturity Model Certification is still in the process of being finalized, agencies may begin considering offerors' compliance with NIST SP 800-171 as an evaluation criterion in competitive procurements in the near future.

BID PROTESTS INVOLVING ISSUES RELATING TO CYBERSECURITY

There recently has been an increase in the number of cybersecurity-related issues in bid protests before both the U.S. Government Accountability Office (GAO) and the U.S. Court of Federal Claims, including the following decisions.

- GAO concluded that an agency reasonably rated an offeror's proposal as technically unacceptable when, in response to a solicitation that expressed a need for an increased focus on cybersecurity, the protestor failed to adequately address how it would meet solicitation requirements for cybersecurity testing and evaluation.[2]
- The GAO found that an agency reasonably evaluated an offeror as being ineligible for award when the offeror's proposal did not adequately demonstrate that its solution would be hosted within an approved Federal Risk and Authorization Management Program (FedRAMP) moderate environment as required by the solicitation.[3]
- The Court of Federal Claims similarly denied a protest alleging that an agency erred in evaluating the FedRAMP authorization of its proposed solution when the protestor could not demonstrate that its proposed solution met the solicitation's FedRAMP authorization requirements at the time of proposal submission, as required by the solicitation.[4]
- The GAO addressed FedRAMP authorization issues in a protest challenging a sole-source award. The GAO determined that the protestor was not an interested party for purposes of challenging the award because the sole-source justification articulated a need for a

---

[2] SimVentions, Inc., B-420967 et al. (Comp. Gen. Nov. 21, 2022).

[3] Computerized Facility Integration LLC, B-420865 (Comp. Gen. Sept. 28, 2022). Conversely, an agency took corrective action in response to an argument that it engaged in disparate treatment by excluding a protestor's solution from a list of approved licenses based on a lack of FedRAMP authorization while also including another offeror's solution on the approved list notwithstanding that the other offeror also lacked FedRAMP authorization. See Meridian Knowledge Sols., LLC, B-420808.3 (Comp. Gen. Dec. 5, 2022).

[4] LS3, Inc. v. United States, No. 22-1274 (Fed. Cl. Oct. 7, 2022).

solution with a FedRAMP moderate authorization, but the protestor's solution lacked such authorization.[5] Thus, the protestor was not an interested party because, even if the contract was competed on a full-and-open basis, the protestor would be ineligible for award.

- The GAO concluded that an agency reasonably canceled a solicitation when the agency had experienced a change in its cybersecurity requirements.[6] The agency in that protest cancelled its solicitation relating to a learning management software system because it decided that, contrary to the terms of the original solicitation, it needed a solution that was authorized at the FedRAMP moderate level or higher. In reaching that conclusion, the agency explained that recent high-profile cybersecurity incidents and Executive Order 14028 ("Improving the Nation's Cybersecurity"), which encouraged agencies to make "bold changes and significant investments" to improve cybersecurity, had led to the agency reconsidering its cybersecurity needs.
- The Court of Federal Claims' issued a decision in the *American Roll-On Roll-Off Carrier Group* litigation.[7]
- The Court of Federal Claims' issued a decision in the *American Roll-On Roll-Off Carrier Group litigation*. In March 2022, the GAO denied a protest that alleged that an awardee had misrepresented its cybersecurity compliance by representing its FedRAMP authorization level as "high" when it should have been represented as "medium." After the GAO denied its protest, the protestor filed a protest in the Court of Federal Claims, which included a protest ground addressing the FedRAMP authorization misrepresentation claim that the GAO had denied. The Court of Federal Claims rejected the FedRAMP misrepresentation ground, finding that the protestor could not demonstrate that it was prejudiced by the alleged misrepresentation. The Court of Federal Claims explained that, although the awardee's claim of having a high FedRAMP authorization was "suspect," the security requirement in the solicitation was not a material term of the solicitation, and the agency did not rely on the FedRAMP authorization representation when making its award decision.

---

[5] Meridian Knowledge Sols., LLC, B-420906 (Comp. Gen. Nov. 2, 2022).

[6] Meridian Knowledge Sols., LLC, B-420150.4 et al. (Comp. Gen. Aug. 25, 2022).

[7] See Connected Glob. Sols., LLC v. United States, No. 22-292C (Fed. Cl. Oct. 28, 2022).

GOING FORWARD

Although the government is increasing its focus on cybersecurity compliance, at least one recent survey of 300 contractors suggests that a majority of companies do not satisfy the applicable cybersecurity requirements in their contracts. Moreover, as illustrated by the recent bid protest decisions discussed above, the trend toward using cybersecurity as an evaluation factor will result in greater scrutiny of contractors' cybersecurity infrastructures and authorizations by both the government and competitors.

All of this is occurring at a time when, even outside the government contracts context, authorities are focused on how companies respond to data breaches – including bringing criminal charges against high-ranking company officials. These issues highlight the importance of government contractors thoroughly reviewing their cybersecurity infrastructure, policies, contract requirements, and representations.