PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 8 **NUMBER 3** **March 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

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

(2022–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.

Cybersecurity Provisions Proliferate in the National Defense Authorization Act

By Christopher R. Hebdon, Kate M. Growley, Evan D. Wolff, Maida Oringher Lerner and Michael G. Gruden*

This article highlights the inclusions and omissions of note for government contractors, cybersecurity professionals and critical infrastructure providers in the National Defense Authorization Act for Fiscal Year 2022.

The National Defense Authorization Act ("NDAA") for Fiscal Year ("FY") 2022, signed into law on December 27, 2021,[1] contains a plethora of cybersecurity provisions on topics from ransomware and incident response, to procurement programs and public-private partnerships, to critical infrastructure. This article highlights the inclusions and omissions of note for government contractors, cybersecurity professionals and critical infrastructure providers.

RANSOMWARE

In response to the recent rise in ransomware attacks, Section 1510 directs the Department of Defense ("DoD") to conduct a comprehensive assessment of its ability to disrupt and defend against ransomware attacks and develop recommendations to deter and counter such attacks. The DoD will brief Congress on its assessment and recommendations by the end of July 2022.

INCIDENT RESPONSE

Section 1546 and 1547 instruct the Cybersecurity and Infrastructure Security Agency ("CISA") to update and then evaluate the National Cyber Incident Response Plan. Section 1546 amends 6 U.S.C. § 660 to require CISA to update the National Cyber Incident Response Plan at least every two years to address the evolving threat landscape and adds a requirement for CISA to engage with industry on the government's responsibilities and capabilities with regard to incident response.

Section 1547 establishes within CISA a National Cyber Exercise Program intended to evaluate the National Cyber Incident Response Plan. The program

---

* Christopher R. Hebdon (chebdon@crowell.com) and Michael G. Gruden, CIPP/G (mgruden@crowell.com) are associates at Crowell & Moring. Kate M. Growley, CIPP/G, CIPP/US (kgrowley@crowell.com) and Evan D. Wolff (ewolff@crowell.com) are partners at the firm. Maida Oringher Lerner (mlerner@crowell.com) is a senior counsel at the firm. The authors are members of the firm's Government Contracts and Privacy and Cybersecurity Practice Groups.

[1] https://www.congress.gov/bill/117th-congress/senate-bill/1605/text?q=%7B%22search%22%3A%5B%22S.1605%22%2C%22S.1605%22%5D%7D&r=1&s=1.

will be based on current risk assessments and designed to simulate the partial or complete incapacitation of a government or critical infrastructure network from a cyber attack. As part of the program, CISA will select model exercises that public and private sector entities can adopt and aid such entities with the design, implementation, and evaluation of incident response plans and exercises.

CONTROLLED UNCLASSIFIED INFORMATION

Of note to government contractors, the FY2022 NDAA contains two provisions focused on improving the government's Controlled Unclassified Information ("CUI") program. The first, Section 1526, instructs the DoD to publish a report by the end of June 2022 on the "DoD CUI Program," including:

- The extent to which the DoD is properly marking or otherwise identifying CUI;
- The circumstances under which commercial information can be considered CUI;
- The benefits and drawbacks of requiring CUI to be marked with a unique CUI legend; and
- Examples of information that is and is not considered CUI.

The second, Section 6423, addresses a subset of CUI common in the transportation sector, known as Sensitive Security Information ("SSI"). This section gives the Transportation Security Administration ("TSA") until the end of March 2022 to ensure:

- Clear and consistent designation of SSI;
- Update SSI identification guidelines;
- Identify challenges affecting the identification, redaction, and designation of SSI; and
- Ensure that TSA personnel are adequately trained on applicable policies and procedures.

Thereafter, the TSA will communicate with stakeholders who handle SSI, including contractors, to raise awareness of the TSA's policies and guidelines governing the handling and use of SSI.

CYBERSECURITY MATURITY MODEL CERTIFICATION

The Act also instructs the DoD to publish two separate reports on the implementation of Version 2.0 of its Cybersecurity Maturity Model Certification ("CMMC") program. Section 1533 requires the submission of a report on the Department's plans for the CMMC program, including, among other things:

- The rulemaking process;
- Communications with industry;
- Reimbursing contractors for the cost of compliance; and
- The role of prime contractors with respect to the cybersecurity of their subcontractors.

Of note, the report must address the DoD's plans for reimbursing small and non-traditional defense contractors for the cost of certification and ensuring that companies seeking a DoD contract for the first time are reimbursed for their cost of compliance in the event they are not awarded a contract.

Section 866, meanwhile, mandates the issuance of a report on the effects of CMMC on small businesses, including the estimated costs of compliance; an explanation of how such costs will be recoverable from the government; and the DoD's plans to mitigate negative effects on small businesses, ensure that small businesses are appropriately trained, and work with small businesses to enable them to bid on and win contracts without having to risk funds on compliance.

The reports are due by the end of March and June 2022, respectively.

PROCUREMENT OF CYBERSECURITY PRODUCTS AND SERVICES

Section 1521 gives the DoD until the end of 2022 to designate an executive agent for the enterprise-wide procurement of so-called "cyber data products and services" (i.e., commercially available datasets and analytic services germane to offensive and defensive cyber operations, including products and services that provide technical data, indicators, and analytic services relating to cyber threats). Thereafter, by July 2023, DoD components will be prohibited from independently procuring a cyber data product or service that has been procured for enterprise-wide use, unless such component is able to conduct the procurement at a lower price or the executive agent approves the purchase.

PUBLIC-PRIVATE PARTNERSHIPS

Section 1508 instructs U.S. Cyber Command to establish a voluntary process to partner with private sector information technology and cybersecurity companies to explore and develop methods and plans to coordinate the actions of private sector entities and U.S. Cyber Command against malicious cyber actors. The coordination process should be up and running by January 1, 2023, and requires U.S. Cyber Command to ensure that trade secrets and proprietary information remain private and protected.

Section 1550 creates a five-year pilot program within CISA to assess the possibility of establishing voluntary public-private partnerships with "internet

ecosystem companies" to support actions by such companies to discover and disrupt malicious cyber actors. As used here, the phrase internet ecosystem company means a U.S. business that provides, among other things, cybersecurity, internet, telecommunications, content delivery, and/or cloud services. As part of the program, CISA may:

- Help companies develop effective know-your-customer programs;
- Provide technical assistance and analytics to improve the private sector's ability to detect and prevent illicit or suspicious actions through their services;
- Develop and socialize best practices for the collection, retention, and sharing of data to support discovery and disruption of malicious cyber activity; and
- Share actionable intelligence and indicators of compromise for ongoing and potential threats; as well as
- Provide recommendations for workflows, training, automated tools, and technical capabilities for internet ecosystem companies to implement to reliably detect, analyze, disrupt, and mitigate malicious cyber operations conducted using their services.

ZERO TRUST

Section 1528 seeks to further the government-wide adoption of zero trust architectures and instructs the DoD to develop a zero trust strategy and model architecture for use across the DoD Information Network. The strategy must include:

- Policies for implementing zero trust in on-premises, hybrid, and cloud environments;
- Policies specific to operational technology, critical data, infrastructure, weapons systems, and classified networks;
- Specifications for the enterprise-wide acquisition of zero trust capabilities; and
- A metrics-based assessment plan.

Congress instructed the DoD, in developing the strategy, to encourage the use of third-party cybersecurity-as-a-service models and engage with industry on issues relating to the deployment of zero trust architectures.

CRITICAL INFRASTRUCTURE

In order to further strengthen the nation's critical infrastructure against cyber threats, such as last year's ransomware attack against Colonial Pipeline, Section

1541 requires CISA to identify and address threats and vulnerabilities to information and operational technologies intended for use in the automated control of critical infrastructure. To do so, the NDAA directs CISA to:

- Lead government efforts to identify and mitigate cybersecurity threats to industrial control systems;
- Maintain threat hunting and incident response capabilities;
- Provide technical assistance to identify, evaluate, assess, and mitigate vulnerabilities; and
- Disseminate vulnerability information to the critical infrastructure community.

Sections 1542 through 1544 also relate to the identification and remediation of cybersecurity vulnerabilities. Section 1542 allows CISA to identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information and industrial control systems; while Section 1543 requires the submission of a report to Congress by the end of 2022 detailing CISA's efforts to mitigate such vulnerabilities and improve information sharing with the private sector. Section 1544, meanwhile, authorizes the Department of Homeland Security ("DHS") to establish an incentive-based program for industry, academia, and others to identify remediation solutions for cybersecurity vulnerabilities in information and industrial control systems.

Section 1548 establishes within CISA a "CyberSentry" program to provide continuous monitoring and detection of cybersecurity risks to owners and operators of critical infrastructure. Private sector participation in the program will be voluntary. As part of the program, CISA will enter into strategic partnerships with critical infrastructure providers to:

- Provide technical assistance in the form of continuous monitoring of industrial control systems;
- Leverage intelligence to advise providers regarding mitigation measures;
- Identify risks to industrial control systems and work with critical infrastructure providers to remediate vulnerabilities; and
- Produce aggregated, anonymized analytic products with findings and recommendations that can be disseminated to partner entities.

NOTABLE OMISSIONS

While debating the FY2022 NDAA, Congress elected to omit a handful of notable cyber provisions that could reappear, at least in some form, in the coming months. The NDAA, for example, does not include a high-profile provision that would have required private sector entities to report ransomware

incidents to CISA within 24 hours and most other cyber incidents within 72 hours. Nor does the legislation include provisions proposed in the House to codify the Federal Risk and Authorization Management ("FedRAMP") program and update the Federal Information Security Modernization Act ("FISMA").