AN A.S. PRATT PUBLICATION
JUNE 2023
VOL. 9 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 5** **June 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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 Web site ..... 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

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires 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 Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Veterans Affairs Contractors Have Broad New Cybersecurity Obligations

By Eric S. Crusius*

In this article, the author discusses the steps that the U.S. Department of Veterans Affairs is taking to overhaul and remake its regulations aimed at contractor cybersecurity and privacy policies.

The U.S. Department of Veterans Affairs (VA) is overhauling and remaking its regulations aimed at contractor cybersecurity and privacy practices.[1] Any companies in the VA supply chain should take note and ensure compliance with these regulations, which significantly increase obligations in certain circumstances – including immediate breach notification requirements and liquidated damages for breaches – and allow unscheduled on-site inspection of contractor information technology (IT) systems.

The following is a summary of some of the significant policies and contract clauses impacting contractors.

POLICIES

Basic Safeguarding of Covered Contractor Information Systems

Initially, the VA creates a new Subpart (804.19) that sets out policies and procedures for the protection of certain VA information – namely, "VA information, information systems, and VA sensitive information." This part covers the acquisition of commercial products and services, excluding commercial off-the-shelf items. While "VA information" is not defined, the definitions for "information system" and "VA sensitive information" indicated a broad and inclusive approach. For instance, "VA sensitive information" includes:

> information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-

* Eric S. Crusius, a partner in the Tysons, Virginia, office of Holland & Knight LLP, focuses his practice on a wide range of government contract matters, including bid protests, claims and disputes, compliance issues and sub-prime issues. He may be contacted at eric.crusius@hklaw.com.

[1] https://www.govinfo.gov/content/pkg/FR-2023-01-25/pdf/2023-00586.pdf.

client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

While not exactly like the definition of controlled unclassified information (CUI), it is likewise arguable that the definition of "VA-sensitive" information is so broad and can include most information contractors create, store or transmit in the performance of a VA contract or subcontract.

Contractors who have a covered contract must, among other things:

(1) Comply with all VA information security and privacy policies;

(2) Complete VA security awareness training annually; and

(3) Disclose all security or privacy incidents within one hour of discovery to the contracting officer and contracting officer's representative. This disclosure is even required if an incident is suspected.

Liquidated Damages

The VA adds a new Subpart (811.5) dedicated to liquidated damages in contracts that involve VA-sensitive personal information. This is narrower than the definition of VA-sensitive information noted above and essentially adds personally identifiable information as a limiting element. In the instances of a data breach involving this type of information, the liquidated damages would be used to pay for credit monitoring services and other things detailed below.

There is no indication that the contractor (or subcontractor) would have had to act contra to VA cybersecurity requirements in order to be responsible for liquidated damages; it appears to be a strict liability standard.

Protection of Individual Privacy

New sections are added within Subpart 824.1, including ones to require the inclusion of new clauses ensuring privacy of individuals with protected health information, the requirement to flow down Business Associate Agreements and inclusion of the liquidated damages clause.

Acquisition of Information Technology

Previously reserved, the VA adds a new Part 839 specifically setting out policies for IT acquisitions. Under this Part, the VA would require contractors providing IT products and services to, among other things, comply with VA Directive 6500 and "use appropriate common security configurations available" from the National Institute of Standards and Technology (NIST). The exact NIST standards are not defined within the policy, except pointing to NIST's checklists.

SOLICITATION CLAUSES

The above policies are implemented through the following clauses that the VA inserts into relevant contracts.

Information and Information Systems Security

This clause is required to be inserted whenever FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, is required and covers a broad base of contractors, including those with access to "VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services."

At its center, it requires that covered VA contractors adhere to VA Directive 6500. VA Directive 6500 is comprehensive and contains more than 150 separate controls, including the necessity of an incident response plan. Besides VA Directive 6500, contractors are also expected to comply with VA Handbooks, and other listed requirements.

Depending on the type of information involved, the prime contractor and subcontractors may be required to enter into Business Associate Agreements. Further, contractors are required to develop software and perform services within the U.S. "to the maximum extent practicable." Services that are proposed to be performed under the contract that are not disallowed by law to be outside the U.S. must be disclosed in the proposal and include a detailed Information Technology Security Plan.

Other notable requirements include:

- A four-hour notification requirement if employees with access to a VA information (including by virtue of working on a VA information system) leave or are reassigned;
- Using data only from the VA or developed by the contractor under the contract for the purposes outlined in the contract;
- Separation of VA information from other information the contractor possesses;
- Sanitation of data in accordance with VA Directive 6500;
- Provision of "all necessary access" to VA and U.S. Government Accountability Office staff for scheduled and unscheduled on-site inspections of contractor information systems assets by the VA;
- Destruction of data in accordance with VA policies, including VA Directive 6371, within 30 days after the termination of the contract and compliance with other policies concerning copying, retaining, using, returning and destroying relevant information;

- Encryption of data consistent with Federal Information Processing Standard 140-3;
- Meeting the VA's guidelines for firewalls and web services security controls;
- Compliance with relevant privacy laws;
- Reporting cybersecurity incidents or imminent cybersecurity incidents in writing to the contracting officer and contracting officer representative within one hour of discovery;
- Providing training to certain employees who have access to VA information or VA information systems; and
- Flowing down this clause to subcontractors covered by the above requirements.

Liquidated Damages

Contractors with access to sensitive personal information must provide liquidated damages in the event of a breach that results in spillage of that information. The contractor may instead provide actual damages if they can be proven. Either way, the damage calculations should take into account costs for notifications, credit monitoring, data breach analysis and impact assessment, fraud alerts, and identity theft insurance. Further, under alternate contract language, the VA may obtain damages for the repurchase of goods and services.

Gray Market and Counterfeit Items

The VA proposes significantly updating an existing clause (852.212-71) that previously concerned only gray market goods. The new clause also prohibits the sale of counterfeit goods to the VA. While this may seem obvious, the definition of "counterfeit" is broad and includes substitutions defined as including "used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics." There is also a new clause (852.212-72) that would specifically allow "used, refurbished, or remanufactured parts" under certain circumstances. Gray market and counterfeit items would still be prohibited.

Other Clauses of Interest

In addition to the above, the following is a selection of clauses that the VA is proposing to revise or add:

- *Security Requirements for Information Technology Resources (852.239-70)*: Contractors with access to VA information are responsible for the security of that information, have an Information System Security Plan submitted within 90 days of contract award, have their system security

accredited, give access to the federal government when requested (including subcontractor systems) and flow these requirements down the supply chain when applicable.

- *Security Controls Compliance Testing (852.239-74)*: This allows the VA, including the VA Inspector General (with 10 working days' notice), access to each location where VA information is "processed or stored, or information systems are developed, operated maintained, or used on behalf of VA …" The VA may also conduct assessments without notice.

SUMMARY

- The VA is revamping its contractor cybersecurity and privacy practice regulations to heighten immediacy of breach of information disclosure and require damages for such breaches, among other enhancements.
- These efforts include better protecting contractor systems that handle sensitive VA information and possibly requiring prime contractors and subcontractors to enter into specified business agreements.
- Current and prospective government contractors are encouraged to review these regulations to ensure compliance and avoid potential significant consequences.

CONCLUSION

Taken together, contractors that do business with the VA will face significant new cybersecurity and privacy responsibilities. These responsibilities do not apply just to contractors with personally identifiable information, but information that contractors will come across or create on most contracts for IT products and services. Contractors covered by this should review these regulations and ensure compliance or risk adverse consequences from the VA.