

THE JOURNAL OF FEDERAL AGENCY ACTION

Editor's Note: Overcriminalization

Victoria Prussen Spears

Trump Administration Takes Aim at Regulatory Overcriminalization

Michael E. Clark, Joe D. Whitley, Jacob Edwards, and Matthew L. Hickman

Government Focus on Oil Smuggling Schemes and Cartels Reinforces the Need for Anti-Money Laundering and Know Your Customer Programs

Carrie Elizabeth DeLange, Deanna R. Reitman, and Joie C. Hand

Bureau of Alcohol, Tobacco, Firearms and Explosives Announces Firearms Regulatory Reforms and Renewed Partnership with Firearms Industry

Michael D. Faucette and Isaac J. Wyant

Targeting “Foreign Adversary” Interests, Federal Communications Commission Proposes Broadly Applicable Ownership Reporting Regime

Sara M. Baxenberg, Eve Klindera Reed, Kathleen E. Scott, Melissa Alba, and Ania Trichet

Prepare Now for EDGAR Next

Daniel Nussen, Jason Rocha, Danielle Herrick, and Guiying Ji

National Highway Traffic Safety Administration Announces First Actions Under Trump Administration's New Framework for Removing Regulatory Barriers for Automated Vehicles

Rebecca Baden Chaney and Rachael Padgett

Ready to Know Your Data? Justice Department Issues Implementation and Enforcement Guidance for Data Security Program Protecting Bulk Sensitive Data

Kate M. Growley, Caitlyn Weeks, Jacob Harrison, Nigel Cory, and Linda Malek

Environmental Protection Agency Ends Environmental Justice Considerations in Enforcement; Highlights Energy Production; Further Emphasizes Deregulatory Actions

Samuel B. Boxerman, Byron F. Taylor, Timothy K. Webster, and Rose Quam-Wickham

Environmental Protection Agency's Deregulatory Initiative to “Power the Great American Comeback”

Rich Gold, Susan G. Lafferty, Andy Emerson, Dimitrios J. Karakitsos, and Maggie P. Pahl

Securities and Exchange Commission's Division of Corporation Finance Issues No-Action Letter Response Regarding Issuer Verification Steps for Accredited Investor Status

Joel I. Greenberg, Sara Adler, Meir Lax, and Peter G. Danias

Department of Defense Mandates Use of Software Acquisition Pathway for Software Development Procurements

Tracye Winfrey Howard, Gary S. Ward, Scott A. Felder, Teresita Regelbrugge, and Vaibhavi Patria

Department of Health and Human Services Office of General Counsel Statement of Organization Suggests Potential Consolidation, Expansion of Authority

Jaime L.M. Jones, Meenakshi Datta, Rebecca K. Wood, Raj D. Pai, Colleen Theresa Brown, and Michael Varrone

What the Foreign Corrupt Practices Act Criminal Enforcement Pause Means for Companies

Kevin B. Muhlendorf, Vesna K. Harasic-Yaksic, Brandon J. Moss, and Corey J. Hauser

The Journal of Federal Agency Action

Volume 3, No. 5 | September–October 2025

- 317 Editor's Note: Overcriminalization**
Victoria Prussen Spears
- 323 Trump Administration Takes Aim at Regulatory Overcriminalization**
Michael E. Clark, Joe D. Whitley, Jacob Edwards, and Matthew L. Hickman
- 329 Government Focus on Oil Smuggling Schemes and Cartels Reinforces the Need for Anti–Money Laundering and Know Your Customer Programs**
Carrie Elizabeth DeLange, Deanna R. Reitman, and Joie C. Hand
- 337 Bureau of Alcohol, Tobacco, Firearms and Explosives Announces Firearms Regulatory Reforms and Renewed Partnership with Firearms Industry**
Michael D. Faucette and Isaac J. Wyant
- 343 Targeting “Foreign Adversary” Interests, Federal Communications Commission Proposes Broadly Applicable Ownership Reporting Regime**
Sara M. Baxenberg, Eve Klindera Reed, Kathleen E. Scott, Melissa Alba, and Ania Trichet
- 349 Prepare Now for EDGAR Next**
Daniel Nussen, Jason Rocha, Danielle Herrick, and Guiying Ji
- 355 National Highway Traffic Safety Administration Announces First Actions Under Trump Administration's New Framework for Removing Regulatory Barriers for Automated Vehicles**
Rebecca Baden Chaney and Rachael Padgett
- 361 Ready to Know Your Data? Justice Department Issues Implementation and Enforcement Guidance for Data Security Program Protecting Bulk Sensitive Data**
Kate M. Growley, Caitlyn Weeks, Jacob Harrison, Nigel Cory, and Linda Malek
- 367 Environmental Protection Agency Ends Environmental Justice Considerations in Enforcement; Highlights Energy Production; Further Emphasizes Deregulatory Actions**
Samuel B. Boxerman, Byron F. Taylor, Timothy K. Webster, and Rose Quam-Wickham

- 373 Environmental Protection Agency's Deregulatory Initiative to "Power the Great American Comeback"**
Rich Gold, Susan G. Lafferty, Andy Emerson, Dimitrios J. Karakitsos, and Maggie P. Pahl
- 381 Securities and Exchange Commission's Division of Corporation Finance Issues No-Action Letter Response Regarding Issuer Verification Steps for Accredited Investor Status**
Joel I. Greenberg, Sara Adler, Meir Lax, and Peter G. Danias
- 385 Department of Defense Mandates Use of Software Acquisition Pathway for Software Development Procurements**
Tracye Winfrey Howard, Gary S. Ward, Scott A. Felder, Teresita Regelbrugge, and Vaibhavi Patria
- 391 Department of Health and Human Services Office of General Counsel Statement of Organization Suggests Potential Consolidation, Expansion of Authority**
Jaime L.M. Jones, Meenakshi Datta, Rebecca K. Wood, Raj D. Pai, Colleen Theresa Brown, and Michael Varrone
- 397 What the Foreign Corrupt Practices Act Criminal Enforcement Pause Means for Companies**
Kevin B. Muhlendorf, Vesna K. Harasic-Yaksic, Brandon J. Moss, and Corey J. Hauser

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Lynn E. Calkins

Partner, Holland & Knight LLP

Washington, D.C.

Helaine I. Fingold

Member, Epstein Becker & Green, P.C.

Baltimore

Nancy A. Fischer

Partner, Pillsbury Winthrop Shaw Pittman LLP

Washington, D.C.

Bethany J. Hills

Partner, DLA Piper LLP (US)

New York

Phil Lookadoo

Partner, Haynes and Boone, LLP

Washington, D.C.

Michelle A. Mantine

Partner, Reed Smith LLP

Pittsburgh

Ryan J. Strasser

Partner, Troutman Pepper Hamilton Sanders LLP

Richmond & Washington, D.C.

THE JOURNAL OF FEDERAL AGENCY ACTION (ISSN 2834-8818 (online)) at \$495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2025 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff

Publisher: Leanne Battle

Production Editor: Sharon D. Ray

Cover Art Design: Morgan Morrisette Wright and Sharon D. Ray

This journal's cover includes a photo of Washington D.C.'s Metro Center underground station. The Metro's distinctive coffered and vaulted ceilings were designed by Harry Weese in 1969. They are one of the United States' most iconic examples of the brutalist design style often associated with federal administrative buildings. The photographer is by XH_S on Unsplash, used with permission.

Cite this publication as:

The Journal of Federal Agency Action (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2025 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005

<https://www.fastcase.com/>

POSTMASTER: Send address changes to THE JOURNAL OF FEDERAL AGENCY ACTION, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and anyone interested in federal agency actions.

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.

QUESTIONS ABOUT THIS PUBLICATION?

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

Leanne Battle, Publisher, Full Court Press at leanne.battle@vlex.com or at
866.773.2782

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2834-8796 (print)
ISSN 2834-8818 (online)

Ready to Know Your Data? Justice Department Issues Implementation and Enforcement Guidance for Data Security Program Protecting Bulk Sensitive Data

Kate M. Growley, Caitlyn Weeks, Jacob Harrison, Nigel Cory, and Linda Malek*

In this article, the authors review implementation and enforcement guidance issued by the Department of Justice regarding its Data Security Program.

The U.S. Department of Justice (DOJ) has issued guidance regarding the implementation and enforcement of the newly enacted final rule, “Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons,”¹ now referred to as the Data Security Program (DSP). The release² included an Implementation and Enforcement Policy,³ a Compliance Guide,⁴ and Frequently Asked Questions (FAQs).⁵ Collectively, these documents are designed to help entities subject to the DSP understand and comply with the obligations set out under the Final Rule.

While much of the content reiterates information already established in the final rule, key insights from the newly released documents are summarized below.

What Is the DSP?

The DOJ created the DSP to establish rules for U.S. persons and entities engaging in certain data transactions that the U.S. government has determined pose an unacceptable risk of giving “countries of concern” or “covered persons” access to government-related data or bulk U.S. sensitive personal data. Among

other requirements, the DSP identifies classes of prohibited and restricted transactions, identifies countries of concern and classes of covered persons to whom the proposed rule applies, identifies classes of exempt transactions, and establishes processes to issue licenses authorizing certain prohibited or restricted transactions. Unofficially, many have equated it to an export control program for the relevant data.

Limited Enforcement Policy for First 90 Days

The DSP final rule took effect on April 8, 2025, with additional compliance requirements, including due diligence, auditing, and reporting, scheduled to become effective on October 6, 2025.

Under the Implementation and Enforcement Policy, the DOJ announced a phased approach to enforcement, offering a 90-day period—from April 8 to July 8, 2025—during which it will deprioritize civil enforcement actions for violations of the DSP, provided that entities are making “good faith efforts” to comply with the DSP during that period. DOJ provided examples of actions that may constitute good faith effort, including:

- Reviewing internal data sets and data types to determine if they are potentially subject to DSP;
- Renegotiating vendor agreements or negotiating contracts with new vendors, or transferring products and services to new vendors;
- Adjusting employee work locations, roles, or responsibilities;
- Evaluating investments from countries of concern or covered persons; and
- Implementing the Cybersecurity and Infrastructure Agency (CISA) Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

However, DOJ reserves the right to pursue enforcement action for “egregious, willful violations” even during the 90-day window, and states that it expects entities to be “in full compliance” with the DSP at the end of the 90 days.

“Know Your Data” Requirements

The FAQs and Compliance Guide explain that entities subject to the DSP must develop and implement “know your data” compliance programs to verify data transactions, including the nature and volume of data, how the data are used, and how the data are marketed. However, FAQ 80 clarifies that entities are not expected to decrypt or aggregate data in their possession to comply with the Rule’s “know your data” standard. This explanation is aligned with the DSP final rule’s explanation that cloud service providers will not be expected to “know” their customers’ encrypted data to comply with DSP.

Health Data

The DSP has significant implications for companies dealing with bulk sensitive personal health and human ‘omic data, necessitating a thorough understanding of the scope and definition of such data.

While the compliance documents largely reiterate the health data–relevant definitions set out in the DSP final rule, FAQ 31 clarifies the scope of personal health data, indicating that it is not solely limited to information collected by healthcare providers or institutions. Rather, it includes any data that meets the definition, regardless of who collects it or in what context. This broader definition is significant because it extends beyond the parameters set by the Health Insurance Portability and Accountability Act (HIPAA), which links health information to the type of entity managing it.

CISA Requirements

The FAQ and Compliance Guidance confirm that restricted transactions—that is, bulk data transactions that would otherwise be prohibited—can be authorized if CISA’s “Security Requirements for Restricted Transactions”⁶ are implemented to mitigate the risk of in-scope data access by countries of concern or covered persons. But FAQ 68 cautions that adherence to the CISA requirements alone does not provide blanket coverage, explaining that entities will need to take additional steps as required by the DSP for the

restricted transaction to proceed (e.g., maintain a due diligence program for restricted transactions).

DSP Versus PADFAA

FAQ 12 provides an overview of the distinction between the DSP and the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA), a law that makes it unlawful for data brokers to sell U.S. persons' sensitive data to foreign adversaries. Key differences identified in FAQ 12 include:

- PADFAA covers a broader array of data types than the DSP, including U.S. individual's photos, videos, and other private communications;
- PADFAA applies only to the activities of third-party "data brokers," while the DSP applies to all U.S. entities that engage in covered transactions; and
- While both PADFAA and the DSP restrict transactions involving China, Russia, North Korea, and Russia, the DSP also includes Venezuela and Cuba as countries of concern. Although not noted in the FAQ, DSP also expressly includes Hong Kong and Macau, while PADFAA is limited to just Mainland China.

Exemption for U.S. Government Official Business

FAQ 73 clarifies that the exemption for covered data transactions conducted pursuant to a grant, contract, or other agreement with U.S. federal government departments and agencies applies even if the transaction also involves some funding from non-federal entities. However, DOJ also notes that the exemption applies only if the relevant federal grant or contract directs or authorizes the covered data transaction.

No Cookie-Cutter Compliance Programs

The FAQs reiterate in several places that there is no one-size-fits-all compliance program for the DSP. Rather, each organization will need to assess its own risk profile, considering factors such as its

size, sophistication, offerings, third-party partners, and geographic footprint. That said, the Compliance Guide is intended to help organizations understand how to navigate those considerations. This is also consistent with the CISA requirements, which demands a risk assessment to determine appropriate mitigation measures to prevent access to covered data.

Conclusion

The DOJ's phased approach to enforcement will be much welcomed. Many organizations have been anxious that their active preparations for the DSP's effective date were uninformed by anticipated guidance that, up until last week, was unavailable. With that guidance in hand, those subject to the DSP should review the DSP Implementation and Enforcement Policy, a Compliance Guide, and FAQ in full, and use these documents as a reference in implementing their DSP compliance regimes. As part of that process, organizations should also document their "good faith efforts" to implement the DSP requirements so that they can take full advantage of the DOJ's 90-day soft enforcement period and mitigate the risk of alleged noncompliance.

Notes

* The authors, attorneys with Crowell & Moring LLP and policy advisors with the firm's subsidiary Crowell Global Advisors, may be contacted at kgrowley@crowell.com, cweeks@crowellglobaladvisors.com, jharrison@crowell.com, ncory@crowellglobaladvisors.com, and lmalek@crowell.com, respectively.

1. <https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern>.

2. <https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive>.

3. <https://www.justice.gov/opa/media/1396346/dl?inline>.

4. <https://www.justice.gov/opa/media/1396356/dl>.

5. <https://www.justice.gov/opa/media/1396351/dl>.

6. https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf.