ALERT MEMORANDUM

Enforcement Countdown: Is DOJ Ready for the Bulk Data Rule "Grace Period" to End?

July 7, 2025

As of July 8, the U.S. Department of Justice ("DOJ") is scheduled to begin full enforcement of its Data Security Program ("DSP") and the recently issued Bulk Data Rule after its 90-day limited enforcement policy expires, ushering in "full compliance" requirements for U.S. companies and individuals.[1] Although it remains to be seen whether DOJ's National Security Division ("NSD") will have the necessary infrastructure and personnel in place to launch comprehensive investigations to enforce such an expansive regulatory program, companies should be wary to wait to verify the NSD's operational readiness. Instead, companies should bear in mind certain considerations, discussed below, when approaching this new and uncertain enforcement frontier.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

WASHINGTON

Christopher R. Kavanaugh
+1 202 974 1867
ckavanaugh@cgsh.com

David A. Last
+1 202 974 1650
dlast@cgsh.com

Katie McGuire
+1 202 974 1551
kmcguire@cgsh.com

SILICON VALLEY

Matthew Yelovich
+1 650 815 4152
myelovich@cgsh.com

NEW YORK

Melissa Faragasso
+1 212 225 2115
mfaragasso@cgsh.com

[1] U.S. Dep't of Just., Nat'l Sec. Div., Data Security Program: Implementation and Enforcement Policy Through July 8, 2025 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396346/dl?inline [hereinafter Enforcement Policy].

The DSP is a brand new regulatory framework based on the Bulk Data Rule that imposes restrictions designed to prevent certain countries—China, Cuba, Iran, North Korea, Russia, and Venezuela—and covered persons from accessing Americans' bulk sensitive personal data and U.S. government-related data.[2] Violations of the Rule are subject to steep penalties. Pursuant to the DSP and the International Emergency Economic Powers Act ("IEEPA"), DOJ is authorized to bring not only civil enforcement actions, but also criminal prosecutions for willful violations of the DSP's requirements. Civil penalties may reach up to the greater of $368,136 or twice the value of each violative transaction, while willful violations are punishable by up to 20 years imprisonment and a $1,000,000 fine.[3]

Although the DSP largely went into effect on April 8, 2025, DOJ instituted a 90-day limited enforcement period. During this period, NSD stated it would deprioritize civil enforcement actions for companies and individuals making a "good-faith effort" to come into compliance with the DSP. This grace period comes to an end on July 8, 2025. As detailed below, this broad grant of investigative and enforcement authority—especially the potential for both civil and criminal liability—creates a number of potential logistical and legal challenges for DOJ.

Investigation and Enforcement Challenges

Enforcement of the DSP falls to the NSD, and more specifically to a small, specialized section named the Foreign Investment Review Section ("FIRS"). Historically, FIRS was comprised of approximately 10-20 attorneys, with a niche portfolio of responsibilities that included representing DOJ on the Committee on Foreign Investment in the United States and Team Telecom. With this portfolio, FIRS generally enjoyed a comparatively lower profile than other sections within the Department, leaving most federal prosecutors and criminal defense attorneys unfamiliar with its activities.

However, that all could change in the near future given that FIRS has been tasked with implementing and enforcing an entirely new regulatory and enforcement regime. Going forward, FIRS – a section traditionally without litigators or a litigating function – will have both civil and criminal authority to investigate, bring enforcement actions, and prosecute violations of the Rule.

Complications Associated with Adding Criminal Prosecutors to FIRS

The availability of criminal penalties under the DSP will require a number of changes at FIRS. Notably, unlike other NSD sections, the scope of FIRS's work did not previously include criminal prosecutions and instead maintained a regulatory focus.[4]

Given FIRS's lack of experience with criminal cases, FIRS must now decide how it will staff enforcement matters going forward, including whether to hire federal prosecutors directly or to instead coordinate with U.S. Attorneys' Offices or other sections of NSD in connection with criminal investigations and prosecutions. It seems likely that NSD would consider staffing up FIRS in anticipation of its dual criminal and civil enforcement authority under the DSP. But the introduction of criminal prosecutors into the same small section as civil regulators opens up potential risks in terms of parallel civil and criminal investigations:

1. Due Process Considerations: While DOJ often conducts parallel criminal and civil investigations, such coordination is subject to limitations imposed by the Due Process Clause of the Fifth Amendment.[5] In *United States v. Kordel*, the

[2] Our prior alert memorandum on the DSP is available here, and our alert on DOJ's 90-day limited enforcement policy of the DSP is available here.
[3] Enforcement Policy, at 1.
[4] U.S. Dep't of Just., Nat'l Sec. Div., NSD Organizational Chart (June 16, 2023), https://www.justice.gov/nsd/national-security-division-organization-chart

[5] *See, e.g.*, *United States v. Stringer*, 535 F.3d 929, 933 (9th Cir. 2008) ("There is nothing improper about the government undertaking simultaneous criminal and civil investigations.").

Supreme Court suggested that the Government may be found to have acted in bad faith in violation of the Fifth Amendment by bringing "a civil action solely to obtain evidence for its criminal prosecution" or by "fail[ing] to advise the defendant in its civil proceedings that it contemplates his criminal prosecution."[6] Lower courts have "occasionally suppressed evidence or dismissed indictments on due process grounds where the government made affirmative misrepresentations or conducted a civil investigation solely for purposes of advancing a criminal case."[7] In order to avoid such consequences, FIRS will have to ensure that any cooperation or coordination in parallel civil and criminal investigations of DSP violations complies with Due Process requirements.

2. DOJ Internal Policy Limitations: In addition to Due Process requirements, internal DOJ guidance places guardrails around parallel or joint civil and criminal investigations. Section 1-12.00 of the Justice Manual notes that "when conducted properly," parallel investigations can "serve the best interests of law enforcement and the public."[8] However, the same section goes on to warn DOJ attorneys that "parallel proceedings must be handled carefully in order to avoid allegations of . . . abuse of civil process."[9] Section 1-12.100 addresses parallel or joint corporate investigations and similarly emphasizes that DOJ attorneys "should remain mindful of their ethical obligations not to use criminal enforcement authority unfairly to extract, or to attempt to extract, additional civil or administrative monetary payments."[10]

3. Maintaining the Secrecy of Rule 6(e) Grand Jury Materials: Finally, FIRS will need to implement precautions to ensure that its civil enforcement attorneys are walled off from the disclosure of materials covered by Federal Rule of Criminal Procedure 6(e). Rule 6(e) establishes a general rule of secrecy for grand jury materials with limited exceptions. Although Rule 6(e)(3)(A)(i) permits disclosure "to an attorney for the government for use in the performance of such attorney's duty," civil enforcement attorneys within FIRS could only view Rule 6(e) materials if they obtain a court order.[11] Moreover, pursuant to DOJ guidance, even when disclosure is authorized for use in civil proceedings, it is considered a "better practice to forestall the disclosure until the criminal investigation is complete," given the potential "danger of misuse, or the appearance thereof."[12] Given that none of the exceptions under Rule 6(e) appear readily applicable, criminal attorneys within FIRS will have to take particular precautions to ensure that grand jury material covered under Rule 6(e) is not disclosed to their civil colleagues.

[6] *See United States v. Kordel*, 397 U.S. 1, 11 (1970) (holding that the Government did not violate due process when it used evidence from a routine FDA civil investigation to convict defendants of criminal misbranding given that the agency made similar requests for information in 75% of civil cases and there was no suggestion the Government brought the civil case solely to obtain evidence for the criminal prosecution).
[7] *Stringer*, 535 F.3d at 940 (collecting cases).
[8] Justice Manual 1-12.00 – Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings (May 2018), https://www.justice.gov/jm/jm-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings
[9] *Id.*
[10] Justice Manual 1-12.100 – Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018), https://www.justice.gov/jm/jm-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings
[11] *See United States v. Sells Eng'g, Inc.*, 463 U.S. 418, 427 (1983) (rejecting the argument that all attorneys within the DOJ's civil division are covered under (A)(i), and instead holding that "(A)(i) disclosure is limited to use by those attorneys who conduct the criminal matters to which the materials pertain").
[12] U.S. Dep't of Just., Crim. Resource Manual, 156. Disclosure of Matters Occurring Before the Grand Jury to Department of Justice Attorneys and Assistant United States Attorneys (Oct. 2012), https://www.justice.gov/archives/jm/criminal-resource-manual-156-disclosure-matters-occurring-grand-jury-department-justice-attys

Following July 8, as we wait to see whether FIRS initiates investigations and enforcement actions under the DSP, it will need to address the above limitations and potential pitfalls that come with parallel civil and criminal proceedings. This will be especially important given the relatively small size of FIRS, its historic regulatory focus, and the addition of criminal prosecutors and criminal enforcement authority as it tries to administer an entirely new regulatory and enforcement regime.

Limited Investigative Resources

In addition to potential concerns associated with criminal enforcement of the DSP, there is also uncertainty about how FIRS will investigate potential violations. Unlike traditional sanctions and export control enforcement, which relies on the Department of Treasury's Office of Foreign Assets Control and the Department of Commerce's Bureau of Industry and Security, respectively, it is unclear what, if any, dedicated investigative resources or interagency cooperation FIRS will have at its disposal. While federal prosecutors typically investigate alongside agents from the Federal Bureau of Investigation and Homeland Security Investigations, such investigative resources historically were not allocated to FIRS, and it is unclear which federal investigating agency – if any – has been tasked with leading these investigations. This raises questions about FIRS's capacity to effectively investigate and bring enforcement actions for potential violations.

One option that could be considered is to have FIRS limit its role to civil enforcement and – to the extent it comes across potential criminal conduct – make criminal referrals to either (i) the appropriate United States Attorney's Office, all of which have federal prosecutors who have been trained in national security investigations and have routine access to a grand jury, or (ii) NSD's Counterintelligence and Export Control Section, which currently includes federal prosecutors that specialize in investigating criminal violations of sanctions and export control laws.

Alternatively, the Federal Trade Commission ("FTC") could also provide investigative support regarding potential violations under the DSP given its enforcement authority under a related law: the Protecting Americans' Data from Foreign Adversaries Act ("PADFA"). The FTC has enforcement authority under PADFA to seek civil penalties but is first required to refer the matter to the DOJ.[13] Given the potential overlap between the DSP and PADFA, the FTC may be particularly well-situated to investigate and refer cases of DSP violations to FIRS.

Seventh Amendment Implications: The *Jarkesy* Challenge

As noted above, the DOJ has broad authority to pursue both civil penalties and prosecute criminal offenses for non-compliance with the Bulk Data Rule under the DSP, but just *how* the DOJ plans to pursue civil penalties for violations is also unclear. Specifically, to the extent the DOJ seeks to impose penalties in a way that implicates administrative proceedings, it is likely to face challenges following the Supreme Court's decision in *SEC v. Jarkesy*.[14] In *Jarkesy*, the Supreme Court held that the Seventh Amendment entitles a defendant to a jury trial when the SEC seeks civil penalties for securities fraud,[15] thereby limiting the SEC's ability to adjudicate cases for civil penalties through its administrative proceedings.

Jarkesy's reasoning regarding the Seventh Amendment's application to actions seeking civil penalties could impact the DSP's enforcement framework.[16] Similar to the civil penalties at issue in *Jarkesy*, civil penalties imposed under the DSP and IEEPA serve to punish violations and deter future

[13] A violation of PADFA is treated as a violation of an FTC rule pursuant to 15 U.S.C. § 57a(a)(1)(B).
[14] 603 U.S. 109 (2024).
[15] *Id.* at 140.
[16] The Court in *Jarkesy* also established a two-part test for determining whether a cause of action implicates the Seventh Amendment. First, courts must determine whether the cause of action is "legal in nature" and whether the remedy sought is traditionally obtained in courts of law. *Id.* at 121–27. If legal in nature, courts must then assess whether the "public rights" exception permits congressional assignment of adjudication to an agency. *Id.* at 127–34.

misconduct, as opposed to compensate victims.[17] However, unlike antifraud provisions, the DSP arguably lacks clear common law analogies, and it is possible that the DSP and IEEPA could be viewed under the "public rights" exception given the links to national security.[18]

Going forward, *Jarkesy* is expected to affect how other federal agencies conduct enforcement actions seeking civil penalties. The DOJ will have to consider these implications as it decides on an enforcement framework for imposing civil penalties for DSP violations.

Conclusion

The DSP represents the U.S.'s first data localization requirement ripe for enforcement, but its implementation faces substantial practical challenges that may hinder DOJ's ability for wide-ranging or swift action. As companies work to ensure their activities are in compliance with the DSP and the Bulk Data Rule ahead of July 8, many are left wondering whether the DOJ will be ready to begin investigating and enforcing this Rule given its breadth and the clear potential challenges that lie ahead. While we await DOJ's next steps toward enforcement, companies should be prepared to document their good-faith efforts to demonstrate compliance with the DSP and the Rule to prevent early investigations and enforcement actions. Additionally, as emphasized by the DOJ's non-binding Compliance Guidance,[19] companies that proactively implement compliance programs will be better positioned to respond and adapt to this uncertain enforcement environment.

…

CLEARY GOTTLIEB

[17] *Id.* at 121–27.
[18] *Id.* at 135.
[19] U.S. Dep't of Just., Nat'l Sec. Div., Data Security Program: Compliance Guide (Apr. 11, 2025), https://www.justice.gov/opa/media/1396356/dl