Adam Avivi

Professor Christopher J. Borgen

Directed Research

September 9, 2026

Emergency Powers and Ordinary Data: Statutory Reach, Judicial Review, and Compliance Standards in the Department of Justice Data Security Program

I. Introduction

A data broker assembles precise geolocation data harvested from smartphone applications. Among its holdings are movement traces that map, hour by hour, the commutes and errands of people who live and work around a United States military installation. For years the broker sold that data to anyone who paid, and the sale was lawful. Since April 8, 2025, the same sale to a covered person is a federal offense, exposing the broker to civil penalties and, where the violation is willful, to criminal prosecution.[1]

The data are unchanged. What changed is that the President, exercising emergency economic powers, determined that transactions of this kind give foreign adversaries access to the raw material of espionage, and directed the Department of Justice to build a regulatory program to stop them.

The regulatory premise is that foreign adversaries obtain data through lawful commerce rather than through theft. Countries of concern and covered persons, foreign entities, employees, contractors, or residents tied to specific "countries of concern" (such as China, Russia, Iran, North Korea, Cuba, and Venezuela), acquire Americans' sensitive personal data and United States Government-related data through commercial channels. The President determined that this acquisition threatens national security, and the DOJ then issued the rule implementing that determination.[2] Said commercial channels include sales by data

---

1 See 28 C.F.R. §§ 202.205, 202.206, 202.211, 202.222(a)(1), 202.242, 202.301 (2025); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1636 (Jan. 8, 2025); 50 U.S.C. § 1705. The scenario in text is illustrative only and does not describe any identified enforcement matter.

2 Exec. Order No. 14,117, 89 Fed. Reg. 15,421, 15,421 (Mar. 1, 2024) (presidential threat finding); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1646 (Jan. 8, 2025) (explaining DOJ's view that covered data transactions may

brokers, vendor relationships requiring processing access, employment arrangements, and investments in the entities that hold the data.

In 2024, President Biden addressed that problem under the International Emergency Economic Powers Act (IEEPA), which authorizes the President, upon declaring a national emergency to address an unusual and extraordinary threat originating outside the United States, to regulate a broad range of dealings in property in which a foreign country or national holds an interest.[3] Executive Order 14117 invoked IEEPA's authority and directed the Attorney General to prohibit or restrict U.S. persons from engaging in specified data transactions.[4] The implementing regulation focuses on access: a covered data transaction is one giving a country of concern or covered person access to government-related data or bulk U.S. sensitive personal data through data brokerage, vendor, employment, or investment agreements.[5]

The DOJ implemented this Order in a final rule published January 8, 2025. The final rule does not itself specify the security measures a regulated party must take. Instead, it incorporates by reference a set of security requirements that the Cybersecurity and Infrastructure Security Agency (CISA), a federal agency within the Department of Homeland Security, developed through its own notice-and-comment process and published separately. The compliance standard is CISA's text, which is made binding by the DOJ's rule.[6] The rule prohibits covered data-brokerage transactions with countries of concern or covered persons, as well as specified transactions involving bulk human genomic data or biospecimens. Other covered vendor, employment, and investment transactions may proceed only if they satisfy the incorporated CISA security requirements and the rule's other applicable requirements.[7] Those requirements state the compliance obligation for restricted transactions. A U.S. person engaging in such a transaction must adopt a combination of mitigations sufficient to

fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons or countries of concern.[8]

---

enable access by countries of concern or covered persons to covered data to harm U.S. national security).

3 50 U.S.C. §§ 1701(a), 1702(a)(1)(B).

4 50 U.S.C. § 1702(a)(1)(B) (2018); Exec. Order No. 14,117 § 2(a), 89 Fed. Reg. at 15,423.

5 28 C.F.R. § 202.210(a) (2025); Exec. Order No. 14,117 § 2(c)(ii), 89 Fed. Reg. 15,421, 15,424 (Mar. 1, 2024).

6 28 C.F.R. § 202.248 (2025); Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1528–29 (Jan. 8, 2025).

7 28 C.F.R. §§ 202.301, 202.303, 202.248, 202.401(a) (2025); Cybersecurity & Infrastructure Sec. Agency, Security Requirements for Restricted Transactions, E.O. 14117 Implementation §§ I–II (Jan. 2025) [hereinafter CISA Security Requirements].

8 CISA Security Requirements, supra note 7, § II.

CISA has explained that a restricted transaction may proceed either by denying covered persons access to the covered data or by applying pseudonymization, de-identification, aggregation, and encryption alongside organizational and system-level controls.[9] The rule also addresses onward transfers in data-brokerage transactions with foreign persons who are not covered persons. It requires the U.S. person to obtain a contractual commitment against subsequent covered data brokerage of the same data to a country of concern or covered person, and to report known or suspected violations of that commitment.[10]

This paper explores three potential questions raised by this program.

The first question concerns statutory reach. While IEEPA's grant of authority is generally broad, Congress has limited it in the context of information. The Berman Amendment, enacted in 1988 as an amendment to IEEPA and named for its sponsor, Representative Howard Berman, withdrew IEEPA authority to regulate protected imports and exports of information or informational materials, subject to the statutory exclusions. As subsequently amended, it provides that the authority granted "does not include the authority to regulate or prohibit, directly or indirectly," the importation or exportation of "any information or informational materials."[11] Whether non-expressive bulk commercial data falls within that protection is a question of statutory interpretation, and the national-security character of the rule does not supply the answer. By non-expressive data, this paper means compilations of personal information such as geolocation traces, genomic sequences, or financial records, which carry no communicative message and are valued for what can be inferred from them rather than for anything they express. This is addressed in Part II.

The second question concerns judicial review. The DOJ conducted notice-and-comment rulemaking while asserting that the APA's foreign-affairs exception relieved it of any obligation to do so, and the rule rests in part on a classified record.[12] Whether an exemption from rulemaking procedure also limits review of the resulting rule, and whether classified evidence can supply the content of a public standard, are distinct questions governed by different provisions of the Administrative Procedure Act (APA).[13] This is addressed in Part III.

---

9 Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1532 (Jan. 8, 2025).

10 28 C.F.R. § 202.302(a)–(b) (2025).

11 50 U.S.C. § 1702(b)(3).

12 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1637, 1639 n.25 (Jan. 8, 2025).

13 5 U.S.C. §§ 553(a)(1), 706; 50 U.S.C. § 1702(c); see infra Parts III.A–B, IV.B.3.

The third question concerns the content of the compliance obligation. The restricted-transaction pathway turns on the incorporated CISA standard, which imposes organizational controls, covered-system controls, data-level mitigations, and an internal data-risk assessment.[14] Cybersecurity regulation proceeds by general standards because systems, counterparties, technologies, and adversary methods vary, and flexibility is necessary for the standard to remain workable as those conditions change. A party subject to civil and criminal liability must nonetheless be able to determine in advance what the standard requires. It is not clear whether the DOJ rule or the CISA standard is adequately specific for this purpose.[15] This is addressed in Part IV.

II. Does IEEPA Authorize the DOJ Rule Concerning Non-Expressive Bulk Data?

A. What Does the Statutory Text Cover?

Section 1702(a)(1)(B) of IEEPA authorizes the President to regulate, block, compel, nullify, void, prevent, or prohibit dealings in property in which a foreign country or national has an interest. As noted above, Executive Order 14117 delegates implementation of the bulk-data restrictions to the Attorney General.[16] The President's authority operates only "at the times and to the extent specified in section 1701," against a declared emergency.[17] Section 1702(b) then limits the authority given to the President, providing that "[t]he authority granted to the President by this section does not include" the power to regulate the import or export of protected information or informational materials. Executive Order 14117 acknowledges the limit by defining sensitive personal data only "to the extent consistent with" that provision.[18] The contested question is whether non-expressive bulk commercial data falls within the withdrawn category. Such data consists of compilations of personal information — geolocation traces, genomic sequences, biometric identifiers, health and financial records — collected at scale and valued for what an analyst can infer from it. It conveys no message and reaches no audience, which distinguishes it from the publications, films, and recordings the statute lists as examples.

Section 1702(b)(3) removes from IEEPA the power to regulate or prohibit

---

14 28 C.F.R. §§ 202.248, 202.401(a) (2025); Cybersecurity & Infrastructure Sec. Agency, *Security Requirements for Restricted Transactions Pursuant to Executive Order 14117* 1–6 (Jan. 2025).

15 CISA Security Requirements, supra note 7, § II; 50 U.S.C. § 1705.

16 50 U.S.C. § 1702(a)(1)(B) (2018) (authorizing the President to "investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit" covered dealings in property); Exec. Order No. 14,117 § 2(a), 89 Fed. Reg. 15,421, 15,423 (Mar. 1, 2024) (directing the Attorney General to issue regulations prohibiting or restricting covered data transactions).

17 50 U.S.C. §§ 1701(a), 1702(a)(1).

18 50 U.S.C. § 1702(b), (b)(3) (2018); Exec. Order No. 14,117 § 7(l), 89 Fed. Reg. at 15,429.

directly or indirectly, the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.[19]

Three phrases resist a narrow construction. “Any” is expansive; “whether commercial or otherwise” forecloses a commercial-noncommercial distinction; and “regardless of format or medium of transmission” prevents confining the carve-out to familiar carriers.[20] The nonexclusive examples reach electronic media, including tapes, compact disks, and CD ROMs, and the text nowhere says “expressive.”[21] Under ordinary canons of statutory construction, courts presume that Congress does not use surplus words: each term in a statute is given effect, and a reading that renders one term redundant of another is disfavored. Section 1702(b)(3) protects “information” and “informational materials.” If “informational materials” already captured everything Congress meant to protect, “information” would do no work. That presumption supports reading “information” more expansively than the expressive works the examples describe, and a database is in ordinary usage a collection of information. The cases discussed below do not resolve that argument as applied to raw bulk personal data. DOJ responds that “information” refers to expressive content and “informational materials” to the media containing it, giving the terms distinct roles without extending the exemption to non-expressive data.[22]

Section 1702(b)(3) withholds the authority to regulate protected information “directly or indirectly.” In plain terms, the President may not prohibit the movement of such information, and he also may not achieve the same result by regulating something adjacent to it. A rule that leaves the information formally untouched while shutting down the arrangements through which it travels is still an indirect regulation of that information. If the regulated object is protected information, the Berman Amendment is not avoided by regulating hosting, distribution, or the business relationships that suppress a cross-border

---

19 50 U.S.C. § 1702(b), (b)(3) (2018).

20 Id. § 1702(b)(3); Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525(c)(1), 108 Stat. 382, 474–75 (1994).

21 50 U.S.C. § 1702(b)(3); Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525(c)(1), 108 Stat. 382, 474–75 (1994).

22 50 U.S.C. § 1702(b)(3). The distinction drawn here between information and informational materials is an interpretive inference from the statutory text, not a holding of the cited platform cases. For DOJ’s response, see Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1673–74 n.146 (Jan. 8, 2025).

flow.[23] Courts have read the clause that way, as Part II.C explains, though the line between an indirect regulation and a merely tangential effect has not been drawn precisely.[24]

B. Did the 1988 and 1994 Amendments Change IEEPA's Reach to This Kind of Data?

Congress has legislated twice on this exception. The first enactment is the Berman Amendment of 1988, codified at § 1702(b)(3). The second is section 525 of the Foreign Relations Authorization Act of 1994, titled the Free Trade in Ideas Act, which struck the 1988 paragraph and replaced it with the text now in force.

Congress enacted the Berman Amendment in 1988 in response to a specific practice. The Treasury Department's Office of Foreign Assets Control, which administers sanctions programs, had used its authority under the Trading with the Enemy Act and IEEPA to seize books and magazines at the border as they entered the United States from embargoed countries.[25] Congress concluded that using economic-sanctions authority to interdict publications interfered with the free exchange of ideas, and it withdrew that authority.[26] The amendment provides that the President's power "does not include the authority to regulate or prohibit, directly or indirectly," the importation or exportation of "publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, or other informational materials."[27] The withdrawal limited the subject matter the President could reach under IEEPA, while retaining specified export-control and espionage-law exclusions. But the enumerated examples were all media of communication—things people read, watch, and hear—and the amendment said nothing about compilations of data about individuals.[28]

Congress broadened the exemption in 1994 after OFAC construed it narrowly. OFAC had taken the position that the amendment reached only informational materials "fully created and in existence" at the time of a transaction, excluding, for example, the editing or translation of a work in progress, and courts had divided over OFAC's restrictive construction of the exemption.[29] The Free Trade in Ideas Act retained the existing phrase "whether commercial or otherwise," added "regardless of format or medium of

---

23 50 U.S.C. § 1702(b)(3); TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 83 (D.D.C. 2020); Marland v. Trump, 498 F. Supp. 3d 624, 643–45 (E.D. Pa. 2020).

24 TikTok, 490 F. Supp. 3d at 83; Marland, 498 F. Supp. 3d at 643–45.

25 See Tracy J. Chin, Note, An Unfree Trade in Ideas: How OFAC's Regulations Restrain First Amendment Rights, 83 N.Y.U. L. Rev. 1883, 1891 (2008); Cong. Rsch. Serv., R45618, The International Emergency Economic Powers Act: Origins, Evolution, and Use 12 (Jan. 30, 2024) [hereinafter CRS, IEEPA].

26 Chin, supra note 25, at 1891; CRS, IEEPA, supra note 25, at 12.

27 Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 2502(b)(1), 102 Stat. 1107, 1371–72 (codified as amended at 50 U.S.C. § 1702(b)(3)).

28 Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 2502(b)(1), 102 Stat. 1107, 1371–72.

transmission," expressly protected "any information or informational materials," and expanded the examples to include compact disks, CD-ROMs, artworks, and news wire feeds.[30] The existing commercial-neutrality language and the new format-neutrality language both bear on the Data Security Program. The commercial-or-otherwise language means the exemption does not turn on whether an exchange is for profit, which is significant because the program reaches commercial data transactions. The format-neutrality language means the exemption does not turn on the physical medium, which is significant because bulk data moves electronically and in formats that did not exist in 1994. The program cannot be brought outside the exemption merely because the data is sold for value or travels as a database export rather than on tapes and compact disks.[31]

What neither amendment did was speak to subject matter beyond communication. Congress titled the 1994 provision "FREE TRADE IN IDEAS," and the accompanying sense-of-Congress provision urged that the President not restrict "travel or exchanges for informational, educational, religious, cultural, or humanitarian purposes."[32] Those are categories of expression and exchange. The examples added in 1994, artworks and news wire feeds, are communicative works, as the 1988 examples were.

Both amendments contracted IEEPA's authority, and the 1994 amendment did so in ways that may bear on regulation of bulk data transfers. But the contraction operated on the form of protected information and on the character of the exchange, not on the kind of thing that counts as information in the first place. Whether something non-expressive, such as a compilation of geolocation traces or genomic sequences is information within the meaning of § 1702(b)(3) is a question the 1988 Congress did not address and the 1994 Congress did not revisit.

C. Does the Case Law Resolve Whether the Exemption Reaches Bulk Data?

Two district courts enjoined the 2020 TikTok restrictions on Berman Amendment grounds.[33] In *TikTok Inc. v. Trump*, the District Court for the District of Columbia held that user content constituted information and informational materials, emphasized that users shared films, photographs, art, and news across borders, and rejected the argument that

---

29 See United States v. Amirnazmi, 645 F.3d 564, 584–87 (3d Cir. 2011) (recounting OFAC's restrictive construction of the exemption and judicial disagreement involving artwork and intangible broadcasts).

30 Compare Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 2502(b)(1), 102 Stat. 1107, 1371–72, with Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525(c)(1), 108 Stat. 382, 474–75 (1994).

31 50 U.S.C. § 1702(b)(3).

32 Pub. L. No. 103-236, § 525(a), 108 Stat. at 474; 50 U.S.C. § 1702(b)(3) (2018).

33 TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 83 (D.D.C. 2020); TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 112 (D.D.C. 2020); Marland v. Trump, 498 F. Supp. 3d 624, 643–45 (E.D. Pa. 2020).

the prohibitions merely regulated business-to-business transactions.[34] *Marland* described TikTok's short videos as "expressive and informative" and held the Commerce Identification an indirect regulation of protected materials.[35] Those decisions show that a national-security rationale does not by itself avoid the carve-out and that the carve-out also restricts indirect regulation of protected informational materials.[36]

However, these cases do not resolve the question of bulk data. Each case involved user videos, expressive platform access, and social-media communication rather than raw datasets sold for analytics or profiling, and *TikTok* was as equally a speech case and a data-security case: the challenged measures burdened a platform millions used to exchange expressive content.[37]

A further question is whether the exception protects information that does not yet exist when the transaction occurs. Many covered arrangements are not one-time sales of a finished dataset. They are continuing relationships in which a foreign vendor processes data as it is generated, or in which a covered person receives standing access to a database that is updated over time. Courts have addressed the analogous problem in a sanctions context.

The principal decision is *United States v. Amirnazmi*. Amirnazmi, a chemical engineer, was prosecuted under the Iranian Transactions Regulations for dealings with Iranian entities that included providing ChemPlan, proprietary software and an associated database he had developed for modeling chemical plant operations. He argued that ChemPlan was information protected by § 1702(b)(3).[38] The Third Circuit disagreed, accepting OFAC's position that the exception reaches only informational materials fully created and in existence at the time of the transaction. Because the arrangement involved ongoing development and technical services rather than the transfer of a finished product, it fell outside the exception.[39]

A finished dataset avoids the objection that the materials did not exist when the transaction was made, but that does not establish that raw personal data falls within the statutory

---

34 TikTok, 490 F. Supp. 3d at 83.

35 Marland, 498 F. Supp. 3d at 643–45.

36 Marland, 498 F. Supp. 3d at 643–45; 50 U.S.C. § 1702(b)(3).

37 TikTok, 490 F. Supp. 3d at 83; Marland, 498 F. Supp. 3d at 643–45; see also TikTok Inc. v. Garland, 604 U.S. 56 (2025) (addressing the First Amendment challenge to a separate divestiture statute).

38 United States v. Amirnazmi, 645 F.3d 564 (3d Cir. 2011); see also Marland, 498 F. Supp. 3d at 643–45.

39 Amirnazmi, 645 F.3d at 584–87.

exception. Continuous feeds and enrichment services may face an additional obstacle under *Amirnazmi*'s treatment of ongoing development and services.[40]

D. How Do the Agencies Read the Carve-Out?

The Executive Order 13873, which established the national emergency that Executive Order 14117 is based on, also allowed the Commerce Department's Bureau of Industry and Security (BIS) to issue a rule restricting certain connected vehicles and related hardware and software linked to China or Russia.[41] BIS expressly stated its reading of the Berman Amendment. In that rule, the BIS interpreted "information or informational materials" to be "limited to expressive material," grounding that reading in "the statute's text and purpose, as demonstrated by legislative history and context as well as judicial interpretations," and identifying the provision's purpose as protecting "materials involving the free exchange of ideas." BIS cited *Amirnazmi* in explaining the balance between informational exchange and restricting support to adversaries, although that decision did not itself decide whether raw bulk personal data is protected. DOJ's own definition likewise expressly excludes technical, functional, and otherwise non-expressive data.[42] The BIS did not rely on the First Amendment, at least not directly. A broader reading, the BIS added, "would enable adversaries and countries of concern to use non-expressive data to undermine our national security," and the BIS characterized its rule as regulating hardware and software "based on functional capabilities" rather than restricting "expressive speech and communicative works," contrasting expressive materials with functional vehicle data such as geolocation and systems diagnostics.[43]

The CISA security requirements rest on the same premise, describing controls that "fully and effectively prevent[] access" to covered data, though CISA does not interpret § 1702(b)(3) here.[44] CISA's framing shows why the government treats this program as different from *TikTok* and *Marland*. The rule is not aimed at suppressing a communicative platform or preventing speakers from exchanging videos, photographs, or news. Rather, the rule is aimed at preventing covered persons from obtaining access to bulk sensitive personal data through commercial transactions.[45]

---

40 Cf. Amirnazmi, 645 F.3d at 584–87; 28 C.F.R. § 202.226(a)–(c) (2025).

41 Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360, 5360–61, 5372–73 (Jan. 16, 2025).

42 Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360, 5372–73 (Jan. 16, 2025); 28 C.F.R. § 202.226(a) (2025).

43 90 Fed. Reg. at 5372–73.

44 CISA Security Requirements, supra note 7, § II.

45 Exec. Order No. 14,117 § 2(a), 89 Fed. Reg. 15,421, 15,423 (Mar. 1, 2024); CISA Security Requirements, supra note 7, §§ I–II.

Statutory coverage cannot turn on how an agency characterizes the risk it regulates. If bulk datasets are information within § 1702(b)(3), the phrase "directly or indirectly" does not permit the agencies to avoid the exception by characterizing the rule as an access restriction.[46] After *Loper Bright*, a court determines the provision's meaning using its own judgment; the expressive-materials reading may persuade on its merits, but the scope of a statutory limit on executive power is for the court to interpret.[47]

E. Conclusion

The question is unsettled. "Any information or informational materials," "whether commercial or otherwise," "regardless of format or medium of transmission," and "directly or indirectly" are expansive phrases; Congress broadened rather than narrowed the provision in 1994; the platform decisions confirm that the carve-out constrains the Executive; and *Loper Bright* requires the court to independently determine the statutory meaning of the informational-materials exception, without eliminating deference to otherwise reviewable technical or factual judgments.[48]

The narrower reading of the Berman Amendment is nonetheless stronger as applied to the data this program regulates, for three reasons. First, legislative context centers on the free trade in ideas, and Congress described the exchanges it meant to protect in informational, educational, religious, cultural, and humanitarian terms. Second, the statutory examples are overwhelmingly communicative works, and the data carriers among them appear within a list of media through which speakers reach audiences. Third, the decisions discussed here applying the Berman Amendment have involved expressive materials, communicative platforms, or customized information services rather than a raw commercial database.[49] *Amirnazmi* confirms that the exemption is not categorical, though its deference reasoning must be read in light of *Loper Bright*, which does not automatically displace earlier statutory holdings protected by ordinary stare decisis. Also the BIS's interpretation, while not controlling and also expressly adopted by the DOJ, supplies a coherent line between expressive materials and functional data.[50]

---

46 TikTok, 490 F. Supp. 3d at 83; Marland, 498 F. Supp. 3d at 643–45.

47 Loper Bright Enters. v. Raimondo, 603 U.S. 369, 394–96, 412–13 (2024).

48 50 U.S.C. § 1702(b)(3); Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525(c)(1), 108 Stat. 382, 474–75 (1994); TikTok, 490 F. Supp. 3d at 83; Marland, 498 F. Supp. 3d at 643–45; Loper Bright Enters. v. Raimondo, 603 U.S. 369, 391–92, 412–13 (2024).

49 Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525(a), 108 Stat. 382, 474 (1994); TikTok, 490 F. Supp. 3d at 83; Marland, 498 F. Supp. 3d at 643–45; Amirnazmi, 645 F.3d at 584–87.

50 Amirnazmi, 645 F.3d at 584–87; Loper Bright Enters. v. Raimondo, 603 U.S. 369, 402, 412 (2024); 28 C.F.R. § 202.226(a) (2025); 90 Fed. Reg. at 5372–73.

That conclusion does not extend to every transaction the rule reaches. A single sale of a finished dataset is the transaction most likely to fall within the exception, because the data exists in full at the time of transfer. That feature avoids the additional obstacle considered in *Amirnazmi*, but does not establish that raw personal data is protected subject matter. A standing access arrangement, or a platform on which a covered person queries and enriches covered data over time, is further from the exception on that reasoning. The decisions discussed here do not resolve whether raw bulk commercial datasets fall outside § 1702(b)(3). Transaction structure may affect the separate question whether the materials are fully created at the time of the agreement.[51] Subject to that qualification, the program's regulation of non-expressive bulk sensitive personal data likely remains within IEEPA's reach.[52]

III. Procedural Exemptions and the Question of Judicial Review

Two features of the program might limit how a court would review it. The DOJ asserts that the APA's foreign-affairs exception relieved it of notice-and-comment obligations, and the rule rests in part on a classified record. Each is addressed below, followed by the standard of review governing the questions the rule presents. Neither feature removes the rule from judicial review. Both bear on how searchingly a court examines particular questions rather than on whether it may examine them.

This Part concerns the decision-making process and what a court may examine about it. Part IV concerns the substance of what that process produced: whether the standard the agencies adopted is adequately explained.

A. Does the Foreign-Affairs Exception Limit Review?

Section 553 of the APA requires an agency issuing a legislative rule to publish notice, provide an opportunity to comment, and include a concise general statement of basis and purpose.[53] Section 553(a)(1) exempts from those requirements any matter involving "a military or foreign affairs function of the United States."[54] DOJ stated that the rulemaking pertains to a foreign-affairs function and asserted an exemption from the APA's notice-and-comment requirements. It nevertheless conducted notice and comment, as Executive Order 14117 itself directed.[55]

---

51 50 U.S.C. § 1702(b)(3); cf. Amirnazmi, 645 F.3d at 584–87; 28 C.F.R. § 202.226(a)–(c) (2025).

52 50 U.S.C. § 1702(b)(3); 28 C.F.R. § 202.226(a)–(c) (2025); Amirnazmi, 645 F.3d at 584–87; TikTok, 490 F. Supp. 3d at 83; Marland, 498 F. Supp. 3d at 643–45; Loper Bright Enters. v. Raimondo, 603 U.S. 369, 412–13 (2024).

53 5 U.S.C. § 553(b)–(c); Administrative Procedure Act, Pub. L. No. 79-404, ch. 324, § 4, 60 Stat. 237, 238–39 (1946); H.R. Rep. No. 79-1980, at 24–25 (1946).

54 5 U.S.C. § 553(a)(1).

The exemption's scope is contested. The House Report accompanying the APA states that the exceptions apply "only 'to the extent' that the excepted subject matter is clearly and directly involved," and that "foreign affairs functions" is "not to be loosely interpreted" to cover an agency operation merely because it occurs abroad.[56] In *City of New York v. Permanent Mission of India to the United Nations*, New York City sought to tax portions of foreign mission properties used as residences. The State Department issued a notice exempting those properties, without notice and comment, and the Second Circuit held the exception applicable; regulation of foreign missions is the diplomatic setting that the exception addresses, and the court declined to require a case-specific showing of international consequences.[57] However, the Ninth Circuit took a narrower approach in an immigration case. In *East Bay Sanctuary Covenant v. Trump*, the government issued a rule barring asylum for aliens entering outside a port of entry and invoked the foreign affairs exception on the ground that the rule related to ongoing negotiations with Mexico. The court held the showing insufficient, requiring the government to demonstrate that public procedure would produce "definitely undesirable international consequences." The Court of International Trade applied similar reasoning in the Section 301 tariff litigation, rejecting the exception for trade rules merely because they related to ongoing negotiations.[58] In March 2025, the Secretary of State determined that all federal control of cross-border transfers of goods, services, data, and technology constitutes a foreign-affairs function.[59] The Data Security Program regulates commercial transactions among American companies and their vendors, employees, and investors, which seems to place it nearer to the trade and immigration rules that courts have scrutinized rather than the foreign-missions setting.

Section 553 governs how a rule is made; section 706 governs judicial review of final agency action.[60] The APA separated the two in its original enactment, and an exemption from the

---

55 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1639 n.25, 1640 (Jan. 8, 2025); Exec. Order No. 14,117 § 2(a), 89 Fed. Reg. 15,421, 15,423 (Mar. 1, 2024).

56 H.R. Rep. No. 79-1980, at 23 (1946); City of New York v. Permanent Mission of India to the United Nations, 618 F.3d 172 (2d Cir. 2010).

57 City of New York v. Permanent Mission of India to the United Nations, 618 F.3d 172 (2d Cir. 2010).

58 East Bay Sanctuary Covenant v. Trump, 932 F.3d 742 (9th Cir. 2018), as amended (July 24, 2019); In re Section 301 Cases, No. 21-00052-3JP, slip op. at 42–46 (Ct. Int'l Trade Apr. 1, 2022).

59 Marco Rubio, Determination: Foreign Affairs Functions of the United States, 90 Fed. Reg. 12,200, 12,200 (Mar. 14, 2025) (agency determination).

60 See Administrative Procedure Act, Pub. L. No. 79-404, ch. 324, §§ 4, 10, 60 Stat. 237, 238, 243–44 (1946) (separating rulemaking procedures from judicial review); Vermont Yankee Nuclear Power Corp. v. NRDC, 435 U.S. 519, 524, 549 (1978) (limiting judicially imposed procedures but remanding for APA review); Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 42–43 (1983) (requiring reasoned explanation).

first does not withdraw the second.[61] Courts applying the exception have said as much. In *City of New York v. Permanent Mission of India to the United Nations*, the Second Circuit held that the challenged notice was procedurally proper under the exception and separately reviewed whether the State Department possessed statutory authority to issue it, observing that limited review is not the absence of review.[62] The Court of International Trade likewise reviewed the legality of trade actions notwithstanding foreign-affairs objections.[63]

Resolving that dispute is unnecessary, because the cases that apply the exception still review the agencies' legal authority. Adrian Vermeule's account of emergency administrative law supplies a framework for understanding what is at stake. Specifically, Vermeule distinguishes two ways in which law can fail to constrain executive action. A legal black hole exists where a statute formally excludes review, so that no court passes on the action at all. A legal grey hole exists where review is formally available, but the governing standard has been relaxed to the point that it imposes no real constraint. Vermeule recounts the concern of Dyzenhaus and other rule-of-law theorists that this is in one respect the more troubling condition because it preserves the appearance of legality without its substance.[64] Applied here, reading § 553(a)(1) to excuse an agency's reasoning as well as its procedure would create a grey hole of exactly that kind: courts would continue to entertain challenges while the standard they applied had been emptied of content. Nothing in the provision's text supports that reading. The separate question whether a court may require additional procedure is governed by *Vermont Yankee*, which forbids courts from imposing procedures beyond those the APA requires.

Section 553(c) is the source of the ordinary duty to give a concise general statement of a rule's basis and purpose, and § 553(a)(1) exempts covered matters from § 553 as a whole, including subsection (c). If the foreign affairs exception applies, then the DOJ was not obliged to supply a statement of basis and purpose at all. The Department nevertheless conducted notice and comment pursuant to the Order. *Rodway* required USDA to comply with APA procedures because the agency had adopted a regulation making those procedures applicable to otherwise exempt rulemaking. It therefore supports enforcing an agency's binding procedural commitment, but does not itself establish that DOJ's receipt of comments displaced its asserted foreign-affairs exemption.[65] An applicable § 553 exemption does not itself displace § 706 review of final agency action. Whether an agency's

---

61 5 U.S.C. §§ 553, 706; Administrative Procedure Act, Pub. L. No. 79-404, ch. 324, §§ 4, 10, 60 Stat. 237, 238–39, 243–44 (1946).

62 City of New York v. Permanent Mission of India to the United Nations, 618 F.3d 172 (2d Cir. 2010).

63 In re Section 301 Cases, No. 21-00052-3JP, slip op. at 17, 27–28, 42–46 (Ct. Int'l Trade Apr. 1, 2022).

64 Adrian Vermeule, Our Schmittian Administrative Law, 122 Harv. L. Rev. 1095, 1096–97 (2009).

65 Rodway v. U.S. Dep't of Agric., 514 F.2d 809, 813–14, 817 (D.C. Cir. 1975).

explanation permits that review is distinct from whether the APA required it to conduct notice and comment.[66]

Perez v. Mortgage Bankers Ass'n holds that courts may not impose rulemaking procedures beyond those the APA prescribes, so the point is not that the DOJ must repeat its process or that a court could order additional procedure on remand.[67] When a record is built, the rule is reviewed on that record.[68]

B. What Can the Classified Record Support?

The DOJ relied on both unclassified and classified sources in promulgating the rule. The preamble describes the relationship between the rule and the sources used:

Although the unclassified record fully and independently supports the rule without the need to rely on the classified record, the classified record further supports the Department's judgment.[69]

That statement is merely the agency's representation. However, it nonetheless bears on review, because a court evaluates agency action on the grounds the agency actually invoked, and reviews the administrative record already in existence, supplemented where necessary by additional agency explanation of its original reasons.[70]

Courts do accept classified evidence in this field. In *Islamic American Relief Agency v. Gonzales*, the D.C. Circuit reviewed OFAC's blocking of a charity's assets, applied extremely deferential review, found the unclassified record sufficient to support the determination, and noted that the classified record contained further evidence that the organization was a branch of another entity.[71] The classified material there addressed the same factual question the court was reviewing: whether the branch relationship existed.[72]

---

66 5 U.S.C. §§ 553(a)(1), 706(2)(A); Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983).

67 Perez v. Mortg. Bankers Ass'n, 575 U.S. 92, 100–02 (2015).

68 Camp v. Pitts, 411 U.S. 138, 142 (1973) (per curiam).

69 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1637 (Jan. 8, 2025) (agency representation of dual-record posture and public-record sufficiency).

70 *SEC v. Chenery Corp.* (*Chenery I*), 318 U.S. 80, 87 (1943); *SEC v. Chenery Corp.* (*Chenery II*), 332 U.S. 194, 196 (1947) (holding that agency action must be judged on the grounds disclosed by the record); Camp v. Pitts, 411 U.S. 138, 142–43 (1973) (per curiam) (holding that the focal point for review is the administrative record already in existence and that inadequate explanation calls for agency explanation rather than de novo factfinding). This subsection reserves remedy. See id. at 143 (distinguishing additional explanation from vacatur and remand).

71 Islamic Am. Relief Agency v. Gonzales, 477 F.3d 728, 731, 734, 736 (D.C. Cir. 2007).

72 Id. (identifying operative question as whether record supported OFAC's branch-status conclusion).

The questions this rule presents are somewhat different in kind. Whether a combination of safeguards satisfies the incorporated standard, what datasets a recipient is "known to hold," and which organizations count as "recipient-linked" are not factual questions about an adversary's capabilities. They are, instead, the content of a public regulatory standard that private parties must apply before they transact.[73]

C. Which Questions Receive Deference; Factual Judgments and Reasoned Explanation?

Section 706 of the Administrative Procedure Act assigns a reviewing court different tasks depending on what is under review. It directs courts to decide all relevant questions of law, to interpret statutory provisions, to determine the meaning of the terms of an agency action, and to set aside action that is arbitrary, capricious, or in excess of statutory authority.[74] Those are not the same inquiry, and the Data Security Program presents questions of both kinds.

Elena Chachko's account of what she calls "administrative national security" explains why the object of review must be identified before the standard is chosen. Programs of this kind apply general standards to identified private parties, which resembles administrative adjudication more than the exercise of unreviewable foreign-affairs discretion, and it raises the ordinary administrative-law questions that attend agency action affecting regulated parties.[75] The two categories are addressed in turn.

1. Predictive and Factual Judgments Receive Substantial Deference

Arbitrary-and-capricious review is deferential in its ordinary application. A court asks whether the agency examined the relevant data and articulated a rational connection between the facts found and the choice made, and it does not substitute its own judgment for that of the agency.[76] Deference is greatest when an agency makes predictive judgments within its own expertise, particularly at the limits of available knowledge, and greater still in the national-security setting.[77]

In *Department of the Navy v. Egan*, a naval employee challenged the denial of his security clearance before the Merit Systems Protection Board. The Court held that the Board could not review the merits of the clearance decision, reasoning that a predictive judgment about

---

73 28 C.F.R. §§ 202.248, 202.401(a) (2025); CISA Security Requirements, supra note 7, §§ I.C, II.A.2.b.

74 5 U.S.C. § 706 (including § 706(2)(A), (C)).

75 Elena Chachko, *Administrative National Security*, 108 Geo. L.J. 1063, 1066–69 (2020).

76 Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983); Citizens to Pres. Overton Park, Inc. v. Volpe, 401 U.S. 402, 416 (1971).

77 Balt. Gas & Elec. Co. v. NRDC, 462 U.S. 87, 103 (1983); FCC v. Prometheus Radio Project, 592 U.S. 414, 423 (2021).

whether a person can be trusted with classified information "must be made by those with the necessary expertise in protecting classified information," and is committed to the Executive rather than to outside review.[78] *Haig v. Agee* similarly cautions that matters closely tied to foreign policy are rarely proper subjects for judicial intervention.[79] These authorities support substantial deference to the program's predictive threat assessments and technical judgments. *Egan* itself concerns security-clearance review; it does not make the Data Security Program's technical judgments unreviewable. The program's predictive threat assessments are not contested here.[80]

Neither decision converts national security into a general bar on review, and *Egan* itself independently resolved a legal question about the scope of the Board's review authority before deferring on the security-clearance judgment.[81] Deference of that character attaches to the predictive judgment; it does not migrate of its own accord to statutory interpretation or to the coherence of a public compliance standard.

2. Questions of Law and Explanation Are Decided by the Court

Holder v. Humanitarian Law Project shows both categories operating in a single case. The Court first rejected a proposed narrowing construction of the material-support statute as inconsistent with the text, resolving that question as a matter of statutory interpretation. Only when it reached whether ostensibly peaceful support could facilitate terrorism did it describe the question as empirical and credit the political branches' evaluation of the facts. The Court then stated that it did not defer to the Government's reading of the First Amendment, and that national-security concerns "do not warrant abdication of the judicial role."[82]

Some OFAC designation cases apply the same division in administrative-law form. *Islamic American Relief Agency* described review at the intersection of national security, foreign policy, and administrative law as extremely deferential, and still examined the administrative record and asked whether substantial evidence supported the determination.[83] *Al Haramain* held that the APA's judicial-review provisions govern challenges to OFAC designations, that factual findings are reviewed for substantial

---

78 Dep't of the Navy v. Egan, 484 U.S. 518, 520–22, 527–29 (1988).

79 Haig v. Agee, 453 U.S. 280, 292 (1981).

80 Exec. Order No. 14,117, 89 Fed. Reg. 15,421, 15,421 (Mar. 1, 2024); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1646 (Jan. 8, 2025); cf. Balt. Gas & Elec. Co. v. Nat. Res. Def. Council, Inc., 462 U.S. 87, 103, 105–06 (1983).

81 Egan, 484 U.S. at 530.

82 Holder v. Humanitarian Law Project, 561 U.S. 1, 16–18, 33–34 (2010).

83 Islamic Am. Relief Agency v. Gonzales, 477 F.3d 728, 734–37 (D.C. Cir. 2007).

evidence, and that legal questions are reviewed de novo.[84] Even in cases involving classified information and terrorism designations, the court did not apply a single deferential standard to the whole dispute because of its subject matter. It reviewed the agency's factual findings deferentially and its legal conclusions independently, so the intensity of review turned on the kind of question presented rather than on the sensitivity of the topic.

Ordinary administrative law imposes a further limit on how an agency may justify its action. *Department of Homeland Security v. Regents of the University of California* holds that review is confined to the grounds the agency invoked when it acted. There, the Acting Secretary rescinded the DACA program on the ground that it was unlawful, and the government later offered additional policy justifications. The Court refused to consider them, holding that an agency may elaborate on its original reasons but may not supply new ones after the fact.[85] Even where an agency's authority to act is not in doubt, a court may ask whether the agency gave the explanation the APA requires.

Application to This Program

Two consequences follow. The first concerns the presidential emergency. The program addresses the national emergency declared in Executive Order 13873 in 2019 and expanded by Executive Order 14117 in 2024. The National Emergencies Act requires annual continuation notices to keep such an emergency in effect.[86] Section 1701(a) conditions IEEPA authority on a declared emergency addressing an unusual and extraordinary threat, and the National Emergencies Act supplies the procedures governing declaration and continuation.[87] A direct APA challenge to the President's emergency declaration would face a threshold obstacle because the President is not an agency under the APA. *Franklin v. Massachusetts* holds that where the final action complained of is the President's there is no reviewable final agency action.[88]

The second concerns the agency implementation that followed. Executive Order 14117 assigned CISA the task of proposing and publishing the security requirements, and the DOJ's final rule incorporates them as the definition of "security requirements."[89] The DOJ's own guidance materials disclaim binding effect: the Compliance Guide states that it is explanatory and that inconsistencies are controlled by the statute, the order, and the

---

84 Al Haramain Islamic Found., Inc. v. U.S. Dep't of the Treasury, 686 F.3d 965, 979 (9th Cir. 2012).

85 Dep't of Homeland Sec. v. Regents of the Univ. of Cal., 591 U.S. 1, 20–23 (2020).

86 Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 17, 2019); Exec. Order No. 14,117, 89 Fed. Reg. 15,421, 15,421 (Mar. 1, 2024); 50 U.S.C. § 1622(d).

87 50 U.S.C. § 1701(a) (2018); National Emergencies Act, 50 U.S.C. §§ 1601–1651 (2018).

88 Franklin v. Massachusetts, 505 U.S. 788, 800–01 (1992); Dalton v. Specter, 511 U.S. 462, 469–76 (1994).

89 Exec. Order No. 14,117 § 2(d), 89 Fed. Reg. 15,421, 15,424 (Mar. 1, 2024); 28 C.F.R. § 202.248 (2025).

regulations, and the FAQs state that they do not alter legal requirements. Guidance of that kind can channel questions without supplying reasoning absent from a binding rule.[90]

The emergency predicate and the threat assessment receive maximum deference and go uncontested. Questions of law, such as statutory reach, addressed in Part II, and the public compliance standard and the explanation supporting it, addressed in Part IV, remain open.

IV. Does the Compliance Standard Tell Regulated Parties What It Requires?

A. What Do the Security Requirements Require?

The CISA security standard is an incorporated technical document.

Executive Order 14117 assigned two institutional roles. The Attorney General would identify the classes of prohibited and restricted transactions, including those for which CISA's requirements "adequately mitigate the risk" of access. CISA would propose, take comment on, and publish those requirements, based on the NIST Cybersecurity and Privacy Frameworks.[91] The DOJ made those requirements binding: § 202.248 incorporates the January 2025 CISA document by reference, and § 202.401(a) bars a U.S. person from knowingly engaging in a covered vendor, employment, or investment transaction unless it complies.[92] The substantive standard is CISA's; the binding force is from the DOJ. CISA itself stated that later revisions would not bind DOJ-regulated entities unless the DOJ updated the incorporated version.[93]

Those requirements state the program's central compliance obligation in a single sentence, which the parties call the chapeau because it introduces and governs the specific mitigations listed beneath it:

[I]mplement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern.[94]

---

90 DOJ Nat'l Sec. Div., Data Security Program: Compliance Guide 2 (Apr. 11, 2025); DOJ Nat'l Sec. Div., Data Security Program: Frequently Asked Questions 1 (Sept. 24, 2025).

91 Exec. Order No. 14,117 § 2(c)(i)–(ii), (d), 89 Fed. Reg. 15,421, 15,424 (Mar. 1, 2024); 28 C.F.R. §§ 202.248, 202.401(a) (2025); CISA Security Requirements, supra note 7.

92 28 C.F.R. §§ 202.248, 202.401(a) (2025); Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 16,466, 16,466–67 (Apr. 18, 2025).

93 Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1535 (Jan. 8, 2025).

94 CISA Security Requirements, supra note 7, § II.

That formulation has three features. First, CISA requires a combination of mitigations rather than a single technique. Second, the combination must be sufficient in relation to the covered data and the transaction. Third, what must be prevented is access to covered data in four specified forms.[95] Commenters asked whether the chapeau barred any access at all, and CISA revised the final text to require prevention of access to covered data in those forms rather than a literal ban on every version of every dataset.[96] A restricted transaction may proceed either by denying access to the covered data itself or by applying mitigation sufficient under the standard.

Section II sets out the data-level requirements. Its chapeau directs a U.S. person to "implement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, consistent with the data risk assessment described in Section I.C."[97] The mitigations fall into four categories: data minimization and masking (Section II.A), encryption (Section II.B), privacy-enhancing technologies such as privacy-preserving computation or differential privacy (Section II.C), and identity and access management configured to deny covered persons access to covered data (Section II.D).[98] A U.S. person is not required to use any particular one. It selects a combination sufficient, in light of the data risk assessment required by Section I.C, to prevent the access the chapeau describes.[99]

The de-identification obligation at issue arises within the first category. Section II.A requires processing that either renders data no longer covered or minimizes its linkability to U.S. persons before a covered person or country of concern obtains access, through techniques the standard identifies as aggregation, pseudonymization, de-identification, or anonymization.[100] The provision then supplies the condition at the center of this dispute:

When implemented, observability and linkability of data must be minimized to ensure U.S. person identities cannot be inferred or extrapolated from the individual data set at issue or

---

95 Id.

96 Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1532 (Jan. 8, 2025); CISA Security Requirements, supra note 7, § II.

97 CISA Security Requirements, supra note 7, § II.

98 Id. § II.A–.D, at 5–6.

99 Id. § II (chapeau), at 5; id. § I.C, at 4 (requiring an internal data risk assessment evaluating whether the selected Section II approach sufficiently prevents access).

100 Id. § II.A.2 & II.A.2.a, at 5.

in combination with other data sets the recipient or recipient-linked organizations are known to hold.[101]

The qualifier "when implemented" ties the condition to the minimization-and-masking approach: it governs a U.S. person that has selected that technique, not every restricted transaction. But once that approach is selected, the provision forecloses an assessment limited to the transferred dataset in isolation. A release may look nonidentifying within its four corners; Section II.A.2.b requires that it be evaluated against the datasets the recipient and its recipient-linked organizations are known to hold. Using one of the named techniques therefore does not by itself establish compliance. A U.S. person cannot satisfy the requirement by showing that it aggregated, pseudonymized, anonymized, or de-identified the data; it must show that what it did prevents the access the chapeau describes.[102]

CISA's requirements operate at three levels at once. CISA imposes conditions on the covered data, on the covered systems, and on the organization as a whole, dividing them into mandatory organizational and covered-system requirements in Section I and data-level requirements in Section II.[103] Organizational governance and system controls are the preconditions that make data-level controls effective, and Section I.C requires an internal risk assessment evaluating whether the selected Section II approach sufficiently prevents the prohibited access.[104] Systems performing Section II.A processing are themselves covered systems subject to Section I, so data-level processing never leaves the control environment.[105] CISA describes the requirements as a minimum set aimed at the Executive Order 14117 risk rather than a comprehensive cybersecurity program, and it declined to prescribe a single sufficient combination because restricted transactions vary.[106] The NIST frameworks that the Order made the basis for these requirements supply technical context but do not give a legal rule; they are nonbinding, non-prescriptive, and place de-identification within a broader risk-management structure.[107]

---

101 Id. § II.A.2.b, at 5–6.

102 Id. § II.A.2, at 5.

103 Id. at 1; Id. at 2; Id. § I.A–C, at 3–4; Id. § II.A–D, at 5–6.

104 CISA Security Requirements, supra note 7, § I.C; Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1531, 1536 (Jan. 8, 2025).

105 CISA Security Requirements, supra note 7, § II.A.3, .B.2.d, .C.2.

106 CISA Security Requirements, supra note 7, at 1 n.1; Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1533–35 (Jan. 8, 2025).

107 Exec. Order No. 14,117 § 2(d), 89 Fed. Reg. 15,421, 15,424 (Mar. 1, 2024); CISA Security Requirements, supra note 7, at 2; Nat'l Inst. of Standards & Tech., NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, cover (unnumbered), 6, 17, 24 (Jan. 16, 2020); Nat'l Inst. of Standards & Tech., The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, at i, 2, 4–5 (Feb. 26, 2024).

B. Did the Agencies Adequately Explain the Standard?

The rule appears to take inconsistent positions on de-identification. It keeps sensitive personal data within its scope even when the data is "anonymized, pseudonymized, de-identified, or encrypted," yet it permits a restricted transaction to proceed where de-identification and related controls prevent access.[108] The same techniques appear to be treated as inadequate to remove data from regulation and adequate to satisfy it.

1. What Does Reasoned Explanation Require of a Technical Judgment?

Section 706(2)(A) directs a court to set aside agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law."[109] That standard, articulated in *Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Automobile Insurance Co.*, provides that an agency must examine the relevant evidence and articulate a satisfactory explanation, including a rational connection between the facts it found and the choice it made. *Department of Homeland Security v. Regents of the University of California* confines review to the grounds the agency invoked when it acted.[110] The requirement persists in technical settings. *Baltimore Gas & Electric Co. v. Natural Resources Defense Council* emphasized that where an agency makes predictions "within its area of special expertise, at the frontiers of science," a reviewing court must be "at its most deferential," but it also required the agency to consider the relevant factors and articulate a rational connection between the facts found and the choice made.[111]

However, technical vocabulary does not convert every interpretive question into a frontier-science question. CISA's requirements are technical, demanding organizational controls, covered-system controls, risk assessments, encryption, access management, and data-level mitigations.[112] However, the question raised here is not which de-identification algorithm performs best or how much noise differential privacy requires. The question is rather whether a standard tied to datasets a recipient is "known to hold" identifies whose knowledge governs. Since the agencies themselves treat linkage risk as an established concern, the difficulty is one of explanatory fit rather than a question over scientific methods or at the frontiers of science. Where the meaning of the incorporated language is uncertain, the ordinary sources are the statement of basis and purpose in the final rule and the guidance the DOJ and CISA have published, and neither addresses the phrase at issue.

---

108 28 C.F.R. §§ 202.206, 202.401(a) (2025); CISA Security Requirements, supra note 7, §§ I–II.

109 5 U.S.C. § 706(2)(A).

110 Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983); Dep't of Homeland Sec. v. Regents of the Univ. of Cal., 591 U.S. 1, 20–23 (2020).

111 Balt. Gas & Elec. Co. v. Nat. Res. Def. Council, Inc., 462 U.S. 87, 103 (1983); Id. at 105–06.

112 CISA Security Requirements, supra note 7, §§ I–II.

The technical literature supports the agencies' premise. Latanya Sweeney, whose work on re-identification is often cited in the field, showed that organizations often strip obvious identifiers and treat the result as anonymous even though the remaining attributes permit individuals to be re-identified by linking the release to other available data. Using 1990 U.S. Census summary data, Sweeney estimated that 87% of the U.S. population had combinations of five-digit ZIP code, date of birth, and gender that likely made them unique.[113] The protective models she developed can defeat direct matching against known external sources in the right conditions, while other inference techniques and later data releases can still defeat them.[114]

2. Did the DOJ Contradict Itself?

The apparent contradiction is simple. The rule says that stripping names and other identifiers out of a dataset does not take it outside the rule, because such data can often be matched back to individuals. Yet the rule also lets a company complete an otherwise restricted transaction by stripping identifiers out of the data. The same technique appears to be treated as unreliable when a company invokes it to escape the rule and reliable when the company invokes it to satisfy the rule.

The two positions are consistent once the compliance pathway is described accurately. In response to comments arguing that the rule treated anonymized, pseudonymized, de-identified, and encrypted data no differently from unprocessed data, the DOJ explained that the rule does not prohibit covered transactions merely because data has been processed, and that such data remains within scope because it can be exploited when aggregated or combined.[115] CISA's text confirms that the compliance pathway is not de-identification alone: the requirements build on organizational and covered-system controls, require all of them, and permit flexibility only in selecting the data-level combination, which must in any event prevent access to data that is linkable, identifiable, unencrypted, or decryptable.[116] A rule may rationally treat weak anonymization as insufficient to remove data from the problem while recognizing that layered controls may reduce risk enough to permit a transaction, Sweeney's work shows the same distinction.[117]

---

113 Latanya Sweeney, k-Anonymity: A Model for Protecting Privacy, 10 Int'l J. Uncertainty, Fuzziness & Knowledge-Based Sys. 557, 558 (2002); Yves-Alexandre de Montjoye et al., Unique in the Crowd: The Privacy Bounds of Human Mobility, 3 Sci. Rep., art. 1376 (2013).

114 Sweeney, supra note 113, at 560, 566–68.

115 U.S. Dep't of Just., Nat'l Sec. Div., Data Security Program: Compliance Guide 2–4 (Apr. 11, 2025); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1657–58 (Jan. 8, 2025); CISA Security Requirements, supra note 7, §§ I–II.

116 CISA Security Requirements, supra note 7, §§ I–II.

117 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1657–58 (Jan. 8, 2025); 28 C.F.R. §§ 202.210(b)(2), 202.401(a), (c)

3. Data-Level Requirements and What Constitutes "Sufficiency"

The agencies were asked to clarify what combination of controls would be sufficient, and declined to prescribe a universally sufficient combination. In the notice finalizing the security requirements, CISA reported that commenters "took issue with the requirement to fully and effectively prevent access to covered data, and requested guidance and/or clarification about what constitutes a 'sufficient' combination of data-level requirements to prevent access."[118] CISA responded that "the question of what is sufficient to prevent access is a compliance matter and not a technical implementation matter," pointed to the Attorney General's authority under the Order to issue enforcement guidance, and added that it "will coordinate with DOJ if it determines further guidance on the meaning of 'sufficient' is appropriate."[119] The DOJ, for its part, stated in its own preamble that the Order "makes CISA, not the Department, responsible for developing the security requirements," and treated comments directed at those requirements as filed in the wrong docket.[120] The standard that determines civil and criminal exposure thus left unresolved, as of the rule's effective date, whose data holdings a regulated party must consider and what it is expected to know about them. CISA declined to define a universally sufficient combination, treating sufficiency as a compliance question. DOJ, in turn, referred comments about the security requirements to CISA. Neither passage supplies the more specific affiliation and knowledge criteria examined below. This section explores two issues regarding what is sufficient. The first is the class of organizations whose data holdings a transferor must consider; the second is the knowledge the transferor is expected to have about those holdings.

a. The Undefined Class of "Recipient-Linked Organizations"

The standard measures sufficiency against the holdings not only of the recipient but of "recipient-linked organizations," and neither the CISA nor the DOJ's regulation defines that class. The DOJ found that countries of concern cross-reference and layer datasets to generate insights and draw pattern-of-life and population-level inferences, so the transferor must look beyond the dataset it is transferring.[121] But DOJ's definitions of "linked" and "linkable" address associations among data and identifiers, with the note to § 202.233 limiting the inquiry to relevant transactions or a course of dealing between the

---

(1)–(2) (2025); CISA Security Requirements, supra note 7, §§ I–II; Sweeney, supra note 113, at 560, 566–68.

118 Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1534 (Jan. 8, 2025).

119 Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117, 90 Fed. Reg. 1528, 1534 (Jan. 8, 2025) (response to comments on data-level requirements and the meaning of "sufficiency").

120 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636, 1670 (Jan. 8, 2025).

121 Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 89 Fed. Reg. 86,116, 86,126–27 (Oct. 29, 2024); 90 Fed. Reg. at 1642 (explaining that anonymized data may become identifiable when cross-referenced and layered with other anonymized datasets and that anonymized data may itself present national-security risk).

same or related parties. They do not define which organizations are "recipient-linked" for the CISA requirement.[122] The covered-person definition supplies partial analogues in its use of ownership, control, jurisdiction, direction, employment, contractor status, and Attorney General designation, but the rule does not import them into the security requirement.[123] A recipient-linked organization might mean entities under common ownership, entities contractually involved in processing, affiliates within a corporate group, organizations sharing the data environment, or entities linked by state direction or intelligence access. A narrow affiliation-based reading would be easier to administer. However, a broader operational-access reading would better match the recombination risk.

b. The Undefined Standard of Knowledge

Even a settled definition of the relevant organizations would leave open what the transferor must be taken to know about their holdings, because the requirement reaches datasets those organizations are "known to hold" without saying to whom, or on what basis, they must be known. The word admits at least two understandings.

The first is actual knowledge: the transferor accounts only for datasets it is in fact aware the recipient holds. That understanding is administrable, because a company knows what it knows, but it severs compliance from the danger the rule identifies. The risk is the recipient's capacity to recombine data, and that capacity does not depend on what the transferor happens to have learned. Under an actual-knowledge standard a transferor that investigated nothing would face a narrower obligation than one that investigated diligently, which inverts the incentive the rule is meant to create.[124]

A second reading would charge the transferor with what it reasonably should have known. The DSP expressly adopts that approach in its definition of "knowingly," although the relationship between that definition and the CISA phrase "known to hold" still requires interpretation.[125] But a bare reasonableness standard leaves the scope of the inquiry uncertain. Read narrowly, it could ask only what is obvious about a counterparty, which captures little, because a recipient's data holdings are rarely apparent from the face of a transaction. Read broadly without a defined limit on the relevant organizational relationships, such a standard could require inquiry into datasets held by entities the transferor has never heard of, since the recombination risk turns on holdings across a recipient's affiliates and a wider state-linked ecosystem. The standard does not specify how far that inquiry must extend before a regulated party transacts.

---

122 28 C.F.R. §§ 202.232–.233 (2025).

123 28 C.F.R. § 202.211 (2025).

124 See 90 Fed. Reg. at 1642 (identifying the recombination and aggregation risk as the concern the requirement addresses).

125 28 C.F.R. § 202.230(a) (2025).

The rule states neither which of these it intends nor how the standard of knowledge relates to the undefined class of organizations. A transferor cannot determine whether its masking defeats inference until it knows both whose holdings to compare against and what it is charged with knowing about them.

c. A Defined Due-Diligence Obligation Would Resolve Both

The agencies could close both gaps at once by tying the standard to a due-diligence obligation. The rule requires a data compliance program with risk-based procedures addressing data flows, the identity and ownership of transaction parties, and vendor identity. The recordkeeping requirements expressly include the direct and indirect ownership of entities that are parties to the transaction.[126] They do not expressly require investigating other datasets held by those entities or by organizations connected to them through ownership or other relationships. Nor do they specify which organizational relationships, beyond the required ownership inquiry, a transferor must investigate to satisfy the masking condition. The rule supplies a basic diligence framework but leaves these questions unanswered.

The agencies could provide that a transferor is charged with knowing the datasets, and with identifying the linked organizations, that diligence proportionate to the transaction would reveal. They could specify what that diligence requires: which categories of organizational relationship must be considered, what inquiries a transferor must make about other data holdings, what sources it may rely on, and when further inquiry is excused.

A rule of that kind would answer both questions with a single mechanism. It would define the relevant class of organizations and require proportionate diligence to identify its members, resolving the first gap. It would fix the standard of knowledge at what that diligence would reveal about their holdings, resolving the second. It would fit the danger the DOJ identified without imposing an impossible burden of omniscience, and it would convert two indeterminate terms into a defined process.

V. Conclusion

The three questions posed at the outset resolve as follows. The Executive's judgment that countries of concern are acquiring Americans' sensitive data through ordinary commercial channels is supported, entitled to substantial deference, and not seriously contestable on this record. The DOJ probably has the better of the Berman Amendment argument as applied to non-expressive bulk commercial data: the text protecting "any information or

---

126 28 C.F.R. §§ 202.1001(a), (b)(1)–(2), 202.1101(b)(4) (2025).

informational materials" supports a broader reading, but Congress titled the 1994 expansion the Free Trade in Ideas Act, the platform-ban cases that gave the carve-out force all involved expressive exchange, and the decisions discussed here do not establish its application to raw bulk personal datasets. After *Loper Bright*, the scope of the withholding in § 1702(b)(3) is for the court rather than the agency to determine.[127]

The second question concerns judicial review, and the answer is that neither the foreign-affairs exception nor the classified record removes the program from it. The exception, whatever its scope, excuses notice-and-comment procedure rather than the APA's separate demand that final agency action be reasonably explained. The classified record supports the threat finding without supplying the public content of a rule that private parties must obey. That said, review is deferential where deference is owed. Arbitrary-and-capricious review is narrow in its ordinary operation, and it is narrower still for the factual and predictive findings on which this program rests: the DOJ's judgment about adversary acquisition and CISA's judgments about which mitigations reduce risk are the kind of determinations courts decline to second-guess. Deference of that character does not extend to the meaning of a statute or to whether an agency explained the standard it adopted.

The third question concerns the content of the compliance obligation, and it is where the program is thin. A U.S. person relying on the minimization-and-masking approach must address the possibility that identities can be inferred from the transferred dataset in combination with datasets that the recipient or recipient-linked organizations are known to hold.[128] Neither the DOJ nor CISA has said which entities that phrase covers. The rule defines "linked" and "linkable" for data, not for organizations, and the class might extend to a corporate parent, to affiliates under common ownership, to contractual processors sharing the data environment, or to an entire state-linked ecosystem. Those scopes impose materially different obligations, and the agencies have not expressly selected among those possible readings or explained the choice.

The implications beyond this program are correspondingly limited. Flexible, technology-neutral cybersecurity regulation is permissible, and a regulator confronting adversaries who adapt has good reason to avoid a checklist that tells them the margin to beat. Flexibility about methods, though, is not the same as silence about the predicate that determines whether the chosen methods suffice. Where civil penalties and criminal exposure turn on whether a party selected a sufficient combination of safeguards, the

---

127 50 U.S.C. § 1702(b)(3); 28 C.F.R. § 202.226(a)–(c) (2025); Loper Bright Enters. v. Raimondo, 603 U.S. 369, 412–13 (2024).

128 CISA Security Requirements, supra note 7, § II.A.2.b.

public standard must contain enough content for that party, and for a reviewing court, to know what the inquiry is.