Department of Justice

April 11, 2025
www.justice.gov

National Security Division
Foreign Investment Review Section

DATA SECURITY PROGRAM: IMPLEMENTATION AND ENFORCEMENT POLICY THROUGH JULY 8, 2025

The Data Security Program ("DSP") implemented by the National Security Division ("NSD") under Executive Order 14117[1] comprehensively and proactively addresses the continued efforts of foreign adversaries to use commercial activities to access, exploit, and weaponize U.S. Government-related data and Americans' bulk sensitive personal data. The DSP addresses this "unusual and extraordinary threat… to the national security and foreign policy of the United States" that has been repeatedly recognized across political parties and by all three branches of Government—including, notably, in the 2025 Annual Threat Assessment of the U.S. Intelligence Community and the President's America First Investment Policy, NSPM-2 on Imposing Maximum Pressure on Iran, national emergency declared in Executive Order 13873,[2] and 2017 National Security Strategy. To address this urgent threat, the DSP establishes what are effectively export controls that prevent foreign adversaries, and those subject to their control and direction, from accessing U.S. Government-related data and bulk U.S. sensitive personal data.

NSD's primary mission with respect to the implementation and enforcement of the DSP is to protect U.S. national security from the risk caused by countries of concern that seek to collect and weaponize Americans' most sensitive personal data. The International Emergency Economic Powers Act ("IEEPA") and the DSP authorize NSD to bring civil enforcement actions and criminal prosecutions for knowing or, with respect to criminal prosecutions, willful violations of the DSP's requirements. Unlawful acts under IEEPA are subject to civil penalties of up to the greater of $368,136 or twice the value of each violative transaction. Willful violations of IEEPA are punishable by imprisonment of up to 20 years and a $1,000,000 fine.

As the final rule explained, this threat is increasingly urgent, and ensuring prompt compliance with the DSP's requirements is critical to addressing the Administration's priorities and stopping the flow of U.S. sensitive personal data and government-related data to countries of concern. As explained in more detail in the DSP Compliance Guide, to aid compliance with the DSP requirements, U.S. individuals and entities should "know their data," including the kind and volume of data collected or maintained concerning U.S. persons; how their company uses this

[1] Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern). On January 8, 2025, NSD issued a final rule implementing Executive Order 14117, which is now available at 28 CFR Part 202. Unless otherwise indicated, all citations are to the sections of the DSP regulations in 28 CFR part 202.

[2] Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain).

data; whether they engage in covered data transactions with covered persons or countries of concern; and how such data is marketed, particularly with respect to current or recent former employees or contractors, or former senior officials, of the United States government, including the military and U.S. Intelligence Community.

NSD recognizes that individuals and companies may need to take steps to determine whether the DSP's prohibitions and restrictions apply to their activities, and to implement changes to their existing policies or to implement new policies and processes to comply. These steps may vary greatly depending on the existing structure and commercial activities of the entities subject to the DSP, but could include revising or creating new internal policies and processes, identifying data flows, changing vendors or suppliers, adjusting employee roles or responsibilities, deploying new security requirements, and revising existing contracts.

There are two key effective dates associated with the DSP: April 8, 2025 and October 6, 2025. Starting April 8, 2025, entities and individuals are required to comply with the DSP's prohibitions and restrictions, and with all other provisions of the DSP with the exception of the affirmative obligations of subpart J (related to due diligence and audit requirements for restricted transactions), § 202.1103 (related to reporting requirements for certain restricted transactions), and § 202.1104 (related to reports on rejected prohibited transactions). Starting October 6, 2025, entities and individuals must comply with subpart J and §§ 202.1103 and 202.1104. These effective dates remain in force.

However, consistent with the Executive's Article II authority to exercise enforcement discretion, NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (e.g., individuals and companies) additional time to continue implementing the necessary changes to comply with the DSP and provide additional opportunities for the public to engage with NSD on DSP-related inquiries. Specifically, NSD will not prioritize civil enforcement actions against any person for violations of the DSP that occur from April 8 through July 8, 2025 so long as the person is engaging in good faith efforts to comply with or come into compliance with the DSP during that time. This policy aims to allow the private sector to focus its resources and efforts on promptly coming into compliance and to allow NSD to prioritize its resources on facilitating compliance.

At the same time, during this 90-day period, NSD will pursue penalties and other enforcement actions as appropriate for egregious, willful violations. This policy does not limit NSD's authority and discretion to pursue civil enforcement if such persons did not engage in good-faith efforts to comply with, or come into compliance with, the DSP. Examples of evidence of good-faith efforts may include:

- Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitute data brokerage;
- Reviewing internal datasets and datatypes to determine if they are potentially subject to DSP;
- Renegotiating vendor agreements or negotiating contracts with new vendors;
- Transferring products and services to new vendors;
- Conducting due diligence on potential new vendors;
- Negotiating contractual onward transfer provisions with foreign persons who are the counterparties to data brokerage transactions;

- Adjusting employee work locations, roles or responsibilities;
- Evaluating investments from countries of concern or covered persons;
- Renegotiating investment agreements with countries of concern or covered persons; or
- Implementing the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

In considering any civil enforcement, NSD may also favorably consider, consistent with NSD enforcement policies, the extent to which a U.S. person voluntarily cooperated with any NSD inquiries.

This policy does not restrict NSD's lawful authority and discretion to pursue criminal enforcement in cases where individuals or entities willfully violate, attempt to violate, conspire to violate, cause a violation of, or engage in any action intended to evade or avoid the DSP's requirements.

During this 90-day period, NSD encourages the public to contact NSD at nsd.firs.datasecurity@usdoj.gov with informal inquires or information about the DSP and the guidance NSD has released. Although NSD may not be able to respond to every inquiry, NSD will use its best efforts to respond consistent with available resources, and any inquiries or information submitted may be used to develop and refine future guidance. Correspondingly, NSD discourages the submission of any formal requests for specific licenses or advisory opinions during this 90-day period: Although requests for specific licenses or advisory opinions during this 90-day period can be submitted, NSD will not review or adjudicate those submissions during the 90-day period (absent an emergency or imminent threat to public safety or national security).

At the end of this 90-day period, individuals and entities should be in full compliance with the DSP and should expect NSD to pursue appropriate enforcement with respect to any violations.

This Implementation and Enforcement Policy does not create any privileges, benefits, or rights, substantive or procedural, enforceable at law or in equity by any individual, organization, party, or witness in any administrative, civil, criminal, or other matter.