



PRESS RELEASE

# Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries

Friday, April 11, 2025

For Immediate Release

Office of Public Affairs

## Department Answers Frequently Asked Questions, Provides Guidance, and Issues Limited Enforcement Policy for First 90 Days

Today, the Justice Department took significant steps to move forward with implementing a critical program to prevent China, Russia, Iran, and other foreign adversaries from using commercial activities to access and exploit U.S. government-related data and Americans' sensitive personal data to commit espionage and economic espionage, conduct surveillance and counterintelligence activities, develop AI and military capabilities, and otherwise undermine our national security.

The Data Security Program implemented by the National Security Division (NSD) under [Executive Order 14117](#) 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.

The Justice Department's continued prioritization of the Data Security Program delivers on promises made by President Trump in his [America First Investment Policy](#) and [NSPM-2 on Imposing Maximum Pressure on Iran](#), addresses threats identified in the [2025 Annual Threat Assessment of the U.S. Intelligence Community](#) and President Trump's [2017 National Security Strategy](#), and responds to the national emergency President Trump declared in [Executive Order 13873](#).

"If you're a foreign adversary, why would you go through the trouble of complicated cyber intrusions and theft to get Americans' data when you can just buy it on the open market or force a company under your jurisdiction

to give you access?” said Deputy Attorney General Todd Blanche. “The Data Security Program makes getting that data a lot harder.”

To address this urgent threat, the [Data Security Program](#) establishes what are effectively export controls that prevent foreign adversaries, and those subject to their control, jurisdiction, ownership, and direction, from accessing U.S. government-related data and bulk genomic, geolocation, biometric, health, financial, and other sensitive personal data. To assist the public in coming into compliance with the Data Security Program, NSD has issued a [Compliance Guide](#), an initial list of over 100 [Frequently Asked Questions \(FAQs\)](#), and an [Implementation and Enforcement Policy](#) for the first 90 days. NSD will be taking additional steps over the coming weeks and months to implement the Data Security Program, including publishing an initial Covered Persons List that identifies and designates persons subject to the control and direction of foreign adversaries. The Data Security Program went into effect on April 8, 2025.

### **Newly Issued Guidance and FAQs**

The Data Security Program Compliance Guide identifies and describes best practices for complying with the Data Security Program, thereby mitigating the unacceptable national security risk of enabling countries of concern to access and exploit Americans’ sensitive personal data. The document provides guidance on key definitions, prohibited and restricted transactions, and the requirements for building a robust data compliance program. The Compliance Guide also provides model contractual language and suggests best practices for complying with the Data Security Program’s audit and recordkeeping requirements. It is crucial that U.S. persons familiarize themselves and become prepared to comply with the Data Security Program’s prohibitions and restrictions once they became effective on April 8, 2025.

The Data Security Program FAQs address high-level clarifications about Executive Order 14117 and provides valuable information about the Data Security Program, its scope, and accompanying processes for requesting licenses and advisory opinions, making disclosures of Data Security Program violations, and reporting rejected prohibited transactions. The FAQs reflect some of the comprehensive feedback and common issues the Department received and addressed through the rulemaking process, both as public comments in response to the [Advance Notice of Proposed Rulemaking](#) and [Notice of Proposed Rulemaking](#), as well as questions delivered during dozens of engagements with individuals, businesses, trade groups, and other stakeholders that were potentially interested in or impacted by the Data Security Program. NSD will update these FAQs as necessary and appropriate to address additional questions raised by the public.

NSD’s primary mission with respect to the implementation and enforcement of the Data Security Program is to protect U.S. national security from countries of concern that may seek to collect and weaponize Americans’ most sensitive personal data and government-related data. U.S. persons should “know their data” and the front-line role they play in mitigating these risks. As further explained in the Compliance Guide, individuals and entities subject to U.S. jurisdiction, as well as foreign individuals and entities conducting business in or with the United States or with U.S. persons, must comply with the Data Security Program.

The Compliance Guide and FAQs are explanatory and intended to provide general guidance to regulated parties about compliance with the Data Security Program. Nothing in these documents supplements, modifies, or supersedes the requirements set forth in the Data Security Program. NSD intends to update the FAQs on an ongoing basis as NSD identifies additional questions and responses that should be made public to aid the regulated community in compliance.

### **Newly Issued Enforcement Policy for the First 90 Days**

The Data Security Program went into effect on April 8, 2025. Starting April 8, 2025, entities and individuals were required to comply with the Data Security Program’s prohibitions and restrictions on engaging in covered data transactions. To provide additional time for entities and individuals to come into compliance, the Data Security Program delays certain affirmative due-diligence obligations, which do not go into effect until Oct. 6, 2025.

NSD recognizes that individuals and companies may need to take a number of steps to determine whether the Data Security Program’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.

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, NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (e.g., individuals and companies) additional time to implement the changes required by the Data Security Program, provide additional opportunities for the public to engage with NSD, and to minimize potential disruptions for businesses. As explained in NSD’s Data Security Program Implementation and Enforcement Policy Through July 8, 2025, NSD will not prioritize civil enforcement actions against any person for violations of the Data Security Program 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 Data Security Program during that time. These efforts include engaging in compliance activities described in that policy, such as amending or renegotiating existing contracts, conducting internal reviews of data flows, deploying the CISA [security requirements](#), and so on.

At the end of this 90-day period, individuals, and entities should be in full compliance with the DSP. This policy does not limit NSD’s lawful authority and discretion to pursue civil enforcement if entities and individuals did not engage in good faith efforts to comply with, or come into compliance with, the Data Security Program.

During this 90-day period, NSD encourages the public to contact NSD at [nsd.firs.datasecurity@usdoj.gov](mailto: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).

*Updated April 11, 2025*

## Topic

**NATIONAL SECURITY**

## Components

[National Security Division \(NSD\)](#) | [Office of the Deputy Attorney General](#)

# Related Content

---

---

PRESS RELEASE

## **Cameroonian Man Indicted for Conspiring to Provide Material Support to Armed Separatist Fighters to Murder, Kidnap, and Maim Individuals in Cameroon and For Making Threats**

A federal grand jury in Baltimore returned an indictment yesterday charging a Cameroonian national residing in Maryland, Eric Tataw, also known as “the Garri Master,” 38, of Gaithersburg, Maryland, with...

April 25, 2025

PRESS RELEASE

## **Former CIA Official Pleads Guilty to Acting as a Foreign Agent and Mishandling Classified Materials**

Dale Britt Bendler, 68, of Miami, Florida, pleaded guilty today to, while being a public official at the Central Intelligence Agency (CIA), acting as a foreign agent required to register...

April 23, 2025

PRESS RELEASE

## **Former U.S. Army Intelligence Analyst Sentenced for Selling Sensitive Military Information to Individual Tied to Chinese Government**

A former U.S. Army intelligence analyst was sentenced today to 84 months in prison for conspiring to collect and transmit national defense information, including sensitive, non-public U.S. military information, to...

April 23, 2025

---

 **Office of Public Affairs**

U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington DC 20530

 Office of Public Affairs Direct Line  
202-514-2007

Department of Justice Main Switchboard  
202-514-2000