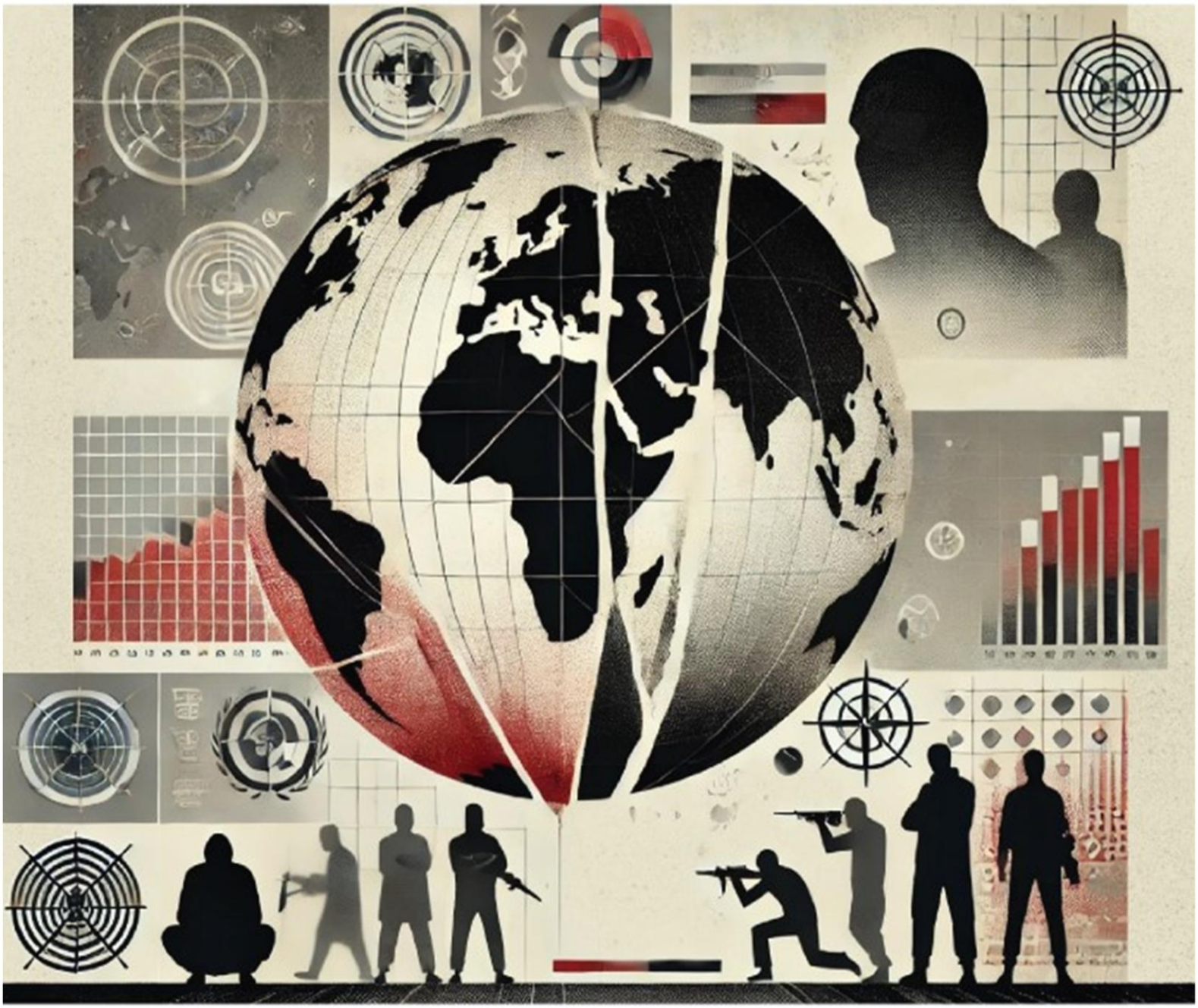
THE

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD



ASSESSMENT AND RECOMMENDATIONS

AUTHORITIES ADDRESSING FOREIGN RACIALLY MOTIVATED EXTREMISM & PRIVACY AND CIVIL LIBERTIES IMPACTS

January 21, 2025

[THIS PAGE INTENTIONALLY LEFT BLANK]

THE
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

ASSESSMENT AND RECOMMENDATIONS
AUTHORITIES ADDRESSING FOREIGN RACIALLY MOTIVATED EXTREMISM & PRIVACY CIVIL LIBERTIES IMPACTS

JANUARY 21, 2025

The Board acknowledges with gratitude the staff members who worked on this project, including Leteisha Boss, Hannah Burgess, Jennifer Fitzpatrick, Ryan Fletcher, Tatjana Naquin, Alexa Potter, Saleela Salahudin, Courtney Sullivan, Julie Tulbert, and other current and former staff members.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Privacy and Civil Liberties Oversight Board (PCLOB or Board) provides the following assessment and recommendations in response to Section 824(b)(3)(A) and Section 824(b)(3)(B) of the Intelligence Authorization Act for Fiscal Year 2022 (Consolidated Appropriations Act, 2022; Division X) (Pub. L. No. 117-103) (IAA). This assessment and these recommendations are submitted in conjunction with an Intelligence Assessment and an Intelligence Report provided to Congress by the Director of National Intelligence (DNI) pursuant to Sections 824(a)(1)-(4) and 824(b)(1)-(2) of the IAA. Section 824(a)(1)-(4) called for the DNI, through the Director of the National Counterterrorism Center (NCTC) and in coordination with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), to submit to Congress an Intelligence Assessment on significant threats to the United States associated with foreign racially motivated violent extremist (RMVE) organizations.[1]

Section 824(b)(1)-(2) called for the DNI to issue a separate Intelligence Report in coordination with the Secretary of State, the Secretary of the Treasury, the Attorney General, and the Secretary of Homeland Security regarding the use of specific laws, regulations, and policies by the federal government to counter significant threats to the United States and U.S. persons associated with foreign RMVE organizations, including an assessment of whether (and if so, to what extent and why) such federal laws, regulations, and policies are sufficient to counter foreign RMVE threats, including a description of any gaps, specific examples to illustrate such gaps, and recommendations regarding how to remedy such gaps. In its Intelligence Report, the Office of the Director of National Intelligence (ODNI) did not identify any legal gaps but stated that it was focused on and recommended increasing relevant information sharing regarding the foreign RMVE threat among federal departments and

[1] In its Intelligence Assessment, the ODNI concluded that foreign RMVE organizations espousing superiority of the white race do not pose a direct threat to U.S. national security and that the "Intelligence Community has not identified any foreign REMVE groups that currently present a direct threat to attack the United States." Off. of the Dir. of Nat'l Intel., *Intelligence Assessment on Significant Threats to the United States Associated with Foreign Racially Motivated Violent Extremist Organizations*, at 3 (Dec. 2022) [hereinafter Intelligence Assessment]. In this report, PCLOB uses the term "racially motivated violent extremist," abbreviated "RMVE," consistent with the terminology used in Section 824. The ODNI Report and Assessment used the term "racially or ethnically motivated violent extremist," abbreviated "REMVE."

agencies; state, local, tribal and territorial governments; the private sector; and foreign partners.[2]

Section 824(b)(3)(A) requires PCLOB to conduct an "assessment of the impacts to the privacy and civil liberties of U.S. persons concerning the use or recommended use of any federal laws, regulations, and policies" used by the federal government to address significant threats to the United States and U.S. persons associated with foreign RMVE organizations, including pursuant to the following provisions:

> (i) Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485) and Section 119 of the National Security Act of 1949 (50 U.S.C. 3056), particularly with respect to the coordination and integration of all instruments of national power;
>
> (ii) Executive Order 12333 (50 U.S.C. 3001 note), as amended;
>
> (iii) the designation of foreign terrorist organizations under Section 219 of the Immigration and Nationality Act (8 U.S.C. 1189);
>
> (iv) the designation of specially designated terrorists, specially designated global terrorists, or specially designated nationals and blocked persons, pursuant to Executive Orders 13886, 13372, and 13224 and parts 594, 595, 596, and 597 of title 31, Code of Federal Regulations;
>
> (v) National Security Presidential Memorandums 7 and 9, particularly with respect to the sharing of terrorism information and screening and vetting activities; and
>
> (vi) any other applicable federal laws, regulations, or policies.

Further, Section 824(b)(3)(B) requires that PCLOB produce "recommendations on options to develop protections to mitigate such impacts" to U.S. persons' privacy and civil liberties.

[2] In its Intelligence Report regarding the U.S. government's use of federal laws, regulations, and policies to counter significant threats posed by foreign RMVE organizations to the United States and U.S. persons, the ODNI stated that federal laws, regulations, and policies pertaining to international terrorists and terrorist organizations are postured to cover foreign RMVEs but noted that although the relevant laws are directed at foreign terrorist groups, "the foreign REMVE threat stems from a largely fluid and fragmented movement, lacking in hierarchical structures rather than foreign REMVE groups." It stated that "the foreign REMVE threat manifests primarily in the form of lone actors." Off. of the Dir. of Nat'l Intel., *Intelligence Report on Foreign Racially Motivated Violent Extremist Organizations*, at 2 (Nov. 2023) [hereinafter Intelligence Report].

The Board's assessment is circumscribed: Section 824 directs PCLOB to assess the privacy and civil liberties impacts to U.S. persons from the use or recommended use of enumerated federal laws, regulations, and policies to counter the threats posed specifically by foreign RMVE organizations and to make recommendations to mitigate any such impacts. In addition, the Board's review is necessarily limited due to both the breadth of the counterterrorism statutes, executive orders, and regulations set forth in Section 824(b)(2)(A), and the number of agencies that use them to counter both foreign RMVE and wider terrorist threats. Assessing in detail—in a single report—the agencies' day-to-day implementation of the many privacy and civil liberties safeguards applicable to the authorities that Congress enumerated is not contemplated by Section 824.

In conducting this assessment, PCLOB engaged with the Civil Liberties and Privacy Officers, mission staff, and counsel from the ODNI, DHS, the Department of Treasury (Treasury), the Department of State (State Department), and the FBI—agencies with which the ODNI coordinated in drafting its foreign RMVE organization Intelligence Assessment and Intelligence Report. The Board requested and received from each agency written and oral descriptions of whether and how the agency employs the legal authorities enumerated in Section 824(b)(2)(A)(i)-(vi) to address significant threats to the United States and U.S. persons associated with foreign RMVE organizations and to identify the privacy and civil liberties safeguards in place for U.S. persons associated with the use of those authorities.[3] The Board has organized this assessment categorically, grouping the enumerated legal authorities as follows: Intelligence Collection, Analysis, and Dissemination; Information Sharing; Terrorist Designations; and Travel and Immigration-Related Vetting.

Federal agencies largely apply the enumerated authorities to counter threats from foreign RMVE organizations in the same manner they apply the authorities to counter threats from other international terrorist groups.[4] The privacy and civil liberties impacts to U.S. persons are likewise similar with respect to both applications. To the extent that such impacts occur, they arise in the context of existing legal structures, whether applied to foreign RMVE groups or any other terrorist organizations. Within those structures, various privacy and civil liberties protections are in place.

[3] Because the ODNI focused its Intelligence Report and Intelligence Assessment (referenced above) on white supremacist organizations, we have focused on such groups. The ODNI reported that "[t]he IC assesses that only foreign REMVEs driven by a belief in the superiority of the white race espouse violent rhetoric that we have seen contribute to related radicalization and violence in the United States." Intelligence Assessment, *supra* note 1, at 3.

[4] In its Intelligence Report, the DNI stated that, "[f]ederal laws, regulations, and policies that pertain to international terrorist and international terrorist organizations are postured to cover foreign REMVE groups." Intelligence Report, *supra* note 2, at 9.

Although the scope of this report is narrow, the Board makes two recommendations where greater clarity and transparency might yield information that could help facilitate future assessments of privacy and civil liberties impacts from the government's use of these authorities to counter foreign RMVE threats. The Board recommends that: (1) Congress should clarify who has authority to appoint a Program Manager for the Information Sharing Environment (ISE); and (2) Congress should demand ODNI resume issuing statutorily required annual reports on the performance of the ISE.

II. ASSESSMENT OF POTENTIAL PRIVACY AND CIVIL LIBERTIES IMPACTS TO U.S. PERSONS

A. Intelligence Collection, Analysis, and Dissemination

Executive Order 12333

Executive Order 12333, United States Intelligence Activities (2008), is a foundational document for the United States' foreign intelligence efforts, including efforts to protect the nation from terrorism.[5] It establishes a framework that applies broadly to the government's collection, analysis, and use of foreign intelligence and counterintelligence—from human sources, by interception of communications, by cameras and other sensors on satellites and aerial systems, and through relationships with the intelligence services of other governments.[6] The ODNI noted in its Intelligence Report that "E.O. 12333 makes no distinction between different types of international terrorism threats, such as those associated with foreign REMVE groups or individuals."[7]

1. *Privacy and Civil Liberties Protections for U.S. Persons*

E.O. 12333 authorizes the collection and use of information concerning U.S. persons only in accordance with Attorney General-approved guidelines (Attorney General Guidelines) governing each intelligence agency's protections of U.S. person information.[8] E.O. 12333 specifies the types of information concerning U.S. persons that such procedures permit to be collected, retained, and disseminated and prohibits the use of specified collection techniques except in accordance with Attorney General Guidelines.[9] E.O. 12333 further limits the types of collection techniques the Attorney General Guidelines may authorize for certain Intelligence Community (IC) elements and where they may be conducted.[10]

Part 2 of E.O. 12333 establishes "certain general principles that . . . are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests."[11] These principles include a requirement to use the least intrusive collection technique feasible when inside the United States or directed against a U.S. person abroad; a prohibition on the use of specified intrusive collection techniques except in accordance with established procedures; and authorization to provide assistance to law enforcement and other civil

[5] U.S. Priv. & C.L. Oversight Bd., *Report on Executive Order 12333*, at 4 (Apr. 2021) [hereinafter PCLOB E.O. 12333 Report] (citing Exec. Order No. 12333, 46 Fed. Reg. 235 (Dec. 8, 1981)), https://www.dni.gov/index.php/ic-legal-referencebook/executive-order-12333).

[6] *Id.*

[7] Intelligence Report, *supra* note 2, at 6.

[8] Exec. Order No. 12333 §§ 2.3-2.4.

[9] *Id.* § 2.3.

[10] *Id.*

[11] *Id.* § 2.2.

authorities.[12] E.O. 12333 further specifies that nothing therein "shall be construed to authorize any activity in violation of the Constitution or statutes of the United States" and that the intelligence agencies' Attorney General Guidelines "shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes."[13]

2. *Potential Privacy and Civil Liberties Impacts to U.S. Persons*

PCLOB has previously conducted oversight of counterterrorism activities conducted under E.O. 12333, including three "deep dives" into specific activities conducted by the Central Intelligence Agency (CIA) and the National Security Agency (NSA). PCLOB also published a high-level public report providing an overview of E.O. 12333.[14] Given the extent of counterterrorism activities and other intelligence collection that are governed by E.O. 12333, it is not possible to address that authority or its privacy and civil liberties impacts in detail in this report. However, the Board anticipates that PCLOB will conduct further oversight of such activities in the future.

As the Board discussed in its April 2021 report on E.O. 12333, "the Order is among the largest and most complex of U.S. surveillance authorities."[15] It does not authorize one specific foreign intelligence program but rather "provides a broad framework for the organization and coordination of missions of the Intelligence Community."[16] Communications between foreigners and U.S. persons as well as between U.S. persons may fall within E.O. 12333's purview. For example, E.O. 12333 requires that agencies' Attorney General Guidelines permit the collection, retention, or dissemination of incidentally obtained information about a U.S. person if the information "may indicate involvement in activities that may violate federal, state, local, or foreign laws."[17] When the government targets foreign RMVE groups, it is possible that it will incidentally collect Americans' First Amendment-protected communications or collect information that could be connected to a U.S. person's racially motivated violent extremist views, even if that person poses no true threat to the United States. Any privacy and civil liberties impacts from the incidental collection of U.S. persons' communications could be compounded if such information were improperly shared throughout the IC; with state, local, tribal, and territorial entities; or with foreign partners.

[12] *Id.* §§ 2.4, 2.6.

[13] *Id.* §§ 2.4, 2.8.

[14] For public, declassified versions of PCLOB's deep dives into E.O. 12333, *see* U.S. Priv. and C.L. Oversight Bd., *Oversight Reports*, https://www.pclob.gov/Oversight (last visited Dec. 5, 2024).

[15] PCLOB E.O. 12333 Report, *supra* note 5, at 4.

[16] *Id.*

[17] Exec. Order No. 12333 § 2.3(i).

B. Information Sharing

Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), as amended, directed the President to establish an "information sharing environment" (ISE) for the sharing of "terrorism information" among appropriate federal, state, local, tribal, and territorial entities "in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[18] It also required the President to designate an ISE Program Manager (PM), establish an Information Sharing Council (ISC), define common standards, and apply technology to enable the access, retention, production, and sharing of terrorism information on the ISE and to ensure that the ISE had certain attributes, including protections for individuals' privacy and civil liberties.[19]

1. *Privacy and Civil Liberties Protections for U.S. Persons*

In 2006, the ISE PM issued ISE Privacy Guidelines stating that "[p]rotecting privacy and civil liberties is a core tenet of the ISE" and requiring each agency that possesses or uses terrorism information to designate an ISE Privacy Official with agency-wide responsibility for privacy issues to oversee the implementation of the ISE.[20] The ISE Privacy Guidelines specified that protected information can be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information.[21]

The ODNI reports that because IRTPA broadly defines "terrorism information,"[22] Section 1016 of "IRTPA and the ISE it created adequately apply to the sharing of information regarding threats to the United States posed by foreign REMVE groups and organizations."[23] The ODNI reports that the ISE continues to serve as the "baseline" for information sharing, in coordination with other authorities (e.g., Attorney General Guidelines), and that it facilitates the sharing of

[18] Intelligence Reform and Terrorism Protection Act of 2004, Pub. L. No. 108-458, § 1016(b) (2004) [hereinafter IRTPA].

[19] *Id.* § 1016(a)(1)-(3).

[20] Off. of the Dir. of Nat'l Intel., *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*, at ii, 6 (Dec. 2006), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Privacy_Guidelines_ISE.pdf.

[21] *Id.* at 2.

[22] Sec. 1016(a)(4) defines "terrorism information" as "all information, whether collected, produced, or distributed by intelligence, law enforcement, miliary, or homeland security, or other activities relating to (A) the existence, organization, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, or to United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." IRTPA § 1016(a)(4).

[23] Intelligence Report, *supra* note 2, at 4.

terrorism information regarding foreign RMVE organizations "on the same terms that it does with other international terrorist groups or individuals."[24] The agencies have advised that they participate in the ISE created by IRTPA, that they developed or followed agency-specific ISE privacy and civil liberties guidelines,[25] and that they also share or can share information to counter foreign RMVE threats through other information sharing authorities, including agencies' Attorney General Guidelines.

Section 119 of the National Security Act of 1949

Section 119 of the National Security Act, as amended by IRTPA, codified NCTC within the ODNI, established NCTC's mission and authorities, and set forth its Director's duties and responsibilities.[26] NCTC serves as the primary organization charged with analyzing and integrating all U.S. intelligence pertaining to terrorism or counterterrorism.[27] It is tasked with ensuring that agencies have access to intelligence needed to accomplish their responsibilities and serving as the central shared knowledge bank on known and suspected terrorist groups, their goals, strategies, capabilities, and support networks.[28] In addition, NCTC coordinates the IC's sharing of information with U.S. government policy makers that implement terrorist designation authorities under Section 219 of the Immigration and Nationality Act and E.O. 13224 (discussed below) and the dissemination of terrorism information to foreign governments. The ODNI reports that NCTC is "well positioned to coordinate and lead the USG's [U.S. government's] counterterrorism enterprise to address the threats posed by foreign REMVE groups."[29]

---

[24] *Id.*

[25] U.S. Dep't of Treasury, *Treasury Directive 25-10, Information Sharing Environment Privacy and Civil Liberties Policy* (Aug. 2023), https://home.treasury.gov/about/general-information/orders-and-directives/td25-10; U.S. Dep't of Just., *Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment* (Jan. 2010), https://www.justice.gov/opcl/docs/doj-ise-privacy-policy.pdf; Off. of the Dir. of Nat'l Intel., *Implementation of the Information Sharing Environment Privacy Guidelines for Sharing Protected Information* (Sept. 2009), https://www.dni.gov/files/documents/ODNI%20ISE%20Privacy%20Guidelines.pdf; U.S Dep't of Homeland Sec., *The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy* (June 2009), https://www.dhs.gov/sites/default/files/publications/privacyandcivillibertiespolicyguidancememorandum2009-01.pdf.

[26] National Security Act of 1947, Pub. L. No. 235, 61 Stat. 496, § 119 (1947).

[27] *Id.*

[28] Off. of the Dir. of Nat'l Intel., *National Counterterrorism Center Implementation Procedures for the ODNI Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, at 5 (Mar. 2021), https://www.dni.gov/files/NCTC/documents/news_documents/NCTC_Implementation_Procedures_executed_3_22_21_U_final.pdf.

[29] Intelligence Report, *supra* note 2, at 5. In its Intelligence Report, the ODNI also referenced E.O. 13388, issued in 2005, requiring heads of federal departments and agencies possessing terrorism information to promptly provide that information to other federal agencies with counterterrorism responsibilities, as supporting NCTC's mission under Section 119 of the National Security Act.

1. *Privacy and Civil Liberties Protections for U.S. Persons*

Section 119, a codification of the NCTC entity, does not itself explicitly address the protection of privacy and civil liberties. However, Section 103 of the Act did establish a Civil Liberties Protection Officer to, among other things, "oversee compliance by the Office and the Director of National Intelligence with requirements under the Constitution and all laws, regulations, executive orders, and implementing guidelines relating to civil liberties and privacy."[30] NCTC, as a subcomponent of the ODNI, reports directly to the DNI. NCTC is governed by the ODNI Attorney General Guidelines concerning U.S. person information and the NCTC Implementation Procedures for the ODNI Guidelines, which provide a number of protections for the privacy and civil liberties of U.S. persons.[31]

National Security Presidential Memorandum-7

National Security Presidential Memorandum-7 (NSPM-7), *Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans* (2017), which post-dates implementation of the ISE, established U.S. policy around the identification, integration, management, use, and sharing of information concerning cyber threat actors, foreign intelligence threat actors, military threat actors, transnational criminal actors, and weapons proliferators who threaten the United States.[32] It also directed the Attorney General, the Secretary of Homeland Security, and the DNI to lead, in consultation and coordination with the Secretaries of State, Treasury, Defense, Energy, and the CIA, the development and implementation of technical architectures and policy frameworks to advance these activities.[33]

1. *Privacy and Civil Liberties Protections for U.S. Persons*

The Memorandum requires that NSPM-7 "be implemented in a manner that … appropriately protects privacy, civil rights, civil liberties, and other constitutional and statutory rights, including through compliance with applicable guidelines governing the collection, retention, and dissemination of personally identifiable information."[34] Therefore, for all applications and uses of national security threat actor information managed within technical

[30] National Security Act of 1947 § 103(D)(b).

[31] On December 10, 2024, PCLOB published an oversight report on NCTC's use of these procedures, which includes recommendations for enhancing privacy safeguards. *See* U.S. Priv. & C.L. Oversight Bd., *Report on the National Counterterrorism Center* (Dec. 10, 2024), https://documents.pclob.gov/prod/Documents/OversightReport/72b3b35c-3595-47e2-a97f-142f350f14da/PCLOB%20FY2024%20NCTC%20REPORT-12.10.2024-FINAL.pdf.

[32] The White House, *National Security Presidential Memorandum–7* (Oct. 2017), https://trumpwhitehouse.archives.gov/presidential-actions/national-security-presidential-memorandum-7/#:~:text=This%20memorandum%20shall%20be%20implemented,investigations%3B%20and%20appropriately%20protects%20privacy.

[33] *Id.*

[34] *Id.*

architectures, the applicable agency heads must ensure that appropriate and lawful procedures and safeguards exist to protect such rights and provide appropriate protections before the application or use goes into effect.[35]

2. *Potential Privacy and Civil Liberties Impacts to U.S. Persons*

According to IRTPA, federal government departments or agencies that operate an ISE system or otherwise participate in the ISE must ensure full department compliance with information sharing policies, procedures, guidelines, and standards; ensure the provision of adequate resources for systems and activities supporting the operation of and participation in the ISE; ensure full department or agency cooperation in the development of the ISE to implement government-wide information sharing; and submit, at the request of the President or the PM, any reports on the implementation or the requirements of the ISE within such department or agency.[36]

Though agencies have procedures for collecting, handling, and marking U.S. person information prior to dissemination to other agencies, departments, or interagency offices, there are still risks that information could be improperly shared (e.g., without masking U.S. person information where required) or that an entity with which U.S. person information is shared may not protect U.S. person information in a similar manner or abide by the same privacy standards. Although the potential mishandling of U.S. person communications is not unique to countering the foreign RMVE threat, the potential impact from improper sharing may be compounded if protected communications are shared with state, local, territorial, tribal, law enforcement, or international partners.[37]

Separately, in June 2023, the Government Accountability Office (GAO) issued a report to the House Committee on Homeland Security identifying "action needed to further develop" the ISE. GAO found that, though the relevant federal agencies involved in the ISE achieved almost all of the 2013 ISE implementation plan's priority objectives, the ISE PM role had been vacant since 2017.[38] GAO found that no other official or agency assumed the PM's role of assessing federal implementation efforts since 2017 and the Board confirmed that this is still the case as of January

[35] *Id.*

[36] IRTPA § 1016(i).

[37] As referenced above, in its Intelligence Report, the ODNI recommends that, to assist U.S. policy makers in addressing the threats posed by foreign RMVE groups and individual foreign RMVE actors, information sharing amongst federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and foreign partners should be increased. Intelligence Report, *supra* note 2, at 9.

[38] U.S. Gov. Accountability Off., *Action Needed to Further Develop the Information Sharing Environment*, at 10 (June 2023), https://www.gao.gov/assets/gao-23-105310.pdf. GAO reported that the PM's responsibilities include managing the ISE; assisting with policy development; issuing procedures, guidelines, instructions, and functional standards for the ISE; identifying and resolving information sharing disputes; and assessing and reporting to Congress on federal efforts to implement the ISE.

2025.[39] GAO stated that without a PM it will be difficult to ensure the ISE receives continued leadership commitment and a means to monitor actions and assess progress in completing work on the open priority objectives.[40]

Section 1016 of IRTPA also requires the President, with assistance from the PM, submit an annual report to Congress on the state of the ISE and information sharing across the federal government.[41] Prior to 2017, the ISE PM issued such reports to Congress; however, in the absence of a PM, the ODNI continued to issue these annual reports to Congress through calendar year 2019.[42] GAO concluded that, without assessments from a PM or other designated entity, the impact of agencies' ISE-related efforts on completing the open priority objectives is unknown.[43] GAO recommended that Congress consider amending the ISE's enabling statute to clarify authorities for filling the PM position, and that the Assistant to the President for Homeland Security and Counterterrorism take steps to ensure that (1) a PM is in place, and (2) implementation efforts are assessed.[44] However, the ODNI states in its report and has conveyed to PCLOB that information sharing has successfully continued without a PM, because it is bolstered not just by the ISE guidelines but also other information sharing authorities and agency Attorney General Guidelines.[45] NCTC advised that the information sharing architecture is in place and that the ISE is part and parcel of the other authorities through which NCTC shares information, particularly the NCTC founding authorities, the ODNI Attorney General Guidelines, and the NCTC Implementation Procedures for the ODNI Guidelines.

C. Terrorist Designations

Section 219 of the Immigration and Nationality Act

Under Section 219 of the Immigration and Nationality Act, the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, is authorized to designate an organization as a Foreign Terrorist Organization (FTO) if three criteria are met: (1) the organization is foreign; (2) the organization engages in terrorist activity or terrorism or retains the capability and intent to engage in terrorist activity or terrorism; and (3) the organization's terrorist activity or terrorism threatens the security of U.S. nationals or the national security of the United

[39] *Id*. at 16.

[40] *Id*.

[41] IRTPA § 1016.

[42] Action Needed to Further Develop the Information Sharing Environment, *supra* note 38, at 4.

[43] *Id*. at 15.

[44] *Id*. at 25.

[45] PCLOB Team Notes from Meeting with the ODNI (Apr. 22, 2024); Intelligence Report, *supra* note 2, at 4.

States.[46] The State Department's Bureau of Counterterrorism (CT) is responsible for FTO designations and focuses on groups involved in violent extremism, including those that espouse RMVE ideology, and identifies specific targets for designation.[47] The State Department will also consider recommendations for designation from other agencies and foreign partners.[48] Those agencies provide input or recommendations to the State Department, or gather intelligence that is used to support designations.[49]

The consequences of an FTO designation include: (1) a freeze on assets the organization holds within a U.S. financial institution; (2) criminal prosecution of individuals for material support to an FTO; and (3) immigration restrictions for members and those who provide material support, including removal of non-citizens.[50] The Secretary of State publishes FTO designations in the Federal Register and the State Department reviews them every five years (if no review has yet taken place).[51] In making an FTO designation, the State Department creates an administrative record that could include unclassified or classified U.S. person information.[52] Organizations may file petitions for revocation two years after designation.[53]

1. *Privacy and Civil Liberties Protections for U.S. Persons*

While U.S. persons and organizations cannot be designated FTOs, their rights can be implicated under statutes criminalizing material support to an FTO. Under 18 U.S.C. § 2339B, the government must show that (1) a defendant knew the organization had been designated as an FTO or (2) a defendant knew that the organization has or is engaged in "terrorist activity."[54] The

[46] 8 U.S.C. § 1189(a)(1).

[47] State Dep't Responses to PCLOB Questions (Apr. 9, 2024); U.S. Gov. Accountability Off., *Combating Terrorism: Foreign Terrorist Organization Designation Process and U.S. Agency Enforcement Actions*, at 5 (June 2015), https://www.gao.gov/assets/700/690471.pdf.

[48] *Combating Terrorism: Foreign Terrorist Organization Designation Process and U.S. Agency Enforcement Actions*, *supra* note 47, at 5.

[49] For a general overview of agencies' roles, *see id.* at 24. In PCLOB's meetings with the relevant agencies, DHS's Office of Intelligence and Analysis (I&A) said that it does not participate in the designation process overall, but that intelligence collected by I&A supports the designation process. PCLOB Team Notes from Meeting with DHS I&A (Jan. 5, 2024). Treasury's Office of Intelligence and Analysis (OIA) said that it conducts all-source intelligence research and analysis on foreign-based individuals and groups involved in violent extremism, including those that espouse RMVE ideology. Treasury Dep't Responses to PCLOB Questions (Mar. 28, 2024).

[50] 8 U.S.C. §§ 1182(a)(3)(B)(iv)(VI), 1189(a)(2)(C); 18 U.S.C. § 2339(B).

[51] 8 U.S.C. § 1189(a)(4)(C).

[52] *Id.* § 1189(a)(3).

[53] In addition, if the designated organization has previously filed a petition, the petition period begins two years after the date of the determination of the previous petition. *Id.* § 1189(a)(4)(B).

[54] 18 U.S.C. § 2339B(a)(1). "Terrorism" in this section is defined as it is in Section 140(d)(2) of the Foreign Relations Authorization Act for Fiscal Years 1988 and 1989. The term "terrorism" means "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."

designation is effective for purposes of applying penalties to individuals who supply material support or resources to an FTO upon publication in the Federal Register.[55] The ODNI reports that this authority applies to foreign RMVEs "on the same terms" as other terrorist organizations.[56] There are no foreign RMVE groups currently designated as FTOs.[57]

Executive Orders 13224, 13372, and 13886; 31 C.F.R. § 594, 21 C.F.R. § 596, and 31 C.F.R. § 597

Executive Order 13224 and related authorities establish another mechanism for designating terrorists, including the foreign RMVE threat.[58] Under E.O. 13224, the Secretaries of State and the Treasury, in consultation with each other and the Attorney General, may designate foreign individuals or entities determined to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States.[59] In addition, E.Os. 13224 and 13886 permit designation of persons found to be owned, controlled, directed by, acting for, or providing material support for any designated individuals.[60] Those persons are designated as Specially Designated Global Terrorists (SDGTs) and added to the list of Specially Designated Nationals and Blocked Persons with the SDGT identifier.[61]

In addition, the Terrorism List Governments Sanctions Regulations under the Code of Federal Regulations (C.F.R.) prohibits U.S. persons from engaging in any financial transactions with the government of a country that is designated as supporting international terrorism.[62] The Foreign Terrorist Organizations Sanctions Regulations directs U.S. financial institutions that receive notice from the Secretary of the Treasury to block all financial transactions involving any assets of designated terrorist organizations.[63] Once the State Department designates an individual or entity as an SDGT, Treasury can make its own SDGT designation of certain individuals or

[55] 8 U.S.C. § 1189(a)(2)(B).

[56] Intelligence Report, *supra* note 2, at 6.

[57] *Id.*

[58] Section 824 of the Intelligence Authorization Act for 2022 also authorized the ODNI to examine Executive Order 13372, which modified Executive Order 13224, but this Order will not be described further in this Report.

[59] Exec. Order No. 13224; 3 C.F.R. § 13224 (2001).

[60] Exec. Order No. 13886, 84 Fed. Reg. 48041, § 1(a)(iii) (Sept. 12, 2019); Exec. Order No. 13224, as amended by Exec. Order No. 13886.

[61] 31 C.F.R. §§ 594.201(a), 594.310.

[62] 31 C.F.R. § 596.201 (1996).

[63] 31 C.F.R. § 597.201 (1997).

entities associated with or providing support to the person designated by the State Department under E.O. 13224.[64] Designations are published in the Federal Register.[65]

The Departments of State and Treasury have designated three foreign RMVE groups (and individuals associated with those groups) as SDGTs. In 2020, the State Department designated the Russian Imperial Movement (RIM) and three of its leaders (foreign RMVEs) as SDGTs due to the group's provision of "paramilitary-style training to neo-Nazis and white supremacists," and its "prominent role in trying to rally like-minded Europeans and Americans into a common front against their perceived enemies."[66] Treasury followed in 2022, implementing the Department of State's designations.[67] In 2024, the Department of State designated the Nordic Resistance Movement and three of its members as SDGTs, and the Department of Treasury added the group to their Specially Designated Nationals and Blocked Persons (SDN List) list.[68] According to the State Department, the Nordic Resistance Movement "is the largest neo-Nazi group in Sweden," and its "violent activity is based on its openly racist, anti-immigrant, antisemitic, [and] anti-LGBTQI+ platform."[69] On January 13, 2025, the State Department published a "Fact Sheet" announcing that it had designated The Terrorgram Collective and three of its leaders as SDGTs pursuant to E.O. 13224, as amended. The State Department stated that "Terrorgram" is a transnational group that "promotes violent white supremacism, solicits attacks on perceived adversaries, and provides guidance and instructional materials on tactics, methods, and targets

[64] Exec. Order No. 13886 § 1(a)(iii); Exec. Order No. 13224, as amended by Exec. Order No. 13886; see also *Combating Terrorism: Foreign Terrorist Organization Designation Process and U.S. Agency Enforcement Actions*, *supra* note 47, at 4.

[65] 31 C.F.R. § 594.201 note 2 (2003); *see also* U.S. Dep't of Treasury, *Privacy and Civil Liberties Impact Assessment for the Treasury Office of Foreign Assets Control (OFAC) System (TOS)*, at 2 (Dec. 2021), https://home.treasury.gov/system/files/236/PCLIA-Treasury-Office-of-Foreign-Assets-Control-OFAC-System-TOS-for508-R.pdf.

[66] U.S. Dep't of State, *Designation of Russian Imperial Movement* (Apr. 2020), https://2017-2021.state.gov/designation-of-the-russian-imperial-movement/.

[67] U.S. Dep't of Treasury, *U.S. Sanctions Members of Russian Violent Extremist Group* (June 2022), https://home.treasury.gov/news/press-releases/jy0817.

[68] U.S. Dep't of State, *Terrorist Designations of Nordic Resistance Movement and Three Leaders* (June 2024), https://www.state.gov/terrorist-designations-of-nordic-resistance-movement-and-three-leaders/; U.S. Dep't of Treasury, *Counter Terrorism Designations; West Bank-related Designation; Issuance of Amended Frequently Asked Questions* (June 2024), https://ofac.treasury.gov/recent-actions/20240614.

[69] U.S. Dep't of State, *Terrorist Designations of Nordic Resistance Movement and Three Leaders*, *supra* note 68.

for attacks, including on critical infrastructure and government officials."[70] Treasury designated these entities on the same day.[71]

1. *Privacy and Civil Liberties Protections for U.S. Persons*

Treasury's Office of Foreign Asset Controls (OFAC) has not published a detailed SDGT process,[72] but publicly available information reveals few instances in which U.S. persons or entities were designated as an SDGT.[73] OFAC directs persons to check its List of Specially Designated Nationals and Blocked Persons List (SDN List) to determine if a person or organization has been designated.[74] In order to request removal from the OFAC Sanctions list, a person or organization must submit a written request to OFAC by email.[75]

[70] U.S. Dep't of State, *Terrorist Designations of The Terrorgram Collective and Three Leaders* (Jan. 2025), https://www.state.gov/office-of-the-spokesperson/releases/2025/01/terrorist-designations-of-the-terrorgram-collective-and-three-leaders.

[71] U.S. Dep't of Treasury, *Counter Terrorism Designations; Venezuela-related and Counter Narcotics Designation Removals; Publication of OFAC/OFSI Memorandum of Understanding* (Jan. 2025), https://ofac.treasury.gov/recent-actions/20250113.

[72] Treasury advises that it follows a thorough investigation by OFAC investigators and a review of the totality of information. Its findings and conclusions are documented in a formal evidentiary memorandum that sets out the evidence pertaining to a determination that the person meets one or more of the relevant legal criteria for designation, Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Filing a Petition for Removal from an OFAC List*, https://ofac.treasury.gov/specially-designated-nationals-list-sdn-list/filing-a-petition-for-removal-from-an-ofac-list (last visited Dec. 10, 2024).

[73] The Board did not, however, perform a comprehensive review of SDGT designations or the number of instances in which this has occurred historically. *See* Daniel Meagher, *Caught in the Economic Crosshairs: Secondary Sanctions, Blocking Regulations, and the American Sanctions Regime*, 89 Fordham L. Rev. 999 at 1028 (2020) ("In their current state, OFAC's procedures lack sufficient transparency … to allow for sufficient judicial review and appeal by materially harmed parties."); Louisa Slocum, *OFAC, The Department of State, and The Terrorist Designation Process: A Comparative Analysis of Agency Discretion*, 65 Admin. L. Rev. 387 at 410-11 (2013), https://www.administrativelawreview.org/wp-content/uploads/2014/04/OPAC-The-Department-of-State-and-the-Terrorist-Designation-Process-A-Comparative-Analysis-of-Agency-Discretion.pdf ("OFAC has promulgated its own regulations detailing how it manages the blocked assets of both SDGTs and FTOs. … Notably, the regulations do not provide any guidance on how OFAC actually makes its designation or asset-freezing decisions."). OFAC's Privacy and Civil Liberties Impact Assessment (PCLIA) currently provides only a general description of Treasury's overall designation process (not solely for SDGTs) at a "high level." The process includes identifying targets under one or more of the various OFAC sanctions programs, researching the basis for designation/identification as well as publicly releasable identifiers, and putting together an evidentiary package, which goes through legal review. A blocking memo and Federal Register notice are created and signed off on (usually by the Director of OFAC), and the targets are added to one or more of OFAC's public sanctions lists. The PCLIA covers systems that OFAC uses for designations. *Privacy and Civil Liberties Impact Assessment for the Treasury Office of Foreign Assets Control (OFAC) System (TOS)*, *supra* note 65, at 2. In addition to the PCLIA, Treasury directed the Board to OFAC's counterterrorism sanctions page and sanctions list service available on OFAC's website. *See* Email to PCLOB Staff from Treasury Dep't (July 19, 2024).

[74] *See* Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Afghanistan-Related Sanctions*, https://ofac.treasury.gov/faqs/952 (last visited Dec. 10, 2024).

[75] 31 C.F.R. § 501.807(a) (2024); *see also* Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Filing a Petition for Removal from an OFAC List*, *supra* note 72.

2. *Potential Privacy and Civil Liberties Impacts to U.S. Persons*

The impact of the government's FTO and SDGT designation authorities on U.S. persons' privacy and civil liberties is limited by the fact that these authorities are mostly foreign-facing and, as such, Americans cannot be designated as FTOs. The number of U.S. persons designated as SDGTs is exceedingly low. Americans can nevertheless be charged with providing material support to designated terrorist organizations.[76]

a. Foreign Terrorist Organizations

U.S. persons and entities cannot be designated as FTOs, but U.S. person information could be relevant to an FTO designation process.[77] However, as referenced above, a person in the United States—or subject to the jurisdiction of the United States—who knowingly provides "material support or resources" to a designated FTO can be criminally prosecuted, fined, or subjected to civil forfeiture penalties.[78] A designation is effective for purposes of applying penalties to an FTO, or to individuals who provide material support or resources to an FTO, upon publication in the Federal Register.[79] Any financial institution that becomes aware that it has possession or control over funds in which the designated FTO or its agent has an interest must retain possession or control over the funds and report the funds to OFAC.[80]

There have been cases in which Americans have been convicted for material support to an FTO notwithstanding their assertions that they were supporting what they believed to be a lawful charity.[81] The Supreme Court has held that the material support statute may be applied to prohibit training, expert advice, and other non-tangible services unconnected to FTOs' unlawful, violent actions.[82] NGOs have argued that the material support statute constrains humanitarian aid. OFAC has, however, recently instituted a program to authorize general licenses "to ensur[e] that humanitarian assistance and related trade continues to reach at-risk populations through legitimate

[76] As discussed below, Americans can be civilly fined or criminally prosecuted for providing "material support" to FTOs, but the risk is mitigated by the government's obligations to prove that a defendant who provided material support had the requisite knowledge. 18 U.S.C. § 2339B. To be prosecuted for a crime of providing material support to a SDGT, the person must be found to have "willfully" supported a terrorist organization. 50 U.S.C. § 1705(c).

[77] For instance, the State Department advised PCLOB that U.S. person information could be used in determining whether an organization is foreign or domestic. PCLOB Team Notes from Meeting with the State Dep't (Mar. 20, 2024).

[78] 8 U.S.C. § 2339(B)(a)-(c).

[79] *Id.* § 1189(a)(2)(B), (a)(4).

[80] *Id.* § 2339(B); 31 C.F.R. § 597.201.

[81] *See* U.S. Dep't of Just., *Federal Judge Hands Downs Sentences in Holy Land Foundation Case* (May 2009), https://www.justice.gov/opa/pr/federal-judge-hands-downs-sentences-holy-land-foundation-case; Jeff Breinholt, *Terrorist Financing*, 51 J. FED. L. & PRAC. 1, 14 (2003).

[82] *Humanitarian Law Project v. Holder*, 561 U.S. 1 (2010) (finding that the material support statute was not impermissibly vague under the Fifth Amendment and that application of the statute to such training and advice activities does not violate the First Amendment).

and transparent channels, while maintaining the effective use of targeted sanctions, which remain an essential foreign policy tool."[83]

b. Specially Designated Global Terrorists

The State Department is prohibited from designating U.S. persons and organizations as SDGTs, but Treasury can.[84] An SDGT designation entails extensive financial restriction on the designee.[85] All property and interests in property of designated individuals or entities that are in the United States, that come within the United States, or that come within the possession or control of U.S. persons are blocked.[86] Any transaction or dealing by U.S. persons or within the United States in blocked property or interests in property is prohibited, including but not limited to the making or receiving of any contribution of funds, goods, or services to or for the benefit of designated individuals or entities.[87] For persons designated pursuant to E.O. 13224, as amended, pre-designation notice is not given due to the potential for designated persons to transfer funds prior to the blocking of their assets by Treasury.[88] Neither the State Department, Treasury, nor another government agency has published a report detailing the SDGT designation process, or the extent to which Treasury considers input, including U.S. person information, from other agencies. Treasury has published information generally explaining the designation process,[89] including that Treasury considers input from other agencies prior to making a final determination to add a person to the SDN List, consistent with applicable executive orders.[90]

---

[83] U.S. Dep't of Treasury, *Treasury Implements Historic Humanitarian Sanctions Exceptions* (Dec. 2022), https://home.treasury.gov/news/press-releases/jy1175.

[84] Exec. Order No. 13886 § 1(a)(iii); Exec. Order No. 13224, as amended by Exec. Order No. 13886.

[85] *See OFAC, The Department of State, and The Terrorist Designation Process: A Comparative Analysis of Agency Discretion*, *supra* note 73, at 399 ("Once designated as an SDGT, an entity cannot access any of its property or money located within the United States or its financial institutions.").

[86] Exec. Order No. 13224; 3 C.F.R. § 13224 (2001), § 1.

[87] *Id.* § 2.

[88] *Id.* § 10.

[89] OFAC's website explains, "In making a listing determination, OFAC considers information from many sources, including but not limited to relevant U.S. government agencies, foreign governments, United Nations expert panels, and press and other open-source reporting. OFAC investigators then carry out a thorough investigation, including a review of the totality of the information. The findings and conclusion of that investigation are then documented in a formal evidentiary memorandum that sets out the evidence pertaining to a determination that the person meets one or more of the criteria specified in the sanctions authority. Before OFAC's final determination is made, proposed listing actions are subjected to review by the Departments of the Treasury, Justice, State, and other U.S. agencies as warranted." Off. of Foreign Assets Control, U.S. Dep't of Treasury, *Filing a Petition for Removal from an OFAC List*, *supra* note 72.

[90] Treasury advised that OFAC does provide information about its designation process generally, which applies to SDGT designations, and that its designation process does "account for an assessment of whether a designation implicates the interests of a U.S. person." *See* Exec. Order No. 13886, 84 Fed. Reg. 48041, § 1(a)(iii) (Sept. 12, 2019) (requiring that the Secretary of the Treasury consult with the Secretary of State, the Secretary of Homeland Security, and the Attorney General, prior to making any sanctions determination pursuant to that authority).

D. Travel and Immigration-Related Vetting

National Security Presidential Memorandum-9

Issued by President Trump in 2018, National Security Presidential Memorandum-9 (NSPM-9) directed the establishment of a National Vetting Center (NVC), a multi-agency undertaking led by DHS. The NVC is intended to coordinate government vetting efforts (procedures to evaluate an individual's suitability for travel or immigration to the United States) in order to identify individuals who may pose a threat to national security, border security, homeland security, or public safety.[91] Since 2018, the NVC has provided support to various immigration and border security programs, including the Electronic System for Travel Authorization, Enduring Welcome, Refugee Admissions Program, Uniting for Ukraine, Non-Immigrant Visas, Venezuela Migration Enforcement Process,[92] and the general U.S. Asylum Program.[93]

NVC does not own or control the information that is used in the vetting process, nor does it create or consolidate new information or databases.[94] Rather, its role is limited to that of facilitator or service provider for the NVC process and technology used for vetting.[95] Data continues to be owned and controlled by the agencies (including intelligence agencies) involved in the vetting process and is maintained under their authorities.[96] Intelligence agencies do not make any adjudicative travel or immigration-related decisions.[97] The collection of data that is accessed for adjudicating travel or immigration decisions must have been authorized by federal law, including E.O. 12333, and other authorities governing the intelligence agencies' collection, dissemination, and retention of U.S. person information.[98]

[91] NVC focuses on security adjudications for individuals who (1) seek a visa waiver or other immigration benefit, or protected status; (2) attempt to enter the United States; or (3) are subject to an immigration removal proceeding. The White House, *National Security Presidential Memorandum-9 (NSPM-9), Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise*, at 4, 6 (Aug. 2018) [hereinafter NVC Implementation Plan].

[92] U.S. Customs and Border Prot., *National Vetting Center*, https://www.cbp.gov/border-security/ports-entry/national-vetting-center (last visited Dec. 5, 2024).

[93] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the National Vetting Center, DHS/ALL/PIA-072*, at 88-98 (Apr. 2023) [hereinafter NVC PIA].

[94] *Id.*; NVC Implementation Plan, *supra* note 91, at 7.

[95] NVC PIA, *supra* note 93, at 3.

[96] NVC Implementation Plan, *supra* note 91, at 7.

[97] NVC PIA, *supra* note 93, at 3.

[98] *Id.*

Individuals affiliated with foreign RMVE groups, including RIM, have reportedly traveled to the United States for recruitment and other purposes.[99] As such, NVC vetting can play a role in U.S. government efforts to identify and address potential cross-border foreign RMVE threats. However, the ODNI reports that screening and vetting through the NVC does not, in itself, address the threat posed by loose affiliations of individuals, including U.S. persons, who have mere associations with foreign RMVE actors (as opposed to individuals for whom the government also has particularized derogatory information regarding, for example, their association with terrorism or terrorist activities).[100]

1. *Privacy and Civil Liberties Protections for U.S. Persons*

The NVC and the vetting programs that utilize its process and technology are subject to a range of privacy and civil liberties protections. NVC is managed under the oversight of the National Vetting Governance Board (NVGB), the agency forum created by NSPM-9 and composed of senior executives appointed by the Secretary of DHS, the Secretary of State, the Attorney General, the Secretary of Defense, the DNI, and the Director of the CIA.[101] The NVGB provides guidance to the national vetting enterprise and oversees NVC activities to ensure that they comply with applicable law and to ensure that NVC conducts its activities in a manner that appropriately protects privacy, civil rights, and civil liberties.[102] The NVC is supported by a Privacy, Civil Rights, and Civil Liberties Officer, who is an *ex officio* member of the NVGB that is directed to, among other things, ensure that the use of technologies "sustain, not erode, privacy protections relating to the use, collection, and disclosure of personally identifiable information."[103]

2. *Potential Privacy and Civil Liberties Impacts to U.S. Persons*

Some details of the privacy and civil liberties protections applicable to the NVC and related vetting programs are not publicly available. The precise terms and conditions for the use, sharing, and protection of NVC vetting data is established by interagency information sharing agreements,

[99] U.S. Embassy in Georgia, *On the U.S. Designation of the Russian Imperial Movement and its Leaders as Global Terrorists* (Apr. 2020), https://ge.usembassy.gov/briefing-with-coordinator-for-counterterrorism-amb-sales-on-the-u-s-designation-of-russian-imperial-movement-and-its-leaders-as-global-terrorists/.

[100] Intelligence Report, *supra* note 2, at 8-9. In its Intelligence Report, the ODNI associated vetting with terrorist watchlisting, stating that "Screening and vetting under NSPM-9 pose the same implications . . . as it pertains to watchlisting individuals associated with foreign REMVE groups." The Board is reviewing the policies concerning the terrorist watchlist, examining, among other things, the standards for placing individuals on the watchlist and the procedures followed to add and remove individuals. U.S. Priv. & C.L. Oversight Bd., *Oversight Projects*, https://www.pclob.gov/OversightProjects (last visited Dec. 5, 2024).

[101] NVC Implementation Plan, *supra* note 91, at 15.

[102] *Id*. at 16. Two working groups—the Legal Working Group and the Privacy, Civil Rights, and Civil Liberties Working Group—assist with this oversight.

[103] *Id*.

which are not publicly available, and by the NVC Concept of Operations (CONOP), which is classified.[104]

Several NVC-supported programs collect and maintain records provided by travelers, which may include information about U.S. persons. For example, the Electronic System for Travel Authorization (ESTA)—an "automated system" administered by U.S. Customs and Border Protection (CBP) "that determines the eligibility of visitors to travel to the United States under the Visa Waiver Program"—collects and maintains records of U.S. persons whose information is provided in travelers' ESTA applications. [105] These records include, at a minimum, the names, addresses, and phone numbers of travelers' U.S. points of contact, which travelers are required to provide as part of their application.[106]

NVC-supported vetting programs may also collect, access, and/or retain additional U.S. person information during the vetting process itself. This could occur in several ways. First, NVC-supported adjudicating agencies may request and receive additional U.S. person information from vetting support agencies. For example, CBP may request additional information from other agencies—potentially including intelligence agencies—concerning ESTA applicants' U.S. points of contact for use in "counterterrorism-related vetting."[107]

Second, although some vetting processes are required to stop if the applicant becomes a U.S. person,[108] adjudicating agencies may mistakenly subject a traveler to vetting after they become a U.S. citizen or lawful permanent resident. This was the case, for example, when an error in a State Department system resulted in the State Department mistakenly requesting NSA to vet 498 travel applications submitted by lawful permanent residents between November 2020 and January 2023.[109]

---

[104] NVC PIA, *supra* note 93, at 30-31, 34, 67-69.

[105] U.S. Customs and Border Prot., *Electronic System for Travel Authorization*, https://www.cbp.gov/travel/international-visitors/esta (last visited Dec. 5, 2024).

[106] U.S. Customs and Border Prot., *Official ESTA Application*, https://esta.cbp.dhs.gov/ (last visited Dec. 5, 2024).

[107] NVC PIA, *supra* note 93, at 31-32.

[108] In the context of the DHS Continuous Immigration Vetting effort, for example, "ATS stops vetting when it receives a message from ATLAS based on a certificate of naturalization issuance. CBP is required to return an acknowledgment of receipt of such notification as well as a 'stopped CIV' indicator. With the exception of limited data such as unique system identifiers needed to support auditing capabilities, CBP will not retain this data in ATS after the issuance of the naturalization certificate unless the data is linked to active law enforcement lookout records, enforcement activities, or investigations or cases." U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Continuous Immigration Vetting, DHS/USCIS/PIA-076*, at 8 (Feb. 2019), https://www.dhs.gov/sites/default/files/publications/pia-uscis-fdnsciv-february2019_0.pdf.

[109] Memorandum Opinion and Order, at 51, *In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications*, Docket No. 702(j)-23-01 and predecessor dockets, In re DNI/AG 702(h) Certification 2023-B and its Predecessor Certifications, Docket No. 702(j)-23-02 and predecessor dockets, *In re DNI/AG 702(h) Certification 2023-C and its Predecessor Certifications*, Docket No. 702(j)-23-03 and predecessor dockets (FISA Ct. Apr. 11, 2023).

Third, NVC-supported programs that conduct social media checks to vet persons for travel or immigration to the United States may collect and retain social media content from U.S. persons if U.S. persons communicated with the applicant. At least two NVC-supported programs conduct social media checks as part of their vetting processes: the ESTA program[110] and the U.S. Refugee Admission Program.[111] DHS has acknowledged that, at least with respect to the ESTA program, content from U.S. citizens that appears in the applicant's social media profile may be collected during the vetting process.[112] DHS has also acknowledged that, "through link-analysis," CBP may identify "direct," "secondary," or "tertiary contacts associated with the applicant that pose a potential risk to the homeland or demonstrate a nefarious affiliation on the part of the applicant," and that "information related to each of these contacts may be retained" by DHS "and used as part of the vetting process."[113]

Fourth, NVC-supported vetting programs may review U.S. person information incidentally collected under Section 702 of the Foreign Intelligence Surveillance Act (FISA). On April 20, 2024, Congress renewed FISA Section 702 and included in its reauthorization a provision requiring the Attorney General and the DNI to ensure that FISA procedures enable the vetting of all non-U.S. persons who are being processed for travel to the United States, using terms that do not qualify as U.S. person query terms under Section 702. To the extent this results in increased queries of Section 702-derived data, it may increase the likelihood that U.S. person information incidentally collected under Section 702 is reviewed.[114]

[110] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment Update for the Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-007(g)*, at 2 (Sept. 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-september2016.pdf.

[111] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Refugee Case Processing and Security Vetting, DHS/USCIS/PIA-068*, at 7 (July 2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf.

[112] *Privacy Impact Assessment Update for the Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-007(g), supra* note 110, at 3.

[113] *Id.* at 5.

[114] For a detailed discussion of the privacy and civil liberties protections and risks associated with the Section 702 program, *see* U.S. Priv. & C.L. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2023), https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf.

III. RECOMMENDATIONS

As referenced above, Section 824(b)(1)-(2) of the IAA called for the ODNI to include in its Intelligence Report an assessment of whether (and if so, to what extent and why) the federal laws, regulations, and policies discussed herein are sufficient to counter foreign RMVE threats, including a description of any gaps and specific examples to illustrate such gaps, and recommendations regarding how to remedy such gaps. The ODNI did not identify any legal gaps.[115] Thus, there are no recommendations for new or expanded authorities for which PCLOB needs to assess the privacy and civil liberties impacts. Although, as noted above, the Board's review is limited and is not designed to cover each relevant agency's day-to-day implementation of the many applicable privacy and civil liberties safeguards in place, it has made recommendations where greater transparency might yield information that could help facilitate future assessments of privacy and civil liberties impacts from the government's use of the authorities discussed herein to counter foreign RMVE threats.

Given the scope and nature of this report, PCLOB does not include recommendations related to all of the authorities discussed above. For example, as described above, PCLOB has previously conducted oversight of counterterrorism activities conducted under E.O. 12333 and will likely conduct further oversight of such activities in the future. With regard to the process for designating Specially Designated Global Terrorists (SDGTs), the Board will consider whether to conduct further research and examination of this process, including the extent to which it may be appropriate that there be additional transparency regarding the designation process.

The Board's recommendations regarding mitigating potential privacy and civil liberties impacts associated with specific, existing, legal authorities are below.

[115] As indicated above, the ODNI stated that it was focused on, and recommended increasing, relevant information sharing regarding the foreign RMVE threat among federal, state, and local authorities, the private sector, tribal, and foreign partners. Intelligence Report, *supra* note 2, at 9.

RECOMMENDATION 1:

Congress should clarify which federal official has authority to both designate and appoint a program manager (PM) for the information sharing environment (ISE) and, in the interim, ODNI should clarify how the PM role is being fulfilled.

The IC has, through statute, executive orders, and internal guidelines, instituted a variety of privacy and civil liberties protections governing its collection, use, and dissemination of U.S. person information with respect to countering foreign RMVE threats under the enumerated legal authorities that the Board reviewed. Some such protections were installed in the ISE, which, according to GAO, has nearly been fully implemented.[116] However, the PM position remains vacant and, according to GAO, efforts to name a new PM have been complicated by conflicting statutory provisions.[117] Congress should clarify which federal official can designate and appoint a PM. Moreover, although members of the IC have reported to PCLOB that the ISE and information sharing continue under multiple authorities, including the ODNI Attorney General Guidelines concerning U.S. person information and the NCTC Implementation Procedures, in the interim, the ODNI should publicly clarify how the role is being fulfilled. Specifically, ODNI should clarify the means through which NCTC or any other government entities are supporting the statutorily-mandated ISE and the related protection of U.S. person information. The ODNI should clarify the position or department at NCTC that is responsible for fulfilling the PM functions.

RECOMMENDATION 2:

Congress should demand ODNI recommence filing statutorily required annual reports on the performance of the ISE.

Section 1016(h) of IRTPA requires the President to issue annual reports to Congress on the state of the ISE and information sharing across the government, including "an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections." Formerly, the PM issued these reports. In the absence of a PM, the ODNI issued annual reports through 2019, but has ceased doing so. Given the ISE's important focus on privacy and civil liberties, Congress should demand ODNI recommence filing annual reports to Congress on the performance of the ISE, as is already required by statute.

[116] At the start of 2017, thirteen of sixteen of the ISE implementation plan's priority objectives had been met. *Action Needed to Further Develop the Information Sharing Environment*, *supra* note 38, at 24.

[117] *Id.* at 16. The conflicting provisions are the Intelligence Authorization Act for Fiscal Year 2021, Pub. L. No. 116-260, div. W, tit. III, subtit. A, § 307, 134 Stat. 2361, 2368 (2020); Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. No. 116-92, div. E, subdiv. 2, tit. LXIV, subtit. A § 6402(a)-(b), 133 Stat. 2111, 2196 (2019); IRTPA § 1016(b)(f)(1).