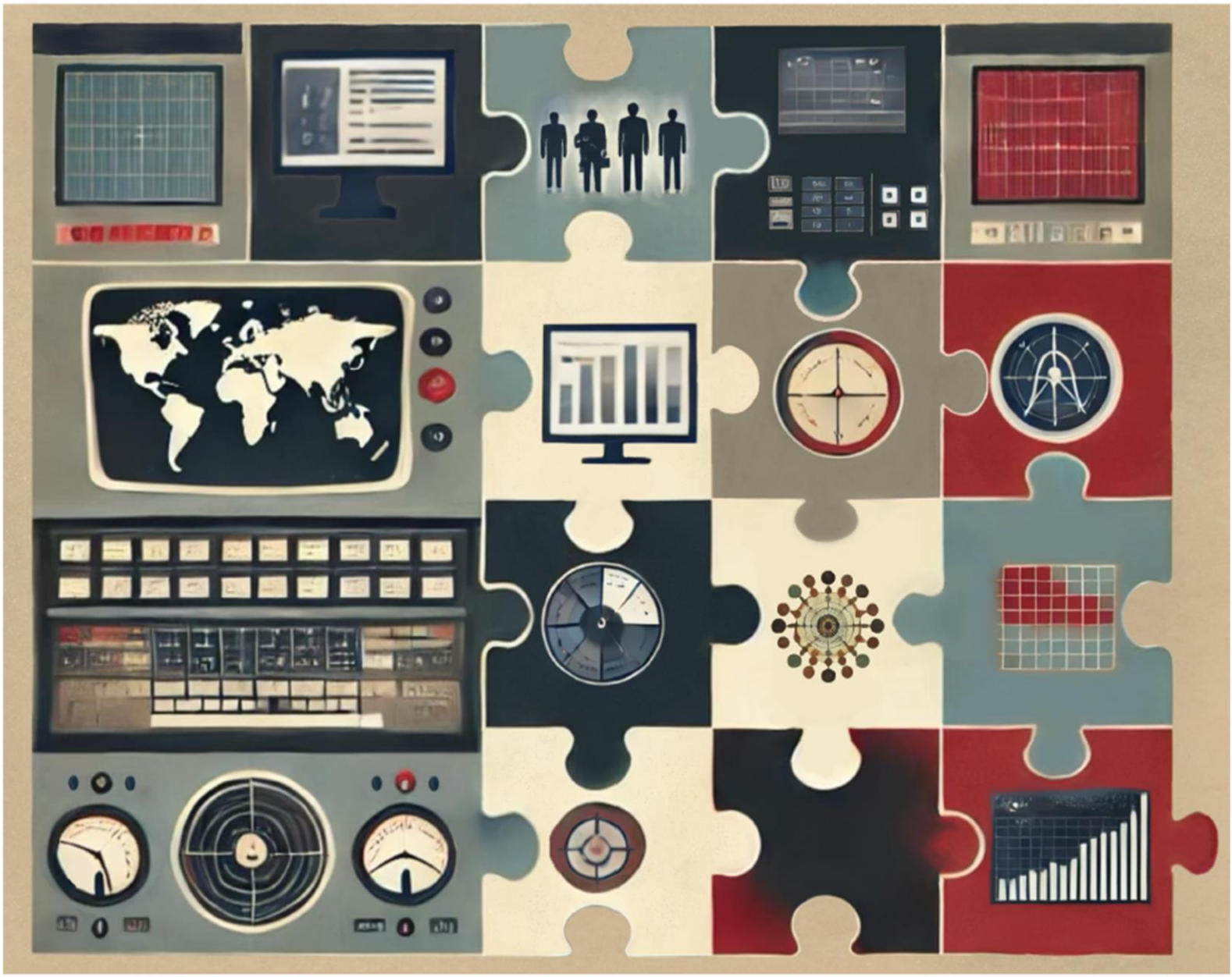
THE

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD



REPORT ON

THE NATIONAL COUNTERTERRORISM CENTER

December 10, 2024

[THIS PAGE INTENTIONALLY LEFT BLANK]

THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

REPORT ON THE NATIONAL COUNTERTERRORISM CENTER

DECEMBER 10, 2024

The Privacy and Civil Liberties Oversight Board

Sharon Bradford Franklin, Board Chair

Edward W. Felten, Board Member

Travis LeBlanc, Board Member

Beth A. Williams, Board Member

The Board acknowledges with gratitude the staff members who worked on this project, including Jennifer Fitzpatrick, Lindsay Kennedy, Annan Mortensen, Alexa Potter, Saleela Salahuddin, John Tran, and other current and former staff members.

TABLE OF CONTENTS

I. BACKGROUND

A. The Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board (PCLOB or Board) is an independent agency within the executive branch, established by the Implementing Recommendations of the 9/11 Commission Act of 2007.[1] The bipartisan Board is appointed by the President and confirmed by the Senate. The PCLOB's mission is to conduct oversight and provide advice to ensure that efforts by the executive branch to protect the nation from terrorism are appropriately balanced with the need to protect privacy and civil liberties.

B. The National Counterterrorism Center

After the 9/11 attacks, the United States government reorganized and restructured the Intelligence Community (IC) to protect and secure the nation against terrorist attacks. As part of this reorganization, the government created the National Counterterrorism Center (NCTC) within the Office of the Director of National Intelligence (ODNI) to lead the nation's effort to protect the United States from terrorism by integrating, analyzing, and sharing information to drive whole-of-government action and achieve the nation's counterterrorism objectives. NCTC's principal roles, missions, and responsibilities include serving as the primary organization for analyzing and integrating all intelligence possessed or acquired by the U.S. government pertaining to terrorism, except for intelligence pertaining exclusively to domestic terrorism; conducting strategic operational planning for counterterrorism activities; ensuring agencies receive, as appropriate, all-source intelligence support and intelligence needed to accomplish their counterterrorism missions; and maintaining an authoritative U.S. government database of known and suspected international terrorists. NCTC asserts it is authorized to access all terrorism-related information held by the U.S. government and its authorities to "bridge the divide between foreign and domestic intelligence, thereby allowing [NCTC] to bring a whole-of-government approach to [its] mission area[s]," including threat analysis, identity management, information sharing, strategic operational planning, and national intelligence management.[2]

[1] Pub. L. No. 110–53, § 801, 121 Stat. 266, 352 (2007).
[2] Nat'l Counterterrorism Ctr., *How We Work*, https://www.dni.gov/index.php/nctc-how-we-work/overview (last visited Dec. 3, 2024).

C. Commencement of NCTC Oversight Project

In January 2017, the Board voted to review the implementation of the 2012 Attorney General-approved "Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information" (2012 NCTC Guidelines). Specifically, the 2012 NCTC Guidelines were designed to govern the access, retention, use, and dissemination by NCTC of terrorism information contained within datasets maintained within other departments and agencies that include "non-terrorism information."[3] The Board approved this project to assess whether NCTC's practices under these Guidelines, including information sharing, appropriately balance privacy and civil liberty interests with national security interests relating to counterterrorism. This project was designed to cover NCTC's replication, access, retention, use, search, dissemination, and purging, in accordance with the 2012 NCTC Guidelines, of datasets originating in other executive departments or agencies that include non-terrorism information.[4]

Shortly after the Board's vote to initiate the NCTC oversight project, the Board entered a 20-month period in which the Board did not have a quorum of Senate-confirmed members. During this sub-quorum period, staff began conducting the review authorized by the Board, including briefings with NCTC officials, follow-up questions, and further engagement with NCTC officials.

D. PCLOB Advice on ODNI Attorney General-Approved Procedures and Update of Oversight Project

In June 2018, the Chief of ODNI's Office of Civil Liberties, Privacy, and Transparency (ODNI CLPT) alerted the Board that work was underway on ODNI Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333 (ODNI AG Guidelines) which, once completed, would apply to all ODNI components, including NCTC, and supersede the 2012 NCTC Guidelines on which the NCTC oversight project was originally focused.[5] Accordingly, staff suspended the oversight investigation of the 2012 NCTC Guidelines and instead began work to enable PCLOB to provide advice on the draft ODNI AG Guidelines.

When the Board regained a quorum in 2018, it voted formally to accept ODNI's request for PCLOB's advice regarding the ODNI AG Guidelines, and in 2019 it voted formally to amend the NCTC oversight project description. The new project description states, "The Board's review will

[3] Nat'l Counterterrorism Ctr., GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION (2012), § I.C [hereinafter 2012 NCTC Guidelines]. Pursuant to Executive Order 12333 § 2.3, agencies within the IC are only authorized to collect, retain, or disseminate U.S. person information in accordance with procedures established by the head of the agency and approved by the Attorney General.

[4] PCLOB NCTC Project Description (2017).

[5] At the time, ODNI operated under two sets of Attorney General-approved procedures: (1) the 2012 NCTC Guidelines for certain NCTC activities; and (2) the Central Intelligence Agency's Guidelines for all other ODNI activities related to U.S. person information, issued in 2017.

consider NCTC's current policies and practices as well as procedures currently being drafted by the [ODNI] pursuant to Executive Order 12333. The Board's review of NCTC's activities pursuant to the forthcoming [ODNI AG Guidelines] will also consider any NCTC-specific implementing guidance."[6]

The Board provided advice on the ODNI AG Guidelines in December 2019 but held the NCTC oversight project in abeyance while NCTC worked to develop NCTC-specific implementing procedures for the new ODNI AG Guidelines. The Attorney General signed the ODNI AG Guidelines on December 23, 2020, and they took effect on March 23, 2021. On March 22, 2021, the Acting Director of NCTC approved the "National Counterterrorism Center Implementation Procedures for the ODNI Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333" (NCTC Implementation Procedures). These NCTC Implementation Procedures (1) implement the NCTC-specific provision in Section 3.3 of the ODNI AG Guidelines pertaining to the additional collection authority of NCTC and (2) provide internal guidance to NCTC employees regarding NCTC application of certain aspects of the ODNI AG Guidelines to NCTC intelligence activities.[7] Thereafter, the PCLOB resumed this oversight project.

[6] PCLOB NCTC Project Description, amended February 2019.
[7] Nat'l Counterterrorism Ctr., IMPLEMENTATION PROCEDURES FOR THE ODNI INTELLIGENCE ACTIVITIES PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 (2021), § 1.A [hereinafter NCTC Implementation Procedures].

II. FACTUAL SUMMARY

A. Evolution of the Guidelines Governing NCTC

Under Executive Order 12333, IC elements are required to have guidelines approved by the head of the IC element and the Attorney General, in consultation with the Director of National Intelligence (DNI), for the collection, retention, and dissemination of information concerning U.S. persons.[8] In 2008, the DNI and the Attorney General approved guidelines governing how NCTC identifies terrorism information in datasets that other federal agencies have already lawfully obtained pursuant to their own authorities and prescribing protections for the information to be shared with NCTC (2008 NCTC Guidelines). The 2008 NCTC Guidelines established three "tracks" for NCTC to access or acquire such information from other federal agencies. Under Track 1, NCTC analysts had account-based access to a relevant agency dataset, while under Track 2, NCTC submitted query terms for the providing agency to perform the search and return responsive information. Under Track 3, the agency dataset was replicated at NCTC so NCTC could use its analytic tools to identify terrorism information; if NCTC could not "promptly" identify terrorism information in the replicated dataset, the 2008 NCTC Guidelines required NCTC to "promptly remove" the information.[9] As implemented at NCTC, this generally required the removal of information within 180 days.[10]

In 2012, the DNI, the Attorney General, and the Director of NCTC approved updated NCTC Attorney General Guidelines (2012 NCTC Guidelines). These updated guidelines carried forward the same three-track framework from the 2008 NCTC Guidelines, while providing that datasets likely to contain significant terrorism information may be temporarily retained for up to five years. The 2012 NCTC Guidelines also added specificity on how data is obtained, retained, and disseminated, and provided for some additional safeguards and an oversight mechanism to protect important privacy and civil liberties interests through the information sharing lifecycle.

In 2016, the DNI instructed IC elements to work to harmonize their guidelines pertaining to retention and dissemination of U.S. persons information:

> Harmonized rules help to set the conditions for an integrated IC. Accordingly, elements' guidelines pertaining to retention and dissemination of U.S. persons information should be the same or similar. Provisions should differ only when required by law or executive order, or to address element-specific mission

[8] Exec. Order No. 12333, 46 F.R. 59941 (1981), § 2.3.
[9] Nat'l Counterterrorism Ctr., MEMORANDUM OF AGREEMENT BETWEEN THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE ON GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER OF TERRORISM INFORMATION CONTAINED WITHIN DATASETS IDENTIFIED AS INCLUDING NON-TERRORISM INFORMATION AND INFORMATION PERTAINING EXCLUSIVELY TO DOMESTIC TERRORISM (2008), §§ III.A.3, III.C [hereinafter 2008 NCTC Guidelines].
[10] ODNI CLPO, INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE UPDATED NCTC GUIDELINES, 1 (Jan. 2013).

requirements. In cases in which differences are necessary, elements should consider whether provisions can be drafted to limit the differences and reduce complexity.[11]

The result of this guidance was the establishment of the ODNI's own Attorney General Guidelines, discussed above.[12] In 2021, the ODNI released its first set of Attorney General-approved U.S. person procedures to apply to all ODNI directorates and centers (ODNI AG Guidelines). These guidelines follow other IC elements in focusing on whether data includes U.S. person information instead of how the data was acquired and are tailored to reflect the ODNI's mission and collection authorities, which are more limited than those of some other agencies. Previously, within ODNI, NCTC operated with respect to certain activities under its own set of Attorney General-approved procedures, while other aspects of ODNI applied the Central Intelligence Agency's Attorney General Guidelines. Because the ODNI AG Guidelines apply to all ODNI directorates and centers, the ODNI AG Guidelines rescind and supersede the prior 2012 NCTC Guidelines.

The ODNI AG Guidelines require NCTC to develop supplementary policies and procedures to address NCTC's additional collection authority established under Section 119 of the National Security Act of 1947, as amended.[13] As referenced above, NCTC accomplished this requirement through the release of its 2021 NCTC Implementation Procedures.

B. Key Updates in the ODNI AG Guidelines and NCTC Implementation Procedures

The ODNI AG Guidelines introduce key structural and substantive updates from the 2012 NCTC Guidelines. In particular, and as discussed below, the ODNI AG Guidelines and subordinate NCTC Implementation Procedures include a revised framework for interacting with datasets in furtherance of NCTC's mission, a framework for NCTC's activities related to its now-limited domestic counterterrorism work, and increased evaluation and retention periods for certain types of information to identify terrorism information within the unevaluated holdings. As further described below, in December 2022, Congress curtailed much of NCTC's domestic terrorism work.

1. *Rules Governing Data Acquisition & Handling*

The 2012 NCTC Guidelines, and the preceding 2008 NCTC Guidelines, among other things, established three "Tracks" for NCTC to access or acquire information from other federal agencies. Under Track 1, NCTC analysts were given accounts in other agencies' repositories to access datasets to determine whether they contain terrorism information, as defined in Section 1016 of

[11] Mem. from DNI James. R. Clapper for Distribution, ES 2016-00202, Intelligence Integration Principles for Executive Order 12333 Guidelines, 2 (April 18, 2016).
[12] Press Release, ODNI, ODNI Releases ODNI Attorney General Procedures for Conducting Intelligence Activities (Jan. 14, 2021).
[13] ODNI, INTELLIGENCE ACTIVITIES PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 (2020), § 3.3 [hereinafter ODNI AG Guidelines].

the Intelligence Reform and Terrorism Prevention Act.[14] Track 1 concerned account-based access to the datasets of data providers, to include NCTC analysts, which contained or may have contained terrorism information.[15] NCTC accessed information under Track 1 only to determine if the dataset contained terrorism information.[16] Track 2 concerned search and retention, where the owner of a dataset, not NCTC analysts, would conduct terrorism-related queries in data that may have contained terrorism information.[17] Under this Track 2 process, information from the dataset that was responsive to queries using NCTC-provided terrorism data points would be given to NCTC by the data provider.[18] Track 3 involved dataset acquisition where NCTC acquired and replicated portions or the entirety of a dataset to identify terrorism information within the dataset. Track 3 was only used after the Director of NCTC or a designee determined that a dataset was likely to contain significant terrorism information and that NCTC's authorized purposes could not effectively be served through Tracks 1 or 2.[19] Under Track 3, NCTC analysts directly accessed and queried the datasets subject to requirements established in the NCTC 2012 Guidelines and in applicable information sharing agreements.

The ODNI AG Guidelines and NCTC Implementation Procedures, however, replace these three tracks and introduce a different framework for handling data, aligned to procedures used by other elements of the IC. Under the ODNI AG Guidelines, NCTC may access, collect, or obtain, and continuously review, datasets maintained by other federal government departments and agencies that may constitute or contain terrorism information, datasets pertaining exclusively to domestic terrorism, and other information maintained by executive departments and agencies identified as including non-terrorism information.[20] NCTC accesses, collects, and obtains a variety of datasets, primarily from other departments and agencies, but also from commercial providers.[21] These include, but are not limited to, datasets that contain evaluated information and datasets that contain unevaluated information.[22]

[14] 2012 NCTC Guidelines § I.B, n.1.
[15] *Id.* §§ I.B., III.C.1.a.
[16] *Id.* § III.C.1.b.
[17] *Id.* § III.C.2.a.
[18] *Id.* § III.C.2.b.
[19] *Id.* § III.C.3.b.
[20] ODNI AG Guidelines § 3.3 ("NCTC shall develop policies and procedures to implement these authorities consistent with the other provisions of these Procedures. Such policies and procedures shall require NCTC, before collecting a new agency dataset, to document the reasons its needs cannot be fully met by accessing that dataset without collecting it. These policies and procedures shall be coordinated with the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer.").
[21] NCTC written responses (Nov. 10, 2021).
[22] *See* ODNI AG Guidelines § 10.20 ("Unevaluated information means information that has been collected or obtained, but that has not yet been determined to (1) relate to an authority and responsibility listed in Section 2; (2) contain any information concerning U.S. persons; and (3) meet the criteria for retention under Section 6.")

Within this new framework, NCTC data handling rules and procedures are specific to the method by which NCTC acquires the data. As a result, NCTC is governed by different rules depending on whether it collects, accesses, or obtains information from other departments and agencies to identify terrorism information. When NCTC collects information, it "[receives] information for official purposes, whether or not the information is retained."[23] All NCTC collection must:

(1) relate to an ODNI authority and responsibility;

(2) be done overtly or through publicly available sources; and

(3) either reasonably be believed to fall within at least one category listed in Subsection 3.1(c) of the ODNI AG Guidelines, contain terrorism information, or contain domestic counterterrorism intelligence.[24]

The ODNI AG Guidelines authorize NCTC to access "any information or intelligence possessed by another executive branch department or agency that is relevant to the national security or the DNI's responsibilities," except for information "excluded by law, by the President, or by the Attorney General acting under the direction of the President or guidelines agreed upon by the DNI."[25] NCTC accesses information when it "view[s] or examin[es] it for official purposes without storing or otherwise maintaining it under NCTC's control,"[26] such as by "copying or saving [the information] onto a local server or using or applying the information in some manner."[27] NCTC analysts may access information by reviewing the information on the data-holder agency's system; therefore, "accessing" is analogous to the NCTC activity under Track 1 in the 2008 and 2012 Guidelines. If NCTC collects or obtains some of the information it accesses, it "will apply the provisions of the [ODNI AG Guidelines] and these NCTC IPs that apply, respectively, to collected or obtained information."[28]

[23] ODNI AG Guidelines § 10.2. As used here, retention means "the indefinite maintenance of information concerning U.S. persons that meets the standard for retention listed in Section 6 [of the ODNI AG Guidelines]." ODNI AG Guidelines § 10.18.
[24] NCTC Implementation Procedures § 3.A. NCTC defines "domestic counterterrorism intelligence" as "Intelligence pertaining exclusively to domestic counterterrorism, or domestic counterterrorism intelligence, is that information and intelligence concerning efforts to counter domestic terrorism, as defined in 18 U.S.C. § 2331(5), with no known nexus to international or transnational terrorism or foreign terrorist organizations." NCTC Implementation Procedures § 10.B. On December 23, 2022, the President signed into law the Intelligence Authorization Act for Fiscal Year 2023, which contained language in the classified annex that curtails NCTC's activities in support of domestic counterterrorism. Consistent with congressional direction, NCTC has ceased the issuance of analytic contributions and products concerning terrorist threats without an identified foreign nexus. Some of NCTC's work in support of domestic counterterrorism continues, however, in so far as it concerns identifying any connections to international terrorism or domestic violent extremists with an identified foreign nexus, attacks of unknown origin, or general tactics, techniques and procedures. NCTC written responses (May 12, 2023).
[25] ODNI AG Guidelines § 3.2.
[26] NCTC Implementation Procedures § 3.B.
[27] *Id.*
[28] *Id.* § 3.B.

In addition to accessing and collecting information, the ODNI AG Guidelines and NCTC Implementation Procedures authorize NCTC to obtain, meaning receive, information from other IC elements in support of its missions so that it can determine whether the information is relevant to its responsibilities and can be retained.[29] If the obtained information has not already been evaluated by another IC element, NCTC must treat that information as unevaluated information and apply its relevant procedures accordingly.[30]

Under the previous framework articulated in the 2012 Guidelines, many of the privacy and civil liberties protections were mapped specifically to each track by which the information was acquired. Under NCTC's new access, collect, and obtain framework, many of those privacy and civil liberties protective provisions previously found in the 2012 Guidelines are applied to more activities in the ODNI AG Guidelines and NCTC Implementation Procedures. For example, the 2012 NCTC Guidelines required all queries of Track 3 data containing U.S. person information to be designed solely to identify information that was reasonably believed to constitute terrorism information.[31] As discussed further below, the NCTC Implementation Procedures require that all queries, regardless of how the information is acquired, be reasonably designed to return information related to an authorized ODNI/NCTC activity. For NCTC, this generally means queries designed to identify terrorism information.[32]

2. *Rules Governing NCTC's Domestic Counterterrorism Activities*

The NCTC Implementation Procedures address NCTC's authority to collect terrorism information and domestic counterterrorism intelligence, the authority for which is derived from Section 119(e) of the National Security Act of 1947.[33] The new domestic counterterrorism framework reflected in the Implementation Procedures provides policy descriptions and guidance to the NCTC workforce on how it should interact with data when the purpose is for domestic counterterrorism, as opposed to foreign or international counterterrorism. For instance, the NCTC Implementation Procedures identify the requirements that must be met to collect domestic counterterrorism intelligence,[34] describe how to handle unevaluated information that NCTC has collected or obtained solely for the purpose of identifying domestic counterterrorism intelligence,[35] and provide query and retention guidance for domestic counterterrorism intelligence.[36]

[29] ODNI AG Guidelines §§ 3.4, 10.13.
[30] *Id.* § 3.4.
[31] 2012 NCTC Guidelines § III.C.3.d.4.
[32] NCTC Implementation Procedures § 5.C.I.
[33] ODNI AG Guidelines § 10.19. Pursuant to Sec. 119(e) of the National Security Act of 1947, NCTC may "receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfil its responsibilities and retain and disseminate such intelligence" consistent with applicable law, presidential directives, and the ODNI AG Guidelines. NCTC interprets the use of "receive" in Sec. 119(e) to include both collecting and obtaining domestic counterterrorism intelligence.
[34] NCTC Implementation Procedures § 3.A.
[35] NCTC Implementation Procedures § 5.B.
[36] NCTC Implementation Procedures §§ 5.C.III, 6.

This domestic counterterrorism intelligence framework had been necessary because in 2018 NCTC began to explore ways to expand its footprint in this space.[37] Particularly, NCTC worked to improve the support it provided to the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), leveraging its own existing processes and procedures to assist FBI and DHS in broadly understanding the racially or ethnically motivated violent extremist (REMVE) threat. By 2020, NCTC had expanded its work also to focus on anti-government/anti-authority extremists, another type of domestic violent extremist ("DVE"—broadly analogous to "domestic terrorism.").[38] NCTC's increased attention to DVE "concerned four main areas: (1) investigative case support, (2) analytic production and analytic outreach, (3) real-time incident reporting, and (4) strategic operational planning."[39]

In December 2022, however, language in the classified annex accompanying the Intelligence Authorization Act for Fiscal Year 2023 (2023 IAA Annex) directed NCTC to pare back its coverage of domestic terrorism.[40] The 2023 IAA Annex provided congressional direction to NCTC not to prepare or contribute to intelligence products that had no foreign nexus, such as connections to known or suspected foreign terrorists, foreign terrorist groups, foreign powers, or other foreign entities.[41] As a result, NCTC narrowed its domestic terrorism-related work to connections that DVEs might have with foreign terrorist organizations or other foreign entities; issues related to attacks of unknown origin; and general terrorist tactics, techniques, and procedures.[42] Although

[37] NCTC began this exploration because federal and foreign partners increasingly voiced concerns about rising racially or ethnically motivated violent extremism (a type of domestic violent extremism).

[38] Since 2019, the U.S. government has defined REMVE as encompassing "threats involving the potentially unlawful use or threat of force or violence, in violation of federal law, in furtherance of political or social agendas which are deemed to derive from bias, often related to race, held by the actor against others, including a given population group. REMVEs use both political and religious justifications to support their racially- or ethnically-based ideological objectives and criminal activities. One set of REMVE threat actors use their belief in the superiority of the white race to justify their use of violence to further their political, cultural, and religious goals. A separate and distinct set of REMVE threat actors use real or perceived racism or injustice in American society, their desire for a separate Black homeland, and/or violent interpretations of religious teachings to justify their use of violence to further their social or political goals." The U.S. government defines a DVE as: "an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence dangerous to human life." The Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), STRATEGIC INTELLIGENCE ASSESSMENT AND DATA ON DOMESTIC TERRORISM, 4–5 (June 2023), [hereinafter Strategic Intelligence Assessment and Data on Domestic Terrorism].

[39] NCTC written responses (May 12, 2023). By early 2022, FBI, DHS, and NCTC were jointly releasing intelligence products addressing DVE issues via a newly formed Joint Analytic Cell (JAC). The JAC, though no longer operational, purportedly bolstered collaboration among the three agencies. NCTC, DHS, and FBI claimed it provides "more data-informed strategic analysis of the domestic terrorism threat environment and better inform[s] policymakers and state and local law enforcement agencies of changes in the threat landscapes." Strategic Intelligence Assessment and Data on Domestic Terrorism at 18, 28.

[40] Email from NCTC Civil Liberties and Privacy Officer (Jan. 10, 2023).

[41] *Id.*

[42] Before December 2022, for example, NCTC had forwarded analytic lead cables to partner agencies such as FBI when its analysts uncovered information in its holdings related to either domestic or international terrorism. Since December 2022, "NCTC now limits these lead cables to connections to international terrorism or identification of a foreign nexus for the DVE subject, such as when DVEs are influenced by foreign counterparts to radicalize and

this restriction is not a statutory requirement, NCTC has adopted internal guidance to ensure compliance with the congressional direction.[43]

To date, NCTC has not issued new NCTC Implementation Procedures to reflect this recent and significant narrowing of domestic terrorism-related work. Updating the NCTC Implementation Procedures explicitly to include the prohibitions and required processes now contained in internal guidance may provide helpful additional clarity.

In this context, the Board has conducted its review of NCTC's current procedures, cognizant that those procedures may be over inclusive of the scope of work NCTC is currently conducting, consistent with congressional direction.

As discussed further below, the NCTC Implementation Procedures require processes and guardrails for NCTC's handling of domestic counterterrorism-related information, including restrictions on how NCTC analysts may collect, obtain, retain, and query this information. Moreover, NCTC maintains additional privacy and civil liberties protections for analytic contributions to finished intelligence or investigations involving DVE threats with an identified foreign nexus. First, NCTC and the ODNI Office of Civil Liberties Privacy & Transparency adopted a policy that requires the NCTC Civil Liberties and Privacy Officer (CLPO) to conduct a review of analytic products that discuss a U.S. person engaging in activities with significant privacy and civil liberties implications before they may be disseminated outside of ODNI.[44] Second, NCTC does not identify in the first instance whether a particular individual should be labeled a DVE; rather, it defers this determination to FBI and DHS. Third, when NCTC contributes to domestic terrorism-related finished intelligence products in conjunction with other agencies, each agency's Attorney General Guidelines must be followed regarding the minimization of all U.S. person information in disseminated documents. Practically, this means that the most restrictive minimization rules govern the document's U.S. person information.[45]

In practice, NCTC furnishes U.S. person information potentially tied to domestic terrorism to federal, state, local, and foreign partners in three ways: (1) analytic production (including finished intelligence reports and outreach briefings); (2) situational awareness and other incident reports in

mobilize to violence." NCTC has also ended its contributions to and production of finished intelligence analysis strictly concerning DVEs. Its analysts still produce intelligence that tackles the transnational dynamics of all violent extremist threats, however, including. addressing instances when foreign actors push DVEs to radicalize and mobilize to violence. NCTC written responses (May 12, 2023).

[43] Nat'l Counterterrorism Ctr., NCTC GUIDANCE ON PROHIBITION ON NCTC ASSESSMENTS WITH NO FOREIGN NEXUS IN THE CLASSIFIED ANNEX TO THE INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2023 (June 29, 2023); Nat'l Counterterrorism Ctr., NCTC GUIDANCE ON PROHIBITION ON NCTC ASSESSMENTS WITH NO FOREIGN NEXUS IN THE CLASSIFIED ANNEX TO THE INTELLIGENCE AUTHORIZATION ACT (June 2024).

[44] NCTC-ODNI CLPT Policy 1: Civil Liberties and Privacy Safeguards for Certain Analytic Products (June 4, 2024).

[45] NCTC written responses (May 12, 2023).

the wake of developments of unknown origin that bear the hallmarks of a terrorist attack; and (3) investigative case support.[46]

Finally, NCTC provides U.S. person information to partners, including private sector entities, in support of FBI, DHS, or other federal agencies. Outside of investigative leads it forwards to FBI, the information NCTC shares with partners includes few specifics and is often publicly available material about terrorist attacks pulled from mainstream media coverage. Most of the information distributed to partners involves general trends and strategic analysis captured in finished intelligence. Notably, NCTC is permitted to provide a foreign partner with information concerning a U.S. person that is not publicly available only after the NCTC Director, "as the DNI's designee, makes a written assessment of the anticipated benefits of disseminating the information and the potential risks resulting from dissemination."[47]

3. *Increased Holding Period for Unevaluated Information*

The ODNI AG Guidelines and NCTC Implementation Procedures introduce new guidelines for maintaining U.S. person information and other information constituting terrorism information or domestic counterterrorism intelligence. Whereas under the 2008 NCTC Guidelines data acquired to identify terrorism information had to be "promptly removed" if NCTC could not "promptly" identify terrorism information, which as implemented at NCTC generally required data to be removed within 180 days,[48] the 2012 Guidelines enabled a five-year temporary retention period[49] and the ODNI AG Guidelines expand the holding period even further to twenty-five years for certain types of unevaluated information.[50] NCTC asserts that this increase in time permitted to evaluate data subject to routine handling requirements reflects similar evaluation periods contained in other sets of recently updated Attorney General-approved guidelines.[51] ODNI also maintains that this alignment of evaluation periods promotes consistency and enables more collaborative intelligence integration among IC elements.[52]

This increased holding period is specific to data that has not been evaluated by NCTC, meaning a determination has not been made as to whether the information relates to a lawful NCTC authority or purpose, contains U.S. person information, or qualifies for retention under the ODNI

[46] Section 7 of the ODNI AG Guidelines identifies federal, state, local, and foreign partners as authorized recipients of evaluated U.S. person information, as well as other recipients (such as private sector partners) if required by or in accordance with law, executive order, directive, policy or agreement. This type of information can also be shared with such partners if it is publicly available. *See also* NCTC written responses (May 12, 2023).
[47] NCTC written responses (May 12, 2023).
[48] 2008 NCTC Guidelines § III.A.3; NCTC Written Responses (June 17, 2024); ODNI CLPO, INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE UPDATED NCTC GUIDELINES, 1 (Jan. 2013).
[49] 2012 NCTC Guidelines § III.C.3.c.
[50] ODNI AG Guidelines § 5.3.3.2.
[51] NCTC written responses (Nov. 10, 2021). *See also* written responses received from NCTC citing 2016 memorandum from then Director of National Intelligence instructing IC elements to work to harmonize their guidelines pertaining to retention and dissemination of U.S. persons information. NCTC written responses (May 12, 2023).
[52] NCTC written responses (Nov. 10, 2021).

AG Guidelines.[53] As provided in Section 5 of the ODNI AG Guidelines, NCTC may maintain this unevaluated information when it is impracticable, infeasible, or detrimental to its mission to determine immediately whether the information qualifies for retention.[54] Exceptional handling is required for sensitive information, including nonpublic telephone or electronic communications acquired without the consent of a person who is party to the communication or information reasonably believed to contain information concerning U.S. persons that is significant in volume, proportion, or sensitivity.[55] Unevaluated information subject to exceptional handling may be held for up to five years.[56] All other types of unevaluated information are subject to routine handling requirements and may be held for up to 25 years.[57]

Because unevaluated information subject to routine handling may now be held for 25 years after the information has been made available to ODNI personnel for analytic use, NCTC analysts may conduct queries during this entire 25-year period if such queries are reasonably designed to retrieve information related to a duly authorized activity.[58] NCTC asserts that it only maintains unevaluated information for the duration of its utility, and particular datasets may have shorter evaluation periods as appropriate and as provided for in any applicable agreement with an information-sharing partner.[59] NCTC states that it would similarly purge any collected or obtained information that it immediately determines does not qualify for retention and lacks a mission need for continuous review.[60] However, because the NCTC Implementation Procedures were only finalized in 2021, the Board has not determined whether and to what extent in practice NCTC purges information prior to its aging off under the extended evaluation periods.

C. The ODNI AG Guidelines and NCTC Implementation Procedures in Practice

In this section, we describe how the ODNI AG Guidelines and Implementation Procedures work in NCTC's day-to-day activities. Of note, the only unevaluated signals intelligence that NCTC acquires and maintains on NCTC systems is data collected by other IC elements under Section 702 of the Foreign Intelligence Surveillance Act.[61] Thus, the datasets NCTC acquires pursuant to the ODNI AG Guidelines and NCTC Implementation Procedures covered by this report do not include any unevaluated signals intelligence.[62]

---

[53] NCTC Implementation Procedures § 5; ODNI AG Guidelines § 5.
[54] ODNI AG Guidelines § 5.
[55] *Id.* § 5.2.1, NCTC Implementation Procedures § 5.B.
[56] ODNI AG Guidelines § 5.2.2.2; NCTC written responses (Nov. 10, 2021).
[57] ODNI AG Guidelines § 5.3.1.
[58] NCTC written responses (Nov. 10, 2021). *See also* ODNI AG Guidelines § 10.20 ("Unevaluated information means information that has been collected or obtained, but that has not yet been determined to (1) relate to an authority and responsibility listed in Section 2; (2) contain any information concerning U.S. persons; and (3) meet the criteria for retention under Section 6.").
[59] NCTC written responses (Nov. 10, 2021).
[60] *Id.*
[61] Telephone conference among ODNI, NCTC, and PCLOB (Aug. 22, 2024).
[62] *Id.*

First, we discuss how NCTC acquires and ingests, accesses, and queries data in order to conduct its counterterrorism mission. Next, we discuss the oversight and training requirements directed by the Implementation Procedures.

1. *Datasets Used to Identify Terrorism Information*

NCTC accesses, collects, and obtains information from a variety of datasets in furtherance of its counterterrorism mission.[63] These datasets come primarily from other executive departments and agencies, and to a lesser degree from commercial providers. These include datasets originating from encounters between the data subjects and government agencies where data subjects are aware they are providing information to the government, certain international travel-related datasets, relevant immigration benefits-related datasets, and some financial-related datasets. The travel-related datasets are generally records relating to an individual's travel, such as the crossing of international borders, and documents utilized in the conduct of travel. NCTC uses travel-related data to support analysis of threat reporting and leads, with a particular focus on U.S. entries and exits of known or suspected international terrorists. The immigration benefit datasets are records relating to an individual's application to the federal government for travel and immigration benefits, which may include U.S. person family members or points of contact. These datasets are used to provide screening and vetting support to federal agencies in the adjudication of applications for U.S. travel and immigration benefits. NCTC also utilizes certain immigration benefit datasets to identify known or suspected international terrorists who attempt to exploit the immigration process. Finally, the financial-related datasets contain records meeting certain federally mandated reporting thresholds, such as data pertaining to suspect financial transactions. NCTC uses these datasets to identify sources of funding of international terrorism.

As of this review, NCTC states that it does not have any datasets that were collected or obtained solely for domestic counterterrorism intelligence but, if it did in the future, this data would fall under the exceptional handling category.[64]

2. *Data Acquisition and Ingestion of Datasets*

NCTC typically acquires new datasets through information sharing agreements, such as memorandums of understanding, memorandums of agreement, and letters of intent, with federal

[63] *See* ODNI AG Guidelines §§ 10.1 ("**Access** means the viewing or examining of information by the ODNI for official purposes, where the information viewed or examined is not stored or otherwise maintained under the control of the ODNI. Access is distinct from collecting or obtaining information."), 10.2 ("**Collection** means the receipt of information by the ODNI for official purposes, whether or not the information is retained. Collected information does not include: (a) information that is accessed by an ODNI employee but is not stored or otherwise maintained under the control of the ODNI; or (b) information obtained from another element of the Intelligence Community that has been lawfully provided by that element pursuant to its Procedures."), 10.13 ("**Obtain** means the receipt by the ODNI for official purposes of information that has been lawfully collected and disseminated by another element of the Intelligence Community under its own Procedures. Obtaining information is distinct from accessing or collecting information.").

[64] Telephone conference among ODNI, NCTC, and PCLOB (Mar. 1, 2021); NCTC Implementation Procedures § 5.B.

data providers or through contracting with a commercial provider.[65] When determining whether to acquire a particular dataset, NCTC evaluates its mission need for the information, conducts a review to understand the data in question, and determines whether the data is pertinent to NCTC operations before collecting or obtaining data.[66] NCTC's review involves coordinating with the data provider partner to understand the type of information involved; the time, place, and circumstances of collection; and other factors to assess whether a given dataset is likely to include information relevant to NCTC's counterterrorism mission.[67] If NCTC collects a new agency dataset, it must document why its needs cannot be fully met by accessing the dataset without collecting it.[68]

Key internal oversight and compliance stakeholders are part of the acquisition process, including NCTC's Office of Enterprise Services (formerly called the Office of Data Strategy and Compliance),[69] NCTC's Office of Information Technology Services, NCTC Legal, and the NCTC CLPO.[70] These offices lead engagement with the data provider to develop terms and conditions on the use of the acquired dataset, including operational, legal, and privacy and civil liberties constraints.[71] Once the dataset has been acquired and ingested into NCTC's systems, it undergoes technical processing to ensure the pre-agreed rules regarding the dataset are applied, such as access safeguards or tagging with retention rules to enable auto-deletion.[72]

[65] NCTC Implementation Procedures § 1.B. During the acquisition process for commercially available information, NCTC is additionally subject to the Intelligence Community Policy Framework for Commercially Available Information (CAI Policy Framework). The CAI Policy Framework governs the access to and collection and processing of commercially available information by elements of the IC. It is intended to augment each IC element's Attorney General Guidelines and related policies. All IC elements must implement the CAI Policy Framework by August 2024. ODNI, INTELLIGENCE COMMUNITY POLICY FRAMEWORK FOR COMMERCIALLY AVAILABLE INFORMATION, 1–2 (May 2024).
[66] Telephone conference among ODNI, NCTC, and PCLOB (Nov. 10, 2021).
[67] NCTC written responses (May 12, 2023).
[68] *Id.*
[69] The Office of Enterprise Services replaced the Office of Data Strategy and Compliance. The Office of Enterprise Services is comprised of the Data Acquisition & Policy Group, Compliance & Transparency Group, and Enterprise Operations Group which consists of budget, human resources, and training elements. NCTC written responses (June 17, 2024).
[70] NCTC written responses (Nov. 10, 2021).
[71] Telephone conference among ODNI, NCTC, and PCLOB (Nov. 10, 2021); NCTC Implementation Procedures § 1.B. NCTC maintains Information Sharing Arrangements, such as Memorandums of Understanding, Memorandums of Agreement, and Letters of Intent between NCTC and data providers, to facilitate NCTC's efforts to collect, access, and obtain information to support its mission.
[72] Telephone conference among ODNI, NCTC, and PCLOB (Nov. 10, 2021).

At times, NCTC may collect or obtain data that exceeds its capacity to evaluate the information immediately to determine what information within the dataset qualifies for retention.[73] In these instances, NCTC's Office of Enterprise Services, in coordination with NCTC Legal, the NCTC CLPO, and NCTC's Office of Information Technology Services, must document why NCTC's needs cannot be met by accessing the data without collecting it.[74] This documentation must also include the purpose of the activity for which the data is needed, which set of handling and querying requirements (routine or exceptional) will be applied to the unevaluated information, and whether the unevaluated information is anticipated to include information concerning U.S. persons that is significant in volume, proportion, or sensitivity.[75] The documentation must be completed and approved before the information is available for analytic purposes.[76] In emergency circumstances, however, the designated senior official responsible for approving such documentation may make the information immediately available for analytic purposes under the exceptional handling rules.[77] NCTC has not implemented any additional guidance or policies for data acquisition in an emergency or exigent scenario where it would be untimely to follow the typical acquisition process.[78]

3. *Access to Datasets*

To determine the datasets to which an analyst may have access, mission managers consult with the Office of Enterprise Services to identify the relevant data for each work role in the manager's component. When an officer begins an assignment in a new work role, the Office of Enterprise Services initiates the process for that officer to receive the designated data required to perform the role's functions.[79]

NCTC users' eligibility for dataset access is based on the particular user's organizational affiliation, established need-to-know, security clearance, training status, and additional attributes as required for accessing the given dataset. The Office of Enterprise Services uses an access management system to validate whether the user is eligible for access and has met the pre-requisites for access, including the appropriate approvals.[80]

[73] ODNI AG Guidelines § 4.1; NCTC Implementation Procedures § 4.
[74] NCTC Implementation Procedures § 4; ODNI AG Guidelines §§ 3.3, 4.2.
[75] NCTC Implementation Procedures § 4; ODNI AG Guidelines § 4.2.
[76] ODNI AG Guidelines § 4.1; NCTC Implementation Procedures § 4.a (NCTC must complete specific documentation for all collection and obtainment that exceeds NCTC's capacity to evaluate the information immediately for retention).
[77] ODNI AG Guidelines § 4.1.
[78] Telephone conference among ODNI, NCTC, and PCLOB (Nov. 10, 2021).
[79] NCTC written responses (June 17, 2024).
[80] *Id.*

The Office of Enterprise Services audits access to restricted repositories, individual access credentials, access to NCTC unevaluated datasets and system tools, information technology system object changes, and audit log modifications and discrepancies. NCTC Legal and the CLPO review audit reports. Additionally, NCTC participates in quarterly ODNI audits pertaining to privileged user need-to-know and training statuses.[81]

4. *Queries*

Before an analyst at NCTC can perform any queries of ingested datasets, a manager must authorize access for the analyst.[82] All queries of information held within the datasets NCTC accesses, collects, and obtains must be reasonably designed to return information related to an authorized ODNI/NCTC activity, generally meaning that queries need to be tailored to identify terrorism information. Additional rules apply depending on whether the information is being either accessed, collected, or obtained and whether the data queried is subject to requirements for routine handling or exceptional handling.[83] Managers do not approve individual queries by analysts.

When accessing data under the NCTC Implementation Procedures, NCTC analysts may only query using terms that are reasonably designed to retrieve information related to a duly authorized NCTC activity, namely counterterrorism, and, to the extent practicable, minimize the return of unrelated U.S. person information.[84] Unlike the 2012 NCTC Guidelines, the NCTC Implementation Procedures do not require analysts to begin queries with a terrorism data point (i.e., known or suspected terrorist identifiers or other pieces of terrorism information), or limit their query purpose to the identification of terrorism information. NCTC maintains that the 2012 query standard hampered NCTC's ability to perform aspects of its authorized mission by limiting its ability to conduct screening and vetting support queries in other agencies' datasets to identify potential terrorism information.[85] The NCTC Implementation Procedures provide that when a query "is designed to retrieve information about an unconsenting U.S. person, analysts should identify the particular purpose of the query."[86] The NCTC Implementation Procedures, however, do not articulate whether and how analysts are required to document that purpose.

Additional rules apply to unevaluated information:[87] For unevaluated information that NCTC has collected or obtained, NCTC may continuously review these datasets to identify terrorism information consistent with the routine and exceptional handling requirements applicable to each dataset.[88] The requirements for queries of information subject to routine handling and exceptional

[81] *Id.*
[82] Typically, this access is approved once for any given role. The Office of Enterprise Services maintains awareness of when NCTC users' need-to-know status changes through self-reporting by a user of a change in role and through an automated tool to monitor daily changes to NCTC's staffing. NCTC written responses (June 17, 2024).
[83] NCTC Implementation Procedures § 5.C.
[84] *Id.* § 3.B.
[85] NCTC written responses (Nov. 10, 2021).
[86] NCTC Implementation Procedures § 3.B.
[87] *Id.* § 5, ODNI AG Guidelines §§ 5, 10.20.
[88] NCTC Implementation Procedures § 5.A.

handling are similar to those discussed above regarding NCTC queries of accessed information. However, queries of unevaluated information subject to exceptional handling and designed to retrieve information concerning a U.S. person must be conducted with the person's consent or, to the extent practicable, be accompanied by a justification statement explaining the particular purpose of the query.[89] These query justifications are generally one or two sentences explaining why an analyst believes the query is reasonably likely to identify information relevant to an authorized ODNI/NCTC activity and, where possible, indicate query source information such as cable numbers or disseminated intelligence reports.[90] Regardless of the applicable evaluation period, if NCTC identifies U.S. person information in unevaluated information, such as in response to a query, it would not change the status of the entire body of data from unevaluated to evaluated. In order to change the status of that specific U.S. person information to evaluated, NCTC would need to determine whether that information relates to an ODNI/NCTC authority and responsibility and meets the criteria for retention.[91] If that specific information meets those conditions, NCTC may retain it and it would no longer be unevaluated information.[92] The status of the remainder of the body of data would continue to be unevaluated information.[93]

Unevaluated information that NCTC "collects or obtains ***solely*** for the purpose of identifying domestic counterterrorism intelligence in support of an agency with an authorized domestic counterterrorism mission is subject to exceptional handling requirements and any additional protections [the NCTC Director] may find appropriate pursuant to Subsection 5.2.1 of the ODNI [AG Guidelines] (emphasis in original)."[94] Further restrictions attach when NCTC analysts query unevaluated information for the purpose of retrieving domestic counterterrorism intelligence. Before conducting such queries, analysts must complete domestic counterterrorism training and be designated by a supervisor to perform authorized domestic counterterrorism activities.[95] When an authorized analyst searches any data by conducting a query for the purpose of retrieving domestic counterterrorism intelligence (a "domestic counterterrorism query"), the analyst must satisfy both the requirements in place for queries subject to exceptional handling and those for domestic counterterrorism queries.[96] Under the exceptional handling query requirements, to the extent practicable, analysts must provide a written justification explaining why they believe the query is reasonably likely to retrieve information relevant to the authorized NCTC activity.[97] Under the domestic counterterrorism query requirements, analysts must provide an additional

[89] *Id.* § 5.C; ODNI AG Guidelines § 5.2.3. The ODNI AG Guidelines and NCTC Implementation Procedures do not define "practicable" as used here, nor do they explain how it may be impossible to include query source information in a query justification.
[90] *Id.*
[91] NCTC written responses (May 12, 2023). *See* ODNI AG Guidelines § 6.
[92] NCTC written responses (May 12, 2023).
[93] *Id.*
[94] NCTC Implementation Procedures § 5.B.
[95] NCTC written responses (Nov. 10, 2021); NCTC Implementation Procedures § 5.C.III.
[96] NCTC written responses (Nov. 10, 2021); NCTC Implementation Procedures § 5.C.II.
[97] NCTC written responses (Nov. 10, 2021); NCTC Implementation Procedures § 5.C.III.

statement explaining how the query satisfies an authorized purpose distinct from one solely designed to monitor constitutionally protected activity and how it supports a lead domestic counterterrorism agency, such as FBI or DHS.[98] These query requirements for domestic counterterrorism intelligence queries apply based on the purpose of the query, irrespective of whether the data is generally subject to routine or exceptional handling.[99]

Similar to auditing access of datasets, query audits are the principal method NCTC uses to ensure queries are in compliance with the ODNI AG Guidelines and NCTC Implementation Procedures. NCTC's audit capabilities and functions differ depending on whether NCTC accesses, collects, or obtains the dataset. Under the access paradigm, NCTC analysts access datasets through the relevant systems of the agency that owns the dataset. Accordingly, NCTC analysts are required to follow the owner agency's compliance requirements and NCTC is reliant on the owner agency to conduct audits of NCTC activities.[100] NCTC analysts with this account-based access to the data of other departments and agencies generally are subject to the compliance regimes of those departments and agencies for preventing and detecting unauthorized use of their data and, as such, complete relevant training and other access requirements of the owning entity.[101] As a result, the NCTC query standard for accessed information, namely that analysts must query using terms that are reasonably designed to retrieve information related to a duly authorized NCTC activity, is upheld through preventive internal controls, such as training, while the formal query compliance burden remains on the data providers. If a data provider identifies non-compliant queries during its routine audits, NCTC works with its information-sharing partners to address any compliance issues identified on the owning agencies' systems. With regard to any data provider that is not a federal government agency (e.g., commercial, state, local, and international data providers), it would be helpful for NCTC to develop a mechanism to record query terms to enable NCTC to ensure compliance with the query standard.

In contrast to NCTC's need to rely on owner agencies' audit capabilities for data accessed under the access paradigm, NCTC conducts its own audits of queries within datasets it has collected and obtained. On a monthly basis, the Office of Enterprise Services pulls data for queries performed through the different analytical tools used to query the collected or obtained information, and managers review a fixed number of these queries. The monthly audits of queries provide a feedback loop in which NCTC can update its training and engage with the analytic workforce to ensure queries are properly tailored to return the appropriate terrorism information.

[98] NCTC written responses (Nov. 10, 2021); NCTC Implementation Procedures § 5.C.III.
[99] NCTC written responses (Nov. 10, 2021).
[100] *Id.*
[101] NCTC written responses (Nov. 10, 2021).

5. *Oversight Regime*

The ODNI AG Guidelines call for a revised oversight regime implemented by the Principal Deputy Director of National Intelligence, which would incorporate initial and annual training; compliance safeguards including rules, internal controls, and monitoring activities; and a regular review of the oversight program.[102] Previously, the 2012 Guidelines were more prescriptive in their description of the required compliance framework but covered less data and fewer NCTC activities. The ODNI AG Guidelines and NCTC Implementation Procedures, by contrast, are less prescriptive but apply to a broader range of data and NCTC activities. The 2012 Guidelines, for example, required NCTC to conduct periodic compliance reviews, which were to include "spot checks, reviews of audit logs, and other appropriate measures."[103] In contrast, the NCTC Implementation Procedures note that NCTC's former Office of Data Strategy and Compliance, now named the Office of Enterprise Services, "is responsible for managing and coordinating NCTC's compliance activities and compliance-related training,"[104] but does not explain those compliance activities in detail. Moreover, the NCTC Implementation Procedures do not articulate clear compliance, reporting, and oversight roles for its offices with compliance equities, including the former NCTC Office of Data Strategy and Compliance, the NCTC Office of Information Technology Services, NCTC Legal, and the NCTC CLPO. For example, the 2012 Guidelines required NCTC promptly to document and report "significant failures" to comply with the Guidelines and to annually assess how NCTC ensures appropriate handling and protection of U.S. person information under the Guidelines.[105] In contrast, the ODNI AG Guidelines now provide a general requirement for ODNI employees to report activities that may be unlawful or contrary to executive order or presidential directive,[106] and the NCTC Implementation Procedures only provide for a program review every three years and do not state what criteria will be considered in the program review.[107]

6. *Training*

As referenced above, NCTC requires all employees engaged in activities covered by the NCTC Implementation Procedures, including contractors, detailees, and, in certain limited circumstances, assignees, to complete initial and annual training.[108] Specifically, upon joining NCTC, all NCTC analysts must complete training on the ODNI AG Guidelines and the NCTC Implementation Procedures, with a focus on the protection of U.S. person information.[109] Additionally, new analysts must complete training on NCTC's access and use of data.[110] On an annual basis

[102] ODNI AG Guidelines § 9.2.1. *See also* NCTC Implementation Procedures § 9.
[103] 2012 NCTC Guidelines § VI.A.
[104] NCTC Implementation Procedures § 9.A.
[105] 2012 NCTC Guidelines §§ VI.D.1, VI.D.2.
[106] ODNI AG Guidelines § 9.2.6.
[107] NCTC Implementation Procedures § 9.D.
[108] *Id.* §§ 9.B, 10.C.
[109] NCTC document production (Oct. 5, 2022).
[110] *Id.*

thereafter, all NCTC analysts must complete refresher training on NCTC's access and use of data and on U.S. person information, including general rules regarding U.S. persons under Executive Order 12333 activities and NCTC-specific rules regarding U.S. persons and NCTC's activities.[111] Finally, all employees provided access to datasets governed by the ODNI AG Guidelines and NCTC Implementation Procedures receive training in the use of each dataset to which they have access.[112]

Some activities, such as those related to U.S. person information and domestic counterterrorism intelligence, require training before an analyst may conduct the activity.[113] For those analysts who had been designated to work on domestic terrorism matters, NCTC requires an in-person, discussion-based legal training on the application of the ODNI AG Guidelines and NCTC Implementation Procedures to NCTC activities relating to domestic terrorism.[114] This training is required before a designated analyst authorized to perform domestic counterterrorism activity may conduct a query designed to retrieve domestic counterterrorism intelligence.[115] Moreover, the use of retained U.S. person information is limited to those employees with appropriate training, and an analyst conducting a query of retained information designed to retrieve domestic counterterrorism intelligence must complete specialized NCTC training on domestic counterterrorism authorities.[116]

[111] *Id.*
[112] NCTC Implementation Procedures § 9.B.
[113] *Id.* §§ 5.C.III, 6.B.
[114] NCTC document production (Oct. 5, 2022). As a result of congressional direction, NCTC has revised its training materials to reflect that it no longer issues analytic contributions and products concerning terrorist threats without an identified foreign nexus. NCTC written responses (May 12, 2023, Oct. 22, 2024).
[115] NCTC Implementation Procedures § 5.C.III.
[116] *Id.* § 6.B.

III. RECOMMENDATIONS

The Board offers the following recommendations based on its examination of the NCTC Implementation Procedures and additional information obtained during this oversight review. During the bulk of the Board's review, the initial application of the Implementation Procedures was ongoing. Accordingly, the Board did not assess fully all aspects of Executive Order 12333 activity and whether NCTC's use of datasets containing non-terrorism information is appropriately balanced with privacy and civil liberties interests. However, the Board offers the following recommendations to guide ODNI and NCTC as NCTC continues its efforts to apply the requirements of the ODNI AG Guidelines and NCTC Implementation Procedures.

QUERIES

RECOMMENDATION 1:

NCTC should require personnel to document justifications for any query seeking information about a U.S. person before conducting the query, regardless of whether the query searches through "accessed," "obtained," or "collected" information.[117] Further, NCTC should develop a process to audit queries based on documented query justifications.

Section 3(B) of the NCTC Implementation Procedures articulates a standard for queries of accessed information. NCTC analysts may only query accessed information using terms that are reasonably designed to retrieve information related to a duly authorized activity and, to the extent practicable, minimize the return of unrelated U.S. person information. Furthermore, if the query is designed to retrieve information about a U.S. person,[118] analysts should identify the particular purpose of the query.[119]

Despite the standard for queries of accessed information, as noted above, NCTC currently does not audit any queries of accessed information.[120] NCTC states that auditing queries of accessed information poses challenges because NCTC does not administer or control the relevant systems of other departments and agencies.[121] Instead, the query standard is enforced through internal controls and engagement with the analytic workforce, through training and legal and operational

[117] Consistent with the definitions of these terms, this pertains to both unevaluated and retained information. However, this recommendation to document justifications does not apply to U.S. person queries that are structured to ensure that they search only through datasets that include only disseminated reports or other finished intelligence products. This limitation of the recommendation applies provided that current safeguards for U.S. person information included in finished intelligence products continue to be in effect — such as requirements for supervisory and/or compliance review of analysts' determinations that it is appropriate to disseminate the U.S. person information as part of the finished product. The Board recognizes that it may take some time to implement this recommendation and urges NCTC to consider a phased implementation approach beginning with queries of unevaluated information.
[118] Although consent by the person to whom the query pertains is an exception to certain query requirements, PCLOB staff are aware of no indication that such a consent-based query by NCTC has ever occurred.
[119] NCTC Implementation Procedures § 3.B.
[120] NCTC written responses (Nov. 10, 2021).
[121] *Id.*

guides and tutorials, to ensure the guidance is understood and implemented appropriately.[122] Additionally, NCTC analysts accessing other department and agency systems are subject to the compliance regimes of those other departments and agencies to prevent unauthorized use of their data.

To supplement these checks, NCTC should require that analysts document each U.S. person query justification before analysts conduct a query of accessed information. NCTC analysts accessing agency systems outside of NCTC should also, where not already the case, be required to justify in an NCTC system what their need and minimization strategies are for queries in other agency systems. Moreover, mandating query justifications in writing in an NCTC system will facilitate periodic internal audits of queries of accessed information, which are currently the responsibility of the external data provider.

Regarding U.S. person queries against unevaluated information that NCTC collects or obtains, NCTC should adopt the same rule and require analysts to provide a written justification explaining the particular purpose of the query before the query is run against unevaluated information subject to either routine or exceptional handling, not just "when practicable" against information subject to exceptional handling, as is currently required.[123]

Requiring NCTC analysts to provide a written explanation of why a query is reasonably likely to identify information relevant to an authorized NCTC activity and to provide supporting information for this determination before a query is run would provide a key privacy guardrail. Written explanations force analysts to be more thoughtful in query construction and help ensure that all queries meet the requirement that they are reasonably designed to return information related to an authorized activity. Furthermore, mandating query justifications in writing will permit periodic audits of queries of accessed information currently the responsibility of the external data provider.

To assist in this process, NCTC should develop written guidance for analysts authorized to perform such queries to explain clearly the meaning of the standard, "reasonably designed to retrieve information related to an authorized ODNI/NCTC activity." NCTC should also provide illustrative examples of permissible and impermissible queries as well as proper and improper basis on which to conclude that a query of accessed information may identify terrorism information.

[122] *Id.*
[123] NCTC Implementation Procedures § 5.C.

RECOMMENDATION 2:

Require a capability in all appropriate NCTC applications for recording the justification of each query, to include a process that ensures all exceptional handling complies with the ODNI AG Guidelines and NCTC Implementation Procedures.

As noted above, both the ODNI AG Guidelines and the NCTC Implementation Procedures permit queries of unevaluated information subject to exceptional handling.[124] When the query is designed to retrieve information concerning a U.S. person, to the extent practicable, a query justification explaining its particular purpose must be included with the query.[125] Despite this requirement, currently some existing NCTC applications do not include a capability to enable personnel to document their justifications before querying information subject to exceptional handling.[126] Yet NCTC states that documenting a query justification is only practicable when the application in which the query is run has a query justification capability.[127] Further, the need for such a capability will increase if NCTC implements Recommendation 1 above in which the Board urges that NCTC expand the documentation requirement to all queries.

NCTC should work expeditiously to ensure that all appropriate NCTC applications include the capability for analysts to record their justifications for each U.S. person query. Should NCTC require time to develop a query justification capability technologically, it should design an interim manual process to document and record any applicable query justification. Developing functional query justification capabilities in all NCTC applications that query information would ensure that NCTC complies with all query justification requirements articulated in the ODNI AG Guidelines and NCTC Implementation Procedures and would facilitate the implementation of Recommendation 1 above.

RETENTION

RECOMMENDATION 3:

Reduce evaluation periods consistent with NCTC's mission operations.

The ODNI AG Guidelines and NCTC Implementation Procedures substantially expand the temporary retention period to identify terrorism information from the 2012 NCTC Guidelines, which in turn had dramatically expanded the retention period under the original 2008 Guidelines. More specifically, the 2008 Guidelines required NCTC to "promptly review" and "promptly" discard U.S. person information — generally within 180 days — if it did not constitute terrorism information, and the 2012 Guidelines increased the period to five years, which has become a

[124] *Id. See also* ODNI AG Guidelines § 5.2.3.
[125] NCTC Implementation Procedures § 5.C.II.
[126] NCTC AG Guidelines: User Guide for Queries and Retention.
[127] *Id.*

standard baseline period.[128] The current ODNI AG Guidelines maintain the five-year evaluation period for unevaluated information subject to exceptional handling requirements, which includes that unevaluated information reasonably believed to contain information concerning U.S. persons that is significant in volume, proportion, or sensitivity,[129] but have now increased the evaluation period to 25 years if the unevaluated information is subject to routine handling requirements.[130] Accordingly, under the ODNI AG Guidelines, in contrast to the 2012 NCTC Guidelines, NCTC can now store and query information that has not been determined to have counterterrorism value, and which may include sensitive U.S. person information, for a significantly longer period of time.

NCTC has stated that a 25-year evaluation period for data subject to routine handling requirements and a 5-year evaluation period for data subject to exceptional handling requirements reflect similar evaluation periods contained in other sets of recently updated Attorney General-approved Guidelines. However, the significantly longer evaluation period for unevaluated data subject to routine handling requirements in comparison to the 2012 NCTC Guidelines is concerning.

Increasing retention periods increases various risks, including risks of improper secondary uses and data breaches. To minimize privacy risks, ODNI should define when a dataset contains U.S. person information that is significant in volume, proportion, or sensitivity and should be subject to exceptional handling.

NCTC should conduct standardized, periodic reviews of all datasets to determine whether retention and continuous review of those datasets remains appropriate and useful for the identification of terrorism information. In conducting the review, NCTC should consider the purpose for which the dataset was acquired, whether that purpose can be achieved through accessing the data or through other datasets already in NCTC's possession, and privacy and civil liberties considerations applicable to the particular dataset. Where appropriate, NCTC should adopt shorter evaluation periods for certain types of data or specific datasets, even if the default 5- and 25-year periods would otherwise permit lengthier holding.

OVERSIGHT

RECOMMENDATION 4:

Document and formalize oversight roles and responsibilities at each stage of the dataset lifecycle.

[128] 2008 NCTC Guidelines §§ III.A.3, III.C.3.c; ODNI CLPO, INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE UPDATED NCTC GUIDELINES (Jan. 2013) at 1; 2012 NCTC Guidelines § III.C.3.c.
[129] ODNI AG Guidelines § 5.2.1; NCTC Implementation Procedures § 5.B.
[130] ODNI AG Guidelines § 5.3.3.2.

The Board understands NCTC's oversight regime to be composed of the internal oversight and compliance stakeholders discussed above, designed to ensure that NCTC appropriately holds data in accordance with applicable law and policy, including the ODNI AG Guidelines and NCTC Implementation Procedures. However, the Board was unable to determine from its review the exact roles and responsibilities of these offices during different stages of the dataset lifecycle. In particular, it is unclear what specific actions any particular representative takes, what is documented, and where this information is stored.[131]

NCTC can enhance privacy and civil liberties protections by documenting and making public these roles and responsibilities. At a minimum, NCTC should make clear the role and purpose of the NCTC Civil Liberties and Privacy Officer and how that position interacts with the other internal offices to promote privacy and civil liberties protective efforts.[132] NCTC should also document the roles of each office during the data acquisition phase and articulate how decisions regarding whether to access or collect information are made. Similarly, an oversight document should make clear the rules and processes in place for these oversight entities when evaluating data held without documentation or a governing information sharing agreement. Finally, NCTC should make clear how these oversight offices ensure appropriate dissemination. Unclear oversight roles and responsibilities can undermine even vigorous oversight efforts, so formalizing and documenting how each of these entities ensures privacy protections will promote a comprehensive and transparent oversight regime.

RECOMMENDATION 5:

Randomly select a targeted but representative sample of queries to audit each month. Automate monthly query audits and other oversight functions where appropriate.

Both the ODNI AG Guidelines and NCTC Implementation Procedures require routine audits of justifications for certain queries.[133] The Board understands that under current practice, managers of NCTC analysts conduct reviews of query justifications on a monthly basis, although due to time and resource constraints, the number of query audits is relatively low in comparison to the total number of queries of unevaluated information performed during a given month.[134]

NCTC should select a statistically meaningful and appropriate sample of queries to audit each month to ensure, in a more representative manner than presently the case, that the full population of queries complies with the NCTC Implementation Procedures and ODNI AG Guidelines. The procedure for selecting query audit samples should follow best statistical and audit practices in

[131] Telephone conference among NCTC and PCLOB (Mar. 17, 2022).
[132] The NCTC-ODNI CLPT Policy 1: Civil Liberties and Privacy Safeguards for Certain Analytic Products (June 4, 2024) includes a generic description of the responsibilities of the NCTC Civil Liberties and Privacy Officer.
[133] ODNI AG Guidelines § 5.2.2.1; NCTC Implementation Procedures §§ 5.C.III, 9.C.
[134] Telephone conference among ODNI, NCTC, and PCLOB (Nov. 10, 2021).

order to achieve a high level of confidence that the results of the analysis reflect the overall query population.

Acknowledging the labor-intensive process currently used to perform query audits, the Board encourages NCTC to explore technological approaches that may minimize the time and resource issues which currently prevent more queries from being reviewed. For example, NCTC could leverage automation to complement the human-based manual review for the monthly query audits instead of relying exclusively on the time-consuming, resource-constrained, and ultimately hard-to-scale human-based, manual review processes. Doing so should allow NCTC to conduct more query audits per month.[135] Further, technical mechanisms could be implemented to prevent noncompliant query justifications, complementing the human-based, manual review rather than supplanting it, to enable more scaled review.

RECOMMENDATION 6:

Develop a framework to guide the NCTC Implementation Procedures review process. In addition, reinstate certain reporting requirements from 2012 NCTC Guidelines.

The NCTC Implementation Procedures call for a review of the program every three years.[136] In anticipation of those reviews, NCTC should establish a written framework that guides the review process, requires documenting the results of the review, and establishes public reporting requirements, such as those listed below, consistent with national security. Many of these items were articulated in the 2012 NCTC Guidelines for internal reporting:[137]

- A description of NCTC's compliance and audit processes, including the results of any audits, any identified compliance issues, and any mitigation techniques implemented;
- The results of the periodic reviews of datasets referenced in Recommendation 3 above, including whether retention continues to be appropriate, and whether any shorter retention periods are ultimately adopted;
- A description of any reviews conducted during the previous three years and any identified problems and mitigations;
- A description of how NCTC purges or removes information that does not qualify for retention or does not qualify for continued evaluation or retention and is unnecessary for continuous review, to include the numbers of datasets per year that are (1) determined not to qualify for collection or retention, and (2) determined not necessary for continuous review;

[135] The Board notes the 2012 NCTC Guidelines required NCTC when designing its computer systems to take reasonable steps to facilitate the compliance, auditing, and reporting requirements imposed by the Guidelines themselves. *See* 2012 NCTC Guidelines § VI.C.
[136] NCTC Implementation Procedures § 9.D.
[137] 2012 NCTC Guidelines § VI.D.2.

- An assessment of U.S. person information disseminated by NCTC directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that NCTC imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification;

- A description of any bulk dataset disseminations;[138]

- An assessment of whether there is a need for enhanced safeguards, procedures, or oversight, beyond what is already required regarding the handling of U.S. person information or other sensitive information, or whether any other reasonable measures should be taken to improve the handling of information;

- A description of any material changes or improvements NCTC implemented during the previous reporting period, or is considering implementing, to improve compliance with the ODNI AG Guidelines and NCTC Implementation Procedures.

[138] Unlike the 2012 NCTC Guidelines, the NCTC Implementation Procedures do not address bulk dataset disseminations. *See* 2012 NCTC Guidelines §§ IV, VI.D.2, Appendix: Safeguards, Procedures, and Oversight Mechanisms for Bulk Dissemination of Information Acquired Under Track 3 to IC Elements.

ANNEX A: SEPARATE STATEMENT OF BOARD MEMBER EDWARD W. FELTEN

I fully concur with the Board's report. I write separately to expand on one technical issue discussed in the report: the need for a comprehensive compliance framework that addresses information security risks and auditing requirements for data that NCTC accesses through non-federal government entities.[139] This should include, but not be limited to, ensuring there is a mechanism to record query terms to enable NCTC to comply with the query standard.

Under the access[140] paradigm, NCTC neither owns nor controls the systems which maintain and process datasets NCTC analysts are permitted to access. NCTC is thus dependent on the owning entity to take any necessary steps to enable compliance with the ODNI AG Guidelines and NCTC Implementation Procedures, such as the ability to conduct audits of NCTC analyst queries. In the case of datasets owned by other federal departments or agencies, NCTC relies on their compliance regimes to provide access, training, auditing, and prevention of unauthorized data access or use. Such reliance by NCTC is appropriate given the common federal information security regime laid out by statute in the Federal Information Security Modernization Act, standards set by the National Institute of Standards and Technology, and guidance from the Office of Management and Budget and Department of Homeland Security.[141]

In the case of datasets owned and controlled by commercial vendors, there does not appear to be a common information security and auditing framework applicable to each vendor. Commercial vendors are not generally subject to federal information security standards unless imposed contractually and should not be presumed to be meeting such standards, absent clear contractual commitments. NCTC should apply a comprehensive compliance framework that addresses information security risks and auditing requirements for commercial vendors that own or control datasets that NCTC analysts access via the access paradigm. Such a framework should address training requirements, user behavior agreements, encryption requirements, incident response procedures, audit requirements, and other elements typically required by an information security program. This framework should be agreed to contractually between NCTC and each commercial vendor who owns or controls the relevant datasets, to ensure commercial vendors are providing appropriate protections.

[139] Data owners that are non-federal government entities are likely to primarily include commercial data vendors but may also include state, local, tribal, and territorial governments or international data providers. For simplicity, I use the term commercial vendors throughout this statement, but this term should be understood to apply to all non-federal government entities that may provide data to NCTC.
[140] *See* ODNI AG Guidelines §§ 10.1 ("**Access** means the viewing or examining of information by the ODNI for official purposes, where the information viewed or examined is not stored or otherwise maintained under the control of the ODNI. Access is distinct from collecting or obtaining information.").
[141] *See* 44 U.S.C. §§ 3551 *et seq.*; NIST SP 800-53 Rev. 5.

With regards to audits, NCTC should ensure that there is a mechanism to automatically record the query terms used by NCTC analysts to query commercial databases, to enable NCTC to comply with the query standard. In addition, NCTC should incorporate into the framework an audit logging schedule equivalent to that required under federal information security standards. If necessary, the framework should permit NCTC access to the audit logs pertaining to NCTC analysts who query data maintained or processed in the commercial vendor datasets. To be clear, this need not require NCTC to access the entirety of the commercial vendor's audit but only the subset applicable to NCTC analysts.

NCTC should seek to hold commercial vendors to the same information security standards that NCTC and other federal agencies and departments would be held to. Any deviation should be clearly identified as part of the overall framework and describe the reason for such deviation (i.e., the commercial entity meets a similarly equivalent private-sector standard such as ISO 27001). In general, such deviations from the common compliance framework should provide equivalent or greater protection as the impacted federal information security standard. If the deviation may provide less protection, NCTC should clearly document the risk acceptance methodology and criteria for accepting such lesser protection and ensure any such deviation still enables NCTC to comply with the ODNI AG Guidelines and NCTC Implementation Procedures.

ANNEX B: SEPARATE STATEMENT OF BOARD MEMBER BETH A. WILLIAMS

I join in the Board's Report with one exception, and one further recommendation. First, I disagree with Recommendation 1 to the extent that the Board seeks at this time to apply additional requirements to evaluated information. Second, I would add another recommendation to the Report: NCTC should revise its Implementation Procedures to reflect the congressional limitation on NCTC's activities concerning purely domestic terrorism.

I. The Board Needs More Information to Determine the Appropriate Scope of Recommendation 1.

I agree with the Board that requiring NCTC analysts to record their written justification for U.S. person queries in unevaluated information would help ensure that the query standard is met, and would better facilitate periodic audits. Indeed, my former colleague, Richard DiZinno, and I previously endorsed the legislative codification for such a requirement in the context of FBI queries of unevaluated Section 702 information.

I therefore agree with the thrust of Recommendation 1. I disagree, however, with the current scope of the Recommendation to the extent the Board suggests through footnote 117 that this requirement would apply to evaluated, as well as unevaluated, information. The Board does not have enough information at this time to assess the implications of such a requirement.

Unlike unevaluated information, evaluated information has been examined to determine "whether it relates to an authority and responsibility" of the Intelligence Community (e.g. terrorism information), "whether it contains any information concerning U.S. persons," and "whether that information meets retention criteria and thus may be retained."[142] That means such information has already been subject to some level of review for legal and privacy and civil liberties protection, as opposed to "raw" intelligence information that has not been so evaluated. The concerns with querying evaluated information are therefore somewhat lower than with regard to querying unevaluated information.

Evaluated information in this context could include anything from finished intelligence products (which the Board exempts from its requirement) to information in the Terrorist Identities Datamart Environment (TIDE), the government's database on known or suspected terrorists (which the Board does not exempt from its requirement). It likely includes many other categories

[142] Nat'l Counterterrorism Ctr., IMPLEMENTATION PROCEDURES FOR THE ODNI INTELLIGENCE ACTIVITIES PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 (2021), § 10.18.

of data as well. Written justification requirements have generally not been applied to evaluated information.

The Board has not asked NCTC to engage in a systematic review of the types of evaluated data in order to inform a determination as to whether applying a wholesale written requirement justification across the board is either feasible or advisable. Nor has the Board had the opportunity to weigh the added burden of the requirement against the anticipated privacy benefits. This balance could understandably differ based upon different datasets.[143]

Rather than taking the approach expressed in footnote 117, I would either limit the application of the recommendation to unevaluated information at this time, or request that NCTC engage in a 60- or 90-day review of the datasets to which its analysts have access, the configuration of its systems, and its existing policies and procedures with regard to these datasets to inform our determination of the scope of the proposal.

II. NCTC Should Revise its Implementation Procedures to Reflect the Congressional Limitation on NCTC's Activities Concerning Purely Domestic Terrorism.

As described in the Report, Congress has circumscribed NCTC's role with regard to domestic terrorism by directing it not to prepare or contribute to intelligence products without a foreign nexus. This limitation reflects longstanding concern about protecting the privacy and civil liberties for U.S. persons in a counter-terrorism center that has been structured largely to address foreign and foreign-inspired threats.[144] I share those concerns. Domestic terrorism poses a serious and continuing threat to the American public. But the Federal Bureau of Investigation has the primary mission of conducting intelligence gathering and law enforcement operations within the country. For purposes of this Report, we have not assessed whether NCTC's assistance is necessary to supplement that work, or if such expanded mission justifies what could be additional exposure and dissemination of U.S. person information.[145]

Nonetheless, it is a matter of good governance to ensure that NCTC's Implementation Procedures reflect and incorporate NCTC's current internal policy guidance, which significantly narrows its domestic terrorism-related work in accordance with congressional direction.

[143] The Board effectively acknowledges this fact when it provides an exemption from the proposed recommendation for finished intelligence products. In the absence of more investigation, however, the Board cannot be sure that the exemption is appropriately calibrated to cover other types of evaluated information for which the benefit would outweigh the burden.

[144] *See, e.g.*, Todd M. Masse, THE NAT'L COUNTERTERRORISM CTR: IMPLEMENTATION CHALLENGES AND ISSUES FOR CONGRESS, 10 (2005) ("[T]he possibility exists that unintentional mission creep and operational zeal could lead to situations in which rules designed to guide traditional foreign intelligence collection may be applied to U.S. persons.").

[145] The Board is currently engaged in a separate oversight project on domestic terrorism where those questions could be addressed.

Amending the Implementation Procedures would prevent any potential confusion or perceived conflict between the internal guidance and the Implementation Procedures, and would emphasize to persons at the agency—many of whom are detailed from across the Intelligence Community—the significance of the congressional limitation. It would therefore help to ensure NCTC's fidelity to the restriction and to increase public and congressional confidence in NCTC's compliance with it.

I agree with the Board's statement that "[u]pdating the Implementation Procedures explicitly to include the prohibitions and required processes now contained in internal guidance would provide helpful additional clarity."[146] I would go a step further formally to recommend it.

[146] *See supra* at p.10.