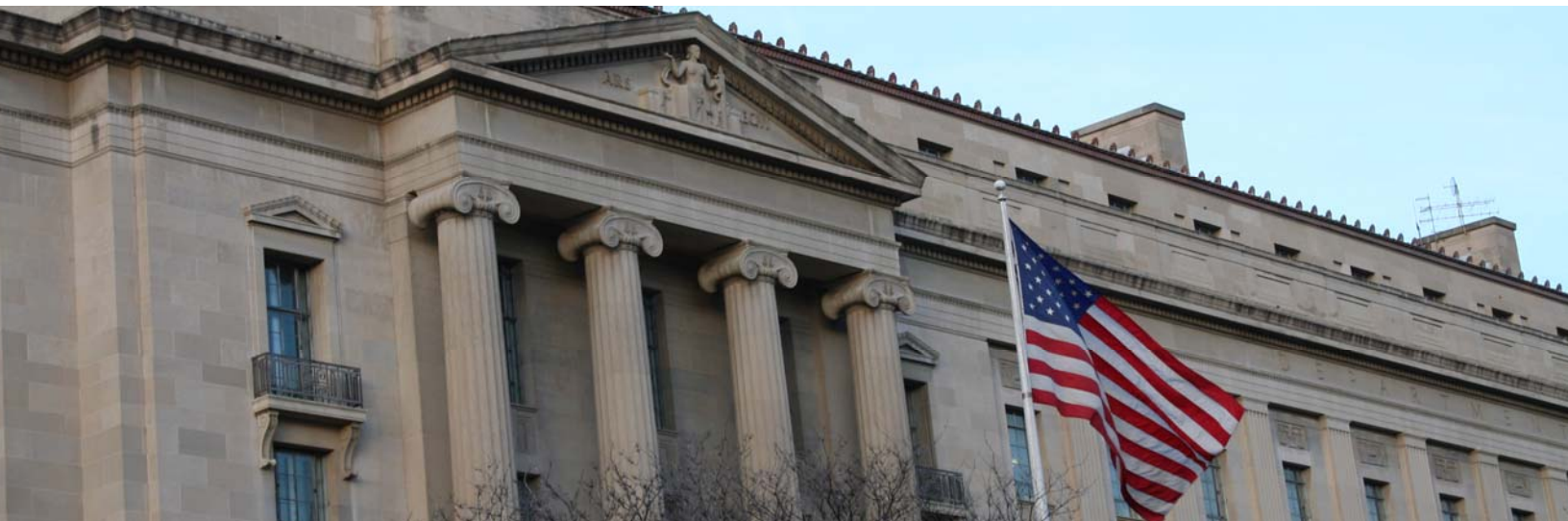




## Office of the Inspector General U.S. Department of Justice

**OVERSIGHT ★ INTEGRITY ★ GUIDANCE**



# A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data

Oversight & Review Division 19-01

March 2019  
(Revised March 2025)

## NOTICE

---

This report was originally issued on March 28, 2019. The report included the following Notice page:

The Drug Enforcement Administration (DEA) and another government entity determined that portions of this report constitute Law Enforcement Sensitive (LES) information. Those portions have been redacted to enable the issuance of this public version of the report. Issuance of this report follows efforts by the Office of the Inspector General (OIG), the DEA, and the other government entity to agree on the scope of the redactions. The OIG continues to believe that some redacted material is not LES, but defers to the judgment of DEA and the other government entity. This public version of the report contains an Executive Summary without any redactions.

Consistent with the OIG's ordinary practice, the full, unredacted report has been produced to the DEA, the Department of Justice, and to relevant Congressional oversight committees.

In the years following the report's issuance, the OIG received inquiries from congressional oversight committees regarding the information about a particular program described in the report—the Hemisphere program—that was redacted in the public version of the report based on LES determinations made by DEA and another government entity, and whether that information was appropriately designated as LES. In light of these inquiries, and the OIG's own disagreement with some of the LES determinations that were made by DEA and the other government entity, the OIG requested that the DEA conduct an updated sensitivity review of the report.

The version of the report issued on March 11, 2025, reflects the results of the DEA's updated sensitivity review of information in the report about the Hemisphere program, which is described primarily in Chapter Five of the report. This version of the report makes public a substantial amount of information that was previously redacted as LES based on determinations made by DEA and another government entity. This information appears on the following pages:

- Table of Contents, pages vi to vii
  - Chapter Five, pages 75-91
  - Chapter Six, pages 102-106, 120-121
-





# Executive Summary

## *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data*

The Department of Justice Office of the Inspector General (OIG) conducted a review of the Drug Enforcement Administration's (DEA) use of its administrative subpoena authority under 21 U.S.C. § 876(a) to collect or exploit "bulk data."<sup>1</sup> Section 876(a) authorizes the DEA to issue administrative subpoenas, without court or other approval outside the agency, requiring the production of records that are "relevant or material" to certain drug investigations. 21 U.S.C. § 876(a).

For purposes of this review, we relied on the Department of Justice's (Department or DOJ) definition of a "bulk collection" of data as a collection of a significant amount of data that is unrelated to an individual, group, or entity that is a target of an investigation, where the data is acquired or updated periodically on an ongoing basis. Typically, a "bulk collection" of data captures records relating to broad categories of transactions, such as the non-content records of all telephone calls handled by a particular telecommunications service provider. Collections of bulk data may include millions or even billions of data points and are often loaded into computers and analyzed by means of automated searches. The relevance of any individual record within the large-scale collection (such as a record of a single phone call) to a specific open investigation is typically not determined until *after* the bulk collection is acquired and queried.

### The Programs

Our report addresses three programs in which the DEA has used its administrative subpoena authority to collect or exploit bulk data in recent years. The DEA has identified all of the programs discussed in this report as Law Enforcement Sensitive. Accordingly, we have removed program names and some operational details about the programs to enable issuance of this public Executive Summary.

**Program A:** Program A is a federal interagency data analysis program spearheaded by the DEA, but initiated with the approval of DOJ leadership. From the 1990s until mid-2013, as part of Program A, the DEA issued "non-target-specific" subpoenas to multiple telecommunications service providers to amass an extremely large collection of bulk telephone call records ("Collection 1"). The Collection 1 subpoenas were "non-target-specific" in that they were not directed at or related to particular identifiable investigations or targets. Rather, the Collection 1 subpoenas required the production of records for all calls made from the United States over a recipient company's telecommunications network to countries that the DEA determined had a "nexus to drugs." The call records that were collected, also known as "telephone metadata," included the originating and receiving telephone numbers and the date, time, and duration of the call, but did not include the content of any calls or subscriber information.

Under Program A, the DEA used Collection 1 data together with other data to create analytic products for investigations. Investigators from the DEA or other participating federal agencies contacted a Program A Staff Coordinator and provided relevant facts regarding the connection between a target telephone number and an active case. The Staff Coordinator reviewed the request to determine if it contained a sufficient basis connecting the target number with an active case, referred to as "reasonable articulable suspicion" (RAS). Once the request was approved, the DEA created Program A investigative products by using the target number to query the Collection 1 dataset and other records in order to identify calls made to or from that target number and in some cases a more in-depth analysis of a target's telephone contacts to identify relevant investigative links. The resulting analytical products were sent back to the requesting office for use in investigations.

<sup>1</sup> Department of Justice Inspector General Michael E. Horowitz recused himself from this review because he occupied senior management positions within the Criminal Division from 1999 through 2002, a time period during which DEA operated, with Criminal Division involvement, one of the programs examined herein. We did not interview Mr. Horowitz or review his conduct because of the inherent conflict for this

office to evaluate the role of the Inspector General. Although auditing standards are not applicable to this review, which is not an audit, they provided useful guidance on his issue. See Generally Accepted Government Auditing Standards (December 2011).





# Executive Summary

## *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data*

In the summer of 2013 the Department suspended issuance of Collection 1 administrative subpoenas and usage of existing Collection 1 bulk data. Shortly thereafter, Program A was significantly modified to eliminate the use of the non-target-specific Collection 1 subpoenas for bulk collection of telephone metadata. Instead, in 2014, the DEA began issuing periodic subpoenas to one or more telecommunications service provider(s) for telephone metadata related to telephone numbers that the DEA or other participating federal agency had determined was relevant to specifically identified investigations. Each such subpoena aggregates a large number of targeted requests in specific cases into a single subpoena. Under this target-specific approach (Collection 2), the telecommunications service provider/subpoena recipient, rather than the DEA, queries a bulk telephone metadata collection that it maintains for its own business purposes. DEA guidance requires that investigators requesting Program A products containing Collection 2 data demonstrate that RAS exists that a target number is being used in the conduct of criminal activities. After the service provider delivers the responsive telephone metadata for calls to or from the target numbers, the DEA generates similar Program A analytical products for the requesting federal agencies as were generated during the Collection 1 era. Program A, modified by the target-specific Collection 2 approach, remains active.

**Program B:** Program B involved the use of administrative subpoenas from 2008 to 2013 to collect bulk purchase data for a particular good or service sold by selected vendors. The administrative subpoenas for Program B data were not directed at or related to particular identifiable investigations or targets. Instead, the Program B subpoenas were issued periodically to selected vendors of the particular good or service and required production of customer information for each purchase of the good or service. The DEA then queried the responsive Program B bulk purchase data provided by the vendors against various law enforcement databases to identify any matches, or "hits," in order to identify potential targets for further investigation. In September 2013, following inquiries from the OIG regarding Program B, the DEA stopped issuing

administrative subpoenas in connection with this program.

**Program C:** Program C is a contractual service program, initiated by a non-DOJ government entity in 2007, under which a telecommunications service provider maintains and analyzes its own collection of bulk telephone metadata for billions of calls to produce expedited or advanced telephone analytical products in response to target-specific administrative subpoenas from law enforcement agencies, including DEA. Program C does not include the content of calls. Among other things, upon receiving an administrative subpoena, the provider can analyze its own bulk data collection to generate reports that identify unique connections to target phone numbers. The provider maintains and queries the bulk collection; the DEA's administrative subpoenas for Program C products are issued for particular identifiable investigations or targets. Although this program is not one that the DEA owns, the DEA is a major customer for Program C products. Program C remains active.

## Findings

### Sufficiency of Legal Reviews

Our review found that the DEA (and the Department with respect to Program A, Collection 1) failed to conduct a comprehensive legal analysis of the DEA's use of its administrative subpoena authority to collect or exploit bulk data before initiating or participating in any of the three programs. We found this failure troubling with respect to Program A, Collection 1 and Program B because these programs involved a uniquely expansive use of Section 876(a) authority to collect data in bulk without making a prior finding that the records were, in the language of that statutory provision enabling DEA's subpoena authority, "relevant or material" to any specific defined investigation. Several published court decisions have clearly suggested potential challenges to the validity of the DEA's use of its statutory subpoena power in this expansive, non-targeted manner. We also found the absence of a robust legal review troubling because the DEA utilized the bulk data collected by means of Program A, Collection 1 and Program B





# Executive Summary

## *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data*

subpoenas on an unknown number of occasions in support of investigations by non-DEA federal agencies that had no apparent connection to specific drug investigations. This utilization raised significant legal questions because the DEA had amassed the Program A, Collection 1 and Program B bulk data collections under its statutory authority, in 21 U.S.C. § 876(a), to require the production of data that was "relevant or material" to a *drug* investigation.

We found that Program C raised different kinds of challenging legal issues that the DEA also failed to fully assess. We found that the DEA failed to formalize a complete and adequate legal assessment regarding its use of Program C to obtain reports and other advanced analytical information to ensure such use was lawful and appropriate under its administrative subpoena authority, 21 U.S.C. § 876(a), and the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)(2).

### **Adequacy of Procedural Safeguards**

We found that the DEA's procedural safeguards for Program A, Collection 2 are not sufficiently clear or strong enough to ensure compliance with the requirement under Section 876(a) that the information being demanded is "relevant or material" to a drug investigation. The DEA's guidance document instructed users to identify RAS on an electronic request form by selecting from a fixed "drop-down" list that contains only generic categories of *sources* from where an investigator might have learned about the target number, such as a confidential informant. This procedure did not provide any particularized factual basis on which to assess whether the requisite level of "relevance" under Section 876(a) exists between the target number to be included on the Collection 2 subpoena and the underlying investigation. Additionally, the electronic form only contained one section, a "Remarks" section, where specific facts connecting the requested target number to the underlying investigation could be documented. However, the DEA's procedures lacked standards or written guidance on what the "Remarks" section must contain. In practice, the DEA typically did not require more "particularization" than a single conclusory sentence, and did not explicitly require the

documentation or certification that the request was relevant to a *drug* investigation, as required for a Section 876(a) subpoena.

We also found that the DEA failed to establish any policies on storage or retention of the Program B bulk data at any time before or during the operation of that program. Although Program B is no longer active, the DEA has failed to develop a final disposition plan regarding tens of thousands of records of purchases that reside on DEA servers. Without such a plan, there is a risk that the data will be retained for a substantial period.

### **Efficacy of Audits**

We determined that the DEA's current audit practices do not meaningfully examine whether the Collection 2 subpoenas issued by the DEA in response to Program A product requests comply with the requirement in 21 U.S.C. § 876(a) that the information requested be "relevant or material" to a Title 21 drug investigation. These audits consisted mainly of confirming that each of the thousands of requests from the DEA and other participating federal agencies included a selection of one of the fixed drop-down selections for RAS. The DEA's current audit practices fail to scrutinize the "Remarks" section of the form where the only substantive information about "relevance" may appear. But, as noted above, the information provided in this section often lacks specificity sufficient to establish the particularized facts or basis for connecting the target number to a drug investigation, even if such review had occurred. We determined that the current version of the Program A request form does identify the requester and case number, which information would enable an auditor to track a Program A product request to the case file and interview the requester to assess whether the necessary predication for the request existed.

### **Use of Parallel Construction**

In order to protect the unique capabilities of Program A and Program C, agents and analysts are instructed not to use the information provided in the analytical products in affidavits, pleadings, or the like, and to keep them isolated from the official files. Users are





# Executive Summary

## *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data*

instructed to "parallel construct" the information obtained in these products before using it in reports or court proceedings. This may require, for example, issuing a new, target-specific administrative subpoena to a telephone service provider for the relevant telephone numbers identified in the Program A investigative product that were determined to be related to the investigation.

We found that there is nothing inherently inappropriate about using parallel construction to re-create information originally derived from a confidential program for use as evidence in court filings, such as warrant applications, or even at trial. This practice is analogous to using conventional investigative techniques to confirm a fact initially disclosed to a law enforcement agency in a confidential tip. However, parallel construction should not be used to prevent prosecutors from fully assessing their discovery and disclosure obligations in criminal cases. While the DEA has denied misusing parallel construction in this manner, we found some troubling statements in the DEA's training materials and other documents, including that Program A investigative products cannot be shared with prosecutors. Such statements appear to be in tension with Department policy on a federal prosecutor's "duty to search" for discoverable information from all members of the "prosecution team," which typically includes federal law enforcement officers who participated in the investigation of the defendant.

### Recommendations

In total, the OIG made 16 recommendations to the DEA to address the issues and concerns identified during our review, including the following:

- Before initiating or reinstating a "bulk collection" program by use of non-target-specific administrative subpoenas, the DEA should conduct a rigorous written legal assessment that specifically addresses whether 21 U.S.C. § 876(a) authorizes the issuance of non-targeted subpoenas for exploratory or target-development purposes, and the permissible

conditions under which such bulk data may be shared with other federal agencies for non-drug purposes.

- The DEA should issue a final legal opinion and updated policy on Program C and its permissible uses.
- The DEA should modify the electronic request form for Program A products to require more particularized documentation of the information to establish RAS and certification that the request pertains to a drug investigation.
- The DEA should develop legally supportable criteria for retention of Program B data collected by use of administrative subpoenas, and policies for the disposition of such bulk data.
- The DEA and other participating federal agencies should conduct periodic audits, on a set schedule, of an appropriate sample of Program A product requests to confirm, by tracking to the investigation from which the request originated, that there was an adequate particularized factual basis sufficient to establish RAS that the target number was relevant or material to an ongoing drug investigation.
- The Department should undertake a comprehensive review of "parallel construction" policies and practices with respect to Program A and Program C investigative products to ensure that these policies and practices do not conflict with the government's discovery and disclosure obligations in criminal cases, or Department policy on this subject, and that the Department's and DEA's guidance and training materials on this subject be clarified as warranted.



## TABLE OF CONTENTS

CHAPTER ONE INTRODUCTION .....	1
I. Background .....	1
II. Methodology .....	4
III. Organization of the Report.....	5
IV. Access Issues .....	5
CHAPTER TWO RELEVANT STATUTES, REGULATIONS, RULES, AND POLICIES ...	8
I. Statutory and Constitutional Provisions .....	8
A. 21 U.S.C. § 876 (Administrative Subpoenas) .....	8
B. 18 U.S.C. § 2703 (Electronic Communications Privacy Act).....	9
C. Fourth Amendment and the Third-Party Doctrine.....	10
II. 28 C.F.R. § 0.104, App., Sec. 4 (DEA and FBI Personnel Authorized to Issue Subpoenas).....	12
III. DEA Agents Manual .....	12
A. Business Records Generally .....	12
B. Subscriber/Toll Records.....	14
C. Documentation Requirements .....	14
CHAPTER THREE THE [REDACTED] PROGRAM .....	15
I. The [REDACTED] Collection .....	15
A. The [REDACTED] Subpoenas .....	16
B. The [REDACTED] Analytical Products.....	18
C. Use of [REDACTED] Products in Drug Investigations.....	20
D. Use of [REDACTED] Data in Non-Drug Investigations.....	21
E. Programmatic Safeguards .....	24
1. Reasonable Articulable Suspicion (RAS) .....	26
2. Auditability of Queries.....	28
F. Legal and Legislative Oversight.....	30
1. Early Years .....	30
2. The August 1999 Memorandum.....	31
3. [REDACTED].....	33
4. Congressional Oversight.....	35
G. Termination of the [REDACTED] Collection .....	35

<b>II.</b>		<b>37</b>
A.		39
B.		39
C.		41
D.		41
E.		42
F.		42
	1. Relevance and Reasonable Articulate Suspicion (RAS)	43
	2.	50
G.	Legal Oversight	52
<b>CHAPTER FOUR</b>		<b>54</b>
<b>I.</b>	<b>The Collection</b>	<b>54</b>
A.	The Subpoenas	55
B.	Receipt of Data and Dissemination of Leads to Field	57
	1. Dissemination of Raw Data (2008–2013)	57
	2. Expanded Headquarters Efforts to Enhance the Value of Data (2013-2014)	61
C.	Maintaining the Confidentiality of the Program	64
D.	Storage and Retention	65
	1. Bulk Data on Original CDs	65
	2. Bulk Data in Module	66
	3. Bulk Data Stored Elsewhere	66
<b>II.</b>	<b>Legal Review of</b>	<b>66</b>
A.	Initial Review in September 2008	66
B.	FBI Concerns at the Fusion Center in May 2013	69
C.	OCC's Review before OIG Meeting in August 2013	71
<b>III.</b>	<b>DEA Stops Issuing Subpoenas</b>	<b>72</b>
<b>IV.</b>	<b>DEA Assessments of Value of the Program</b>	<b>73</b>
<b>CHAPTER FIVE THE HEMISPHERE PROGRAM</b>		<b>75</b>
<b>I.</b>	<b>Elements of the Hemisphere Program</b>	<b>76</b>
A.	The Data Used in the Hemisphere Program	76
B.	The Hemisphere Analytical Products	76
	1. Basic Product	76



2.	Advanced Product .....	77
3.	.....	77
C.	Value of Hemisphere Products to the DEA .....	78
D.	The Hemisphere Subpoenas .....	78
E.	Administration of the Hemisphere Program.....	79
F.	.....	81
G.	.....	82
<b>II.</b>	<b>Legal Review of Hemisphere .....</b>	<b>83</b>
A.	Field Request for Legal Review in August 2007.....	83
B.	Field Request for Legal Guidance in 2008 .....	83
C.	FBI Request for Legal Guidance in 2010 .....	85
D.	OCC Review in 2012-2013 .....	88
	<b>CHAPTER SIX ANALYSIS AND RECOMMENDATIONS .....</b>	<b>92</b>
<b>I.</b>	<b>OIG Assessment of the Adequacy of Legal Review Conducted for the Bulk Collection Programs .....</b>	<b>92</b>
A.	.....	93
1.	Legal Validity under Section 876(a) .....	93
2.	Querying the ..... Data for Non-Drug Investigations .....	98
B.	.....	99
C.	.....	100
D.	.....	101
E.	Recommendations Regarding Legal Review .....	105
1.	Bulk Collections by Administrative Subpoena .....	105
2.	.....	106
<b>II.</b>	<b>OIG Assessment of Procedural Safeguards .....</b>	<b>106</b>
A.	Safeguards to Ensure Compliance with Section 876(a) and to Prevent Misuse of Collections .....	106
1.	Relevance and RAS in ..... .....	106
2.	..... .....	109
3.	Recommendations Regarding ..... Procedures for Establishing Relevance under Section 876(a) .....	112
B.	..... .....	114
1.	..... .....	114
2.	..... .....	115

■ [REDACTED]	115
III.   OIG Assessments and Recommendations Regarding Audits	117
A.   [REDACTED]	117
B.   [REDACTED]	119
IV.   Parallel Construction	121
V.    General Updates to Policies and Training	124
VI.   Conclusion	125
APPENDIX A: Timeline Of Key Events	A-1
APPENDIX B: Office of the Deputy Attorney General's Response	B-1
APPENDIX C: Drug Enforcement Administration's Response	C-1



# CHAPTER ONE

## INTRODUCTION

### I. Background

This report examines the Drug Enforcement Administration's (DEA) use of its administrative subpoena authority under 21 U.S.C. § 876(a) to collect or exploit "bulk data."<sup>1</sup> For purposes of this review, we relied on the Department of Justice's (Department or DOJ) definition of a "bulk collection" of data as a collection of a significant amount of data that is unrelated to an individual, group, or entity that is a target of an investigation, where the data is acquired or updated periodically on an ongoing basis.<sup>2</sup> Typically, a "bulk collection" of data (often referred to herein as "bulk data") captures records relating to broad categories of transactions, such as all purchases of a given item or all telephone calls to a broad set of geographic areas. The relevance of any individual record within the collection (such as a record of a single phone call or purchase) to a specific open investigation is not determined until *after* the bulk collection is acquired. Collections of bulk data may include millions or even billions of data points and are often loaded into computers and analyzed by means of automated searches. As described herein, in some cases the DEA uses its administrative subpoena authority to benefit from a company's ability to exploit collections of bulk data maintained by the company. Further, none of the bulk collections that we examined included the *content* of private communications.

The government's use of collections of bulk data for counter-terrorism investigative purposes became the subject of great public interest when Edward J. Snowden made public disclosures in June 2013 indicating that the National Security Agency (NSA) was collecting billions of telephone call records, or telephone metadata, encompassing every call made through the systems of certain telecommunications providers where at least one end of the communication was located in the United States.<sup>3</sup>

---

<sup>1</sup> Department of Justice Inspector General Michael E. Horowitz recused himself from this review because he occupied senior management positions within the Criminal Division from 1999 through 2002, a time period during which DEA operated, with Criminal Division involvement, one of the programs examined herein. We did not interview Mr. Horowitz or review his conduct because of the inherent conflict for this office to evaluate the role of the Inspector General. Although auditing standards are not applicable to this review, which is not an audit, they provided useful guidance on his issue. See Generally Accepted Government Auditing Standards (December 2011).

<sup>2</sup> The Office of the Deputy Attorney General used this definition to identify the scope of "bulk collection" programs in DOJ components in the wake of the Edward J. Snowden disclosures in June 2013 regarding the National Security Agency's bulk telephone metadata collection program. For purposes of this review, we applied this definition to such collections amassed by the DEA through its subpoena power, or amassed by private companies and exploited on behalf of the DEA upon receipt of a subpoena.

<sup>3</sup> Telephone call records or telephone metadata include transactional details regarding a call, such as the date and time of a call, but do not include the content of the communications.

Several contemporaneous events after the Snowden disclosures led the Department of Justice Office of the Inspector General (OIG) to initiate this review. Later in the summer of 2013, the OIG learned about the DOJ/DEA's involvement in a bulk telephone metadata collection program, known as [REDACTED] in which bulk data involving calls made from the United States to certain other countries was acquired by means of administrative subpoenas issued to telephone carriers. [REDACTED]

[REDACTED] Also in 2013, the OIG learned that the DEA was using administrative subpoenas to collect bulk information about [REDACTED] (National [REDACTED] Initiative or [REDACTED]), and that the FBI had raised concerns about the DEA's legal authority for that collection. In each of these programs, the DEA was relying on its delegated authority under 21 U.S.C. § 876(a) to issue administrative subpoenas, without court or other approval outside the agency, requiring the production of records that are "relevant or material" to certain narcotics investigations.

In prior investigations relating to the Department's use of telephone metadata, the OIG found problems with the FBI's use of National Security Letters, exigent letters, and other informal requests to obtain the production of non-content telephone records from communications service providers.<sup>4</sup> Also, since 2005, Congress has directed the OIG to conduct four comprehensive reviews of the FBI's use of its investigative powers under Section 215 of the Foreign Intelligence Surveillance Act (FISA) to ensure, among other things, that there has been no improper usage of this authority and to assess the adequacy of safeguards established to protect privacy.<sup>5</sup>

The information the OIG learned about the DEA's use of its administrative subpoena authority to obtain similar non-content telephone records in bulk raised questions that we believe are of potential interest to DOJ leadership, the Congress, and the public. Among these were whether the DEA had adequately

---

<sup>4</sup> See, e.g., U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (January 2010); U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2007). Although these investigations related to intelligence investigative authorities, the legal and policy issues addressed in them have relevance to the issues addressed in this report.


<sup>5</sup> See, e.g., U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records* (March 2007); U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records 2012 through 2014*, Oversight and Review Report 16-04 (September 2016). Classified portions of prior OIG reports on this subject identified the NSA's bulk telephone metadata collection program through the FBI's use of its Section 215 authority. However, only a very limited number of individuals within the Department and Congress were authorized to receive that classified information prior to the Snowden disclosures.



confirmed that it had legal authority to collect bulk data using administrative subpoenas, and whether the DEA had implemented adequate safeguards limiting the retention of bulk data and ensuring that these data collections were protected from unauthorized use by agency employees. Additionally, the OIG had not previously reviewed the DEA's practices in this area, but had done so several times, as noted above, with regard to the FBI.

Concerns regarding the government's ability, through broad subpoena power, to amass private data in bulk have also been the subject of law review commentaries for at least 50 years.<sup>6</sup> Apprehensions about the tension between privacy rights and legitimate and lawful government intrusions have become even more acute in today's advanced computerized society where a wealth of information on people's daily activities is stored electronically by businesses and organizations and accessible to government by subpoena.<sup>7</sup>

Our report addresses three programs in which the DEA has used its administrative subpoena authority to collect or analyze bulk data in recent years. Two of these programs involved the collection or exploitation of bulk telephone metadata:



---

<sup>6</sup> See, e.g., Richard S. Miller, *Administrative Agency Intelligence Gathering: An Appraisal of the Investigative Powers of the Internal Revenue Service*, 6 B.C. Indus. Com. L. Rev. 657, 715-16 (1965) (concluding that "one must not be blind to the dangers [from] an agency [that used its investigatory powers to establish a bulk data collection for use by all other government agencies] would cause to the right to be let alone and to the concomitant protection against the tyranny of petty officialdom which that right affords, for these constitute part of the fabric of a society where governmental interference with individual privacy has been the exception rather than the rule."); Lynn Katherine Thompson, *IRS Access to Bank Records; Proposed Modifications in Administrative Subpoena Procedure*, 28 Hast. Law Journal 247, 281 (1976) (concluding that vast repositories of personal information held by banks, telephone companies, and other third parties were not adequately restricted from government access by administrative subpoena in the "highly computerized society" of the 1970s); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1084 (2002) (expressing concern that ease of government access by subpoena to commercial digital files on people represents "one of the most significant threats to privacy of our times"); and Christopher Slobogin, *Transaction Surveillance by the Government*, 75 Miss. Law. J. 139 (2005) (expressing similar concerns that government access by subpoena to digital records of highly personal activities held by third parties is subject to insufficient legal restrictions).

<sup>7</sup> See *Am. Civil Liberties Union, et al., v. Clapper, et al.*, 785 F.3d 787, 794 (2d Cir. 2015) (citing alleged privacy concerns from bulk metadata collections in today's technological capacity for automated, large-scale reviews).

[REDACTED]<sup>8</sup> The third program addressed in our report, [REDACTED], involved the use of administrative subpoenas to collect purchaser information for every sale of a [REDACTED] by certain major sellers of such devices.<sup>9</sup>

The [REDACTED] program was significantly modified in 2013 to eliminate the use of non-target-specific [REDACTED] subpoenas for bulk calling data. [REDACTED]

[REDACTED] This target-specific approach is called [REDACTED] As modified to incorporate [REDACTED], the [REDACTED] program remains active. [REDACTED] DEA suspended [REDACTED] in 2013.

In examining these programs, we explored (1) the DEA's legal authority for the acquisition or use of these data collections; (2) the policies and procedural safeguards established by the DEA with respect to the collection, use, and retention of the data, including procedures to prevent misuse; (3) the DEA's creation, dissemination, and use of products generated from the data; and (4) the DEA's use of "parallel construction" or other techniques to protect the confidentiality of these programs.<sup>10</sup> A timeline of key events relevant to this review is provided in Appendix A to this report.

## **II. Methodology**

To investigate the above issues, we reviewed more than 175,000 pages of classified and unclassified documents related to the DEA's administrative subpoena usage generally or to one or more of the three programs. These materials included analyses, briefing materials, charts, guidance documents, internal memoranda, investigative materials, policy and procedural manuals, reports, representative subpoenas, and training documents. We also obtained materials from several DOJ components besides the DEA that had materials related to the issues under investigation. These DOJ components were: the Office of the Deputy Attorney General, the Criminal Division, the Federal Bureau of Investigation, and the Office of Legal Counsel. Additionally, we reviewed thousands of pages of emails from the accounts of relevant Department personnel at the DEA and other DOJ components.

---

<sup>8</sup> [REDACTED]

<sup>9</sup> When we initiated this review, we sought information regarding the DEA's use of administrative subpoenas for "bulk collection" since 2008. The DEA identified [REDACTED] and [REDACTED] as the only programs involving the use of administrative subpoenas in this manner during this period.

<sup>10</sup> Parallel construction is a DEA term of art that appears in DEA materials for certain DEA programs. According to the Office of the Deputy Attorney General, the Department does not generally utilize this term for this process in other contexts.

We also conducted more than 50 interviews over the course of our review. These interviews covered a wide range of personnel with operational and managerial responsibility related to the DEA's use of administrative subpoenas in the programs we focused on, or generally, including Special Agents, Intelligence Analysts, Program Analysts, Division Counsel and Department lawyers, Staff Coordinators, Section Chiefs, Office Chiefs, Assistant Special Agents-in-Charge, and several other managerial personnel.

### **III. Organization of the Report**

This report is divided into six chapters, including this Introduction. Chapter Two describes the statutes, regulations, rules, and policies relevant to this review. In Chapter Three we describe the [REDACTED] program, which over time has incorporated two different approaches for using administrative subpoenas to exploit bulk telephone metadata in support of investigations conducted by the DEA and other agencies. In Chapter Four we describe [REDACTED], a DEA program that used administrative subpoenas to collect bulk data regarding purchases of [REDACTED] to identify targets for new investigations. [REDACTED]

[REDACTED] In Chapter Six we present the  
OIG's analysis and recommendations.

### **IV. Access Issues**

For a substantial period after we initiated this review, the DEA took many actions that hindered the OIG's access to information available to it that the OIG was plainly authorized to obtain under the Inspector General Act.<sup>11</sup>

These actions included failing to produce or delaying the production of relevant and responsive materials without any compelling or sufficient basis.

[REDACTED] Additionally,  
the DEA provided the OIG with heavily redacted materials on several occasions and engaged in a lengthy sensitivity screening of emails prior to providing them to the OIG. Further, the OIG discovered many highly relevant documents, which had not been produced, only after learning about them in witness interviews. This latter issue was particularly significant with respect to the dearth of

---

<sup>11</sup> 5 U.S.C. app. 3 §§ 4, 6. See also Select Committee to Study Governmental Operations with Respect to Intelligence Activities, S. Rep. No. 94-755, Book II, at IX, n.7 (1976) (This Senate Select Committee, commonly referred to as the "Church Committee" after then-Chairman, Senator Frank Church, declared that the "most important lesson" derived from their review was that "effective oversight is impossible without regular access to the underlying working documents of the intelligence community") (emphasis added).



documents containing legal reviews of programs in our review, which the DEA failed to produce to the OIG until a witness identified their existence to us. The DEA's actions significantly delayed our review and were wholly inconsistent with the requirements of the Inspector General Act.

The OIG's access to information from the DEA began to improve after high-level communications between the OIG and the DEA in December 2014, and subsequent involvement by the Office of the Deputy Attorney General. Nonetheless, such actions should not have been necessary for the OIG to obtain access to information that it was lawfully authorized to obtain. However, beginning in mid-2015, the DEA demonstrated a marked improvement in its cooperation with the OIG and provided prompt and complete responses to the OIG's information requests.

Additionally, some information necessary for our review was obtained from the FBI. The FBI responded fairly promptly to most of our requests for information. However, the FBI delayed producing a small amount of grand jury materials on the grounds that the OIG was not legally entitled to these materials without approval from the Attorney General or the Deputy Attorney General. The Inspector General disagreed in testimony before Congress and otherwise, noting that the FBI's legal arguments on this issue were inconsistent with the plain language of the Inspector General Act and long standing practice of the Department and the FBI prior to 2010.<sup>12</sup>

---

<sup>12</sup> In response to this issue, as part of the Department's appropriations in fiscal years (FY) 2015 and 2016, Congress prohibited the Department from denying the Inspector General timely access to records available to the Department and instructed the Inspector General to notify Congress if such denial occurred. See Department of Justice Appropriations Act, 2015, Pub. L. No. 113-235, § 218, 128 Stat. 2130, 2200 (2014); Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, Division B, Title V § 540, 129 Stat. 2242, 2332 (2015). In July 2015 and April 2016, the Office of Legal Counsel (OLC) issued two opinions, the first finding that Section 218 in the Department's FY 2015 appropriations bill did not contain a "clear and unambiguous statement" from Congress to override specific limitations on disclosure, such as those for grand jury materials, and the second finding that Section 540 in the Department's FY 2016 appropriations bill did contain such a "clear and unambiguous statement," and thus the Department was prohibited for the duration of FY 2016 from denying the OIG's timely access to such materials. See *The Department of Justice Inspector General's Access to Information Protected by the Federal Wiretap Act, Rule 6(e) of the Federal Rules of Criminal Procedure, and Section 626 of the Fair Credit Reporting Act*, 39 Op. O.L.C. \_\_\_\_ (July 20, 2015); <https://www.justice.gov/sites/default/files/olc/opinions/attachments/2015/07/23/2015-07-20-doj-oig-access.pdf> (accessed December 28, 2017); *Authority of the Department of Justice to Disclose Statutorily Protected Materials to Its Inspector General in Light of Section 540 of the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2016*, 40 Op. O.L.C. \_\_\_\_ (April 27, 2016); <https://www.justice.gov/sites/default/files/olc/opinions/attachments/2016/04/28/2016-04-27-disclosure-to-ig.pdf> (accessed December 28, 2017). The Inspector General consistently maintained, before and after the OLC opinions, that the OIG was entitled to these materials by virtue of the plain language in Section 6(a) of the Inspector General Act, 5 U.S.C. app. 3 § 6.

Ultimately, the access issues faced by the OIG in this and other matters contributed to the basis for Congress's enactment of the Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, 130 Stat. 1595 (2016), to avoid unnecessary and prolonged delays in completing OIG reviews, as encountered in this matter.<sup>13</sup>

---

<sup>13</sup> Section 6(a)(1) of the Inspector General Act, 5 U.S.C. app. 3 § 6(a)(1), as amended by Section 5 of the Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, 130 Stat. 1595, 1603-04, provides that the Inspector General of the Department of Justice is authorized to have timely access to all records, documents, or other materials available to the Department, notwithstanding any other provision of law, except a congressional provision of law that expressly refers to the Inspector General and expressly limits the Inspector General's right of access.

## **CHAPTER TWO**

### **RELEVANT STATUTES, REGULATIONS, RULES, AND POLICIES**

In this chapter we describe the applicable statutes, regulations, rules, and policies that govern DEA's use of administrative subpoenas to obtain or exploit the data in the programs under review in this report.

#### **I. Statutory and Constitutional Provisions**

##### **A. 21 U.S.C. § 876 (Administrative Subpoenas)**

By federal statutes, Congress has long granted federal agencies the power to issue subpoenas to compel the production of records (and to compel testimony) relevant to agency investigations.<sup>14</sup> Subpoenas issued by federal agencies within the Executive Branch are commonly referred to as administrative subpoenas because the federal agency itself can expeditiously issue the subpoena without approval by a prosecutor, grand jury, or court. Congress has delegated this power to federal agencies to enable them to fulfill their statutory mandates, which may include investigating potential violations of federal law.<sup>15</sup>

In the Controlled Substances Act, codified at 21 U.S.C. § 801 *et seq.*, Congress delegated to the Attorney General the power to issue subpoenas in connection with investigations into drug crimes (referred throughout this report as "Title 21" investigative authority).<sup>16</sup> Section 876(a) provides, in relevant part, that:

---

<sup>14</sup> See, e.g., 24 Stat. 379, 383, Sec. 12 (1887) (providing the Interstate Commerce Commission the power to issue subpoenas to compel the production of records relating to any matter under investigation).

<sup>15</sup> Indeed, when the Department of Treasury was responsible for enforcement of narcotics laws, prior to the creation of the DEA, Congress recognized the need to provide the Treasury Department with subpoena power, in 1955, to assist in the enforcement of federal narcotics laws. See H.R. Rep. No. 84-1347 (1955); S. Rep. No. 84-1247 (1955); see also 101 Cong. Rec. 10085 (1955) (remarks of Rep. Cooper noting that lack of subpoena authority "handicaps enforcement officers" in enforcement of narcotics laws); *id.*, (remarks of Rep. Jenkins summarizing that the House bill would authorize the Secretary of the Treasury to subpoena the production of any records which the Secretary found "necessary or relevant to an investigation in connection with the enforcement of laws pertaining to narcotic drugs and marijuana").

<sup>16</sup> The DEA's primary enforcement mission is to enforce Titles II and III of the Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, 84 Stat. 1236, 1242, 1285, which are cited as the Controlled Substances Act and the Controlled Substances Import and Export Act, respectively. The Controlled Substances Act is codified at Title 21, Chapter 13, Subchapter 1, Sections 801-904; 21 U.S.C. §§ 801-904; and the Controlled Substances Import and Export Act is codified at Title 21, Chapter 13, Subchapter 2, Sections 951-971; 21 U.S.C. §§ 951-971. For purposes of this report, references to the DEA's "Title 21" investigative authority refers only the Controlled Substances Act, 21 U.S.C. §§ 801-904.

Two years prior to enactment of the Controlled Substances Act, which placed drug enforcement laws under a single statute, many drug enforcement responsibilities were transferred



In any investigation relating to his functions under this subchapter with respect to controlled substances, listed chemicals, tableting machines, or encapsulating machines, the Attorney General may subpoena [sic] witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, and other tangible things which constitute or contain evidence) which the Attorney General finds relevant or material to the investigation.

21 U.S.C. § 876(a).

**B. 18 U.S.C. § 2703 (Electronic Communications Privacy Act)**

Title II of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2711, as amended, addresses law enforcement access to stored communications.<sup>17</sup> ECPA generally prohibits communications service providers from “knowingly divulg[ing] a record or other information pertaining to a subscriber to or customer of” a communications service to any governmental entity.<sup>18</sup> However, ECPA contains exceptions to this general prohibition, which include when a federal governmental entity issues an administrative subpoena.<sup>19</sup> For example, Section 2703(c)(2) of ECPA requires communications service providers to disclose in response to an administrative subpoena not the content of communications, but the:

- (A) name;
- (B) address;

---

from the Department of Treasury and the former Department of Health, Education, and Welfare to a new agency, the Bureau of Narcotics and Dangerous Drugs, within the Department of Justice. See Reorganization Plan No. 1 of 1968, 33 Fed. Reg. 5611 (1968).

In 1973, the Drug Enforcement Administration was established within the Department of Justice and the Bureau of Narcotics and Dangerous Drugs was abolished. See Reorganization Plan No. 2 of 1973, 38 Fed. Reg. 15932 (1973). Section 1 of this reorganization plan transferred from the Treasury Department to the Attorney General “all intelligence, investigative, and law enforcement functions” relating to illicit drug activities, except those at ports of entry or borders. Reorganization Plan No. 2 of 1973, 38 Fed. Reg. 15932 (1973). For example, the Treasury Department has administrative subpoena power under Section 967 of the Controlled Substances Import and Export Act, 21 U.S.C. § 967, with respect to investigations to enforce 18 U.S.C. § 545 relating to smuggling of unregistered controlled substances into the United States. As referenced below, the Attorney General subsequently assigned to the DEA Administrator all functions vested in the Attorney General by Section 1 of Reorganization Plan No. 2 of 1973, and not otherwise specifically assigned. 28 C.F.R. Part 0, Subpart R § 0.100(c).

<sup>17</sup> Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (sometimes referred to as the Stored Communications Act, in contrast to prospective surveillance of content and non-content information of electronic communications under Title I and Title III of the Electronic Communications Privacy Act, which contains the general federal wiretap statute, 18 U.S.C. § 2511 *et seq.*, and the pen register statute, 18 U.S.C. § 3121 *et seq.*, respectively).

<sup>18</sup> 18 U.S.C. § 2702(a)(3).

<sup>19</sup> 18 U.S.C. § 2702(c); 18 U.S.C. § 2703(c)(2).

- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- (F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service. 18 U.S.C. § 2703(c)(2).<sup>20</sup>

### **C. Fourth Amendment and the Third-Party Doctrine**

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”<sup>21</sup> “Searches” are not limited to “physical intrusions” because the Fourth Amendment “protects people, not places.”<sup>22</sup> Thus, a “search” can occur without any physical intrusion if a court finds that a “reasonable expectation of privacy” exists.<sup>23</sup>

However, the Supreme Court typically held “that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” and thus the Fourth Amendment does not apply in such circumstances.<sup>24</sup> This remains so even if a person provides information to third parties “on the assumption that it will be used only for a limited purpose and the

---

<sup>20</sup> Other provisions of ECPA enable law enforcement agencies to obtain stored *content* or other records beyond the transactional telephone records in Section 2703(c)(2), by administrative subpoena or other means, if more stringent conditions are met. Under Section 2703(a) and (b) of ECPA, law enforcement agencies can require the disclosure of the contents of wire or electronic communications with a search warrant. See 18 U.S.C. § 2703(a) and (b). A law enforcement agency can also require the provider of “electronic communications services” to disclose the contents of wire or electronic communications that have been in electronic storage for more than 180 days by administrative subpoena, if the law enforcement agency provides prior notice to the subscriber or customer. See 18 U.S.C. § 2703(a) and (b)(1)(B)(i). Further, law enforcement agencies may require the disclosure of other records or information of a subscriber or customer, not listed in Section 2703(c)(2) with a court order under Section 2703(d), where the government provides “specific and articulable facts showing that there are reasonable grounds to believe” that the records or other information sought are “relevant and material to an ongoing criminal investigation.” See 18 U.S.C. § 2703(d).

<sup>21</sup> U.S. Const. amend. IV.

<sup>22</sup> *Katz v. United States*, 389 U.S. 347, 351-53 (1967).

<sup>23</sup> *Smith v. Maryland*, 442 U.S. 735, 739-746 (1979) (explaining application of *Katz* “reasonable expectation of privacy” test).

<sup>24</sup> *Smith*, 442 U.S. at 743-44 (holding that a telephone user had no reasonable expectation of privacy in the telephone numbers he dialed and conveyed to telephone company, which were recorded by government surveillance through a pen register device).

confidence placed in the third party will not be betrayed.”<sup>25</sup> Subsequent court decisions have referred to this doctrine as the “third-party doctrine.”<sup>26</sup>

Notwithstanding the foregoing, the Supreme Court recently ruled that the third-party doctrine does not extend to the government’s collection of historical cell-site location information from wireless carriers.<sup>27</sup> The Supreme Court noted that historical cell-site location information provides a “detailed and comprehensive record” of a person’s past movements from his cell phone’s connections to the wireless network.<sup>28</sup> The Supreme Court found that given this “unique nature of cell phone location records, the fact that this information is held by the wireless carrier “does not by itself overcome the user’s claim to Fourth Amendment protection.”<sup>29</sup> The Supreme Court observed that there “was a world of difference” between the limited types of personal information addressed in older cases where the Court found that the third-party doctrine applied (business records of a bank and telephone numbers dialed) and the “exhaustive chronicle of location information casually collected by wireless carriers today.”<sup>30</sup> Moreover, the Supreme Court noted that the underlying rationale of the third-party doctrine—voluntary exposure—did not apply to cell-site location information because the cell phone itself sends a signal as to its location by virtue of operation without any affirmative act by the user.<sup>31</sup> Accordingly, the Supreme Court held that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information],” and thus government acquisition of this information from wireless carriers constitutes a “search” for Fourth Amendment purposes.<sup>32</sup> However, the Supreme Court noted that its decision was a “narrow one” that did not address other matters not before it, including other types of cell-site location information or other business records that might incidentally reveal location information.<sup>33</sup>

---

<sup>25</sup> *United States v. Miller*, 425 U.S. 435, 440-43 (1976) (holding that individual had no reasonable expectation of privacy in his bank records, which were subpoenaed by the government, because he voluntarily conveyed the information to the bank, which was exposed to employees in the ordinary course of business, and the materials were the records of the banks).

<sup>26</sup> See, e.g., *Carpenter v. United States*, 585 U.S. \_\_\_, \_\_\_ (2018) (slip op. at 9-10).

<sup>27</sup> *Id.* at 10-11, 15, 17, 22.

<sup>28</sup> *Id.* at 10-11.

<sup>29</sup> *Id.* at 11.

<sup>30</sup> *Id.* at 13-17.

<sup>31</sup> *Id.* at 17, 22.

<sup>32</sup> *Id.* at 11, 15-17, 22.

<sup>33</sup> *Id.* at 17-18.



## **II. 28 C.F.R. § 0.104, App., Sec. 4 (DEA and FBI Personnel Authorized to Issue Subpoenas)**

By regulation, the Attorney General has delegated authority to issue Title 21 administrative subpoenas to the DEA Administrator.<sup>34</sup> The DEA Administrator has redelegated this power, as codified by regulation, to most managers or supervisors in a field office and to certain managers and personnel in the Inspections Division at DEA headquarters.<sup>35</sup> These authorized personnel at field offices include: Special Agents-in-Charge, Associate Special Agents-in-Charge, Assistant Special Agents-in-Charge, Resident Agents-in-Charge, and Special Agent Group Supervisors.<sup>36</sup>

The DEA Administrator has also redelegated the authority to issue administrative subpoenas to the Deputy Assistant Administrator of the Office of Special Intelligence within the Intelligence Division (formerly known as the Deputy Chief of Intelligence). This redelegation has existed since 1997, although it was effectuated by memorandum and is not codified by regulation.

## **III. DEA Agents Manual**

The DEA Agents Manual (Manual) contains approved operational policies and procedures to guide the conduct of DEA Special Agents and other personnel in drug law enforcement operations and activities. The Manual contains several sections on the appropriate use of DEA's administrative subpoena authority, including an overview of legal requirements and policies or procedures governing the acquisition and use of certain records or information. We discuss below the sections relevant to our review.

### **A. Business Records Generally**

[REDACTED] of the Manual provide guidance on obtaining business records generally by administrative subpoenas. [REDACTED]

[REDACTED] It also identifies the DEA personnel at headquarters or field offices who are authorized to issue administrative subpoenas, which matches the collective personnel codified in the Code of Federal Regulations listed above.<sup>37</sup>

[REDACTED]

---

<sup>34</sup> 28 C.F.R. Part 0, Subpart R § 0.100. The Attorney General has delegated concurrent authority in connection with investigations of illicit drug activities to the FBI Director, who has redelegated the authority to certain other FBI employees. See 28 C.F.R. Part 0, Subpart P § 0.85; App. to Subpart R, Sec. 1 and 4.

<sup>35</sup> See 28 C.F.R. Part 0, § 0.104; App. to Subpart R, Sec. 4.

<sup>36</sup> See *id.*

<sup>37</sup> See *id.*

[REDACTED]

[REDACTED]

Most DEA administrative subpoenas do not seek bulk data. They are issued on a one-time basis to a person or organization seeking specific information relevant to a particular investigation. (For purposes of this report, such subpoenas will be referred to as "conventional administrative subpoenas.") The DEA's conventional administrative subpoenas from the NSG are generated

[REDACTED]

[REDACTED]

---

<sup>38</sup> The NSG came online in November 2008. Prior to then hard-copy templates were used and OCC's Domestic Criminal Law Section or Division Counsel addressed any case-specific questions.

## **B. Subscriber/Toll Records**



## **C. Documentation Requirements**

As noted above, the Attorney General's authority to issue Title 21 administrative subpoenas has been delegated to certain supervisors in DEA field offices, among others. DEA witnesses told us that in general, the process for line agents to obtain approvals from authorized supervisors for administrative subpoenas is informal, involving direct communications between agent and supervisor about the need for such a subpoena in a particular investigation. Although the Manual contains some provisions regarding the appropriate use of administrative subpoenas, as detailed above, there is no requirement that DEA personnel provide an internal written justification accompanying the subpoena request that demonstrates compliance with those policies. In particular, there is no requirement to document in writing the relevance or materiality of the requested information to the investigation for which it is requested. As one DEA manager explained, the DEA generally does not go through a written justification process that might address questions, such as "why do you need this, what are you looking for. . . , what do you expect to get out of it?" Rather, he said "[i]t's pretty much. . . on the trust system," and that if it were used inappropriately it would be tantamount to falsifying an official record.



## CHAPTER THREE

### THE [REDACTED] PROGRAM

[REDACTED] It was developed in the early 1990s to help combat drug trafficking in the United States by internationally-controlled organizations. [REDACTED]

The DEA and the Department of Justice (Department or DOJ) have promoted [REDACTED] for many years as a "critical tool" for identifying and targeting the command and control communications of transnational drug trafficking entities, whose organizations are responsible for the significant percentage of illicit drugs in the United States.

#### I. The [REDACTED] Collection

<sup>39</sup> There is no standard Department (or Executive Branch) definition of "law enforcement sensitive." See 81 Fed. Reg. 63336 (Sept. 14, 2016) (promulgating the Controlled Unclassified Information Program, 32 C.F.R. Part 3200, establishing "an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls" due to the prior "ad hoc, agency-specific approach" of more than 100 different markings for such information across the Executive Branch). The DEA uses the term "law enforcement sensitive" for programs with other law enforcement agencies and considers the term to be similar to its definition of "DEA Sensitive" information. Under Section 3.5 of the DEA's security classification guide, "DEA Sensitive" information is information that, while not meeting the criteria for classified materials, requires controls and restrictions from public access. The types of information that DEA requires protection under this designation includes: information and materials that are investigative in nature and that are critical to the operation and mission of DEA. Protection of information with this designation is governed by exemptions in the Freedom of Information Act, 5 U.S.C. § 552 *et seq.*, such as 5 U.S.C. § 552(b)(7)(E) (exempting public disclosure of information that "would disclose techniques and procedures for law enforcement investigations or prosecutions . . . if such disclosure could reasonably be expected to risk circumvention of the law").

[REDACTED]<sup>40</sup> These call records, also known as "telephone metadata," included the originating telephone number, the receiving telephone number, the date, time, and duration of the call, and the type of payment, but did not include the content of any calls or subscriber information.<sup>41</sup> [REDACTED]

[REDACTED]

[REDACTED] SOD is a headquarters component within the DEA's Operations Division, which is led by the DEA's Chief of Operations, who in turn serves as the principal advisor to the DEA Administrator and Deputy Administrator on all operational matters and programs. SOD was established to manage and process investigative and intelligence products from the [REDACTED] program and other programs containing classified components. Details regarding how NS and SOD offices operated [REDACTED] during the [REDACTED] era are provided in the subsections below.

#### **A. The [REDACTED] Subpoenas**

As detailed below, the [REDACTED] collection was active from 1993 to 2013. The administrative subpoenas for [REDACTED] data were not directed at a particular identifiable DEA investigation or target. [REDACTED]

---

<sup>40</sup> As noted below, the [REDACTED] database was routinely purged of metadata relating to calls more than 2 years old.

<sup>41</sup> The participating carriers provided additional metadata in the form of proprietary codes that the carriers collected for their own business purposes. This data was not meaningful or useful to the DEA, but the companies did not spend extra time or money to weed out the data that the DEA did not want or use.

The [REDACTED] subpoenas required the production of metadata for all calls made from the United States over the recipient company's network to countries that the DEA determined had a "nexus to drugs." Although the explicit criteria used to find a "drug nexus" varied over time, DEA records reflected an emphasis on countries that had a connection to sources of illegal drugs or precursor chemicals, drug trafficking, or drug-related money laundering. By 2012, DEA had expanded the scope of "drug nexus" to include countries in which drug-related proceeds were being used to support terrorist activities.

The DEA reviewed and approved the country list for the [REDACTED] program annually to ensure that these countries continued to have a "drug nexus," as demonstrated by the prior year's law enforcement activities and other sources on drug trafficking trends. NS completed written justification memoranda for proposed countries to retain in, add to, or delete from the [REDACTED] bulk collection, which required written concurrence by senior managers. By 2013, the DEA had developed 10 specific criteria, derived from prior law enforcement activities and sources on drug-related trends, that it used to justify maintaining, adding, or deleting countries from the [REDACTED] bulk collection. DEA documents and testimony indicate that the written justification memoranda and the resulting lists were reviewed and approved at varying intervals ranging from quarterly to every 1 or 2 years by senior DEA managers. Over the years, officials in the DOJ Criminal Division, including but not limited to the Deputy Assistant Attorney General, reviewed and approved the country list at irregular intervals.

[REDACTED] Although most [REDACTED] subpoenas sought metadata for calls made from the United States to countries on the "drug nexus" list, we learned that for some companies the DEA prepared a separate [REDACTED] administrative subpoena to obtain bulk telephone metadata for all calls *between* any of the designated foreign countries that transited a telecommunications service provider's network.

---

<sup>42</sup> As referenced in Chapter Two, the DEA Administrator redelegated the authority to issue administrative subpoenas to the NS Deputy Assistant Administrator in 1997. The DEA could not locate materials that identified the delegated DEA official who issued [REDACTED] subpoenas between 1993 and 1997.



[REDACTED]

[REDACTED]

In each [REDACTED] subpoena, the Department and the DEA affirmed to the company-recipient that the bulk metadata was being sought "in connection with ongoing criminal investigative activities" of the DEA and "other U.S. federal drug law enforcement authorities as authorized by law," and the responsive metadata provided by the recipient "shall be used for that purpose only." Like the DEA's conventional administrative subpoenas, the [REDACTED] subpoenas were issued on a [REDACTED], which contained a footer stating that the subpoena is issued under the authority of 21 U.S.C. § 876. The boilerplate [REDACTED] does not contain statutory language or standards, such as "relevant or material." Conventional DEA administrative subpoenas typically state, "pursuant to an investigation of violations of 21 U.S.C. Section 801 et seq.," or similar phrasing, "please provide" specified items for a referenced investigation and target, whereas the [REDACTED] subpoenas simply stated that the recipient was required to "produce" the requested data and then "affirmed" that the data was sought "in connection with ongoing criminal investigative activities." This difference in language can be attributed to the fact that the [REDACTED] subpoenas were not issued directly for a specific case.

#### **B. The [REDACTED] Analytical Products**

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

**C. Use of [REDACTED] Products in Drug Investigations**

The DEA has consistently stated that the [REDACTED] program played a critical role in identifying the U.S. network for major international drug trafficking organizations and their respective "command and control" structures. [REDACTED]

[REDACTED]

[REDACTED]

Although the paper did not quantify the value of the [REDACTED] data within [REDACTED], this paper and other DEA documents stated that federal investigators would be unable to identify, in most cases, the U.S.-based operators of these international drug trafficking entities without the [REDACTED] component of [REDACTED].

After the [REDACTED] program was suspended as discussed below, the DEA sent documents to ODAG in 2013 advocating reinstatement of the program. It stated that without the [REDACTED] data, the DEA's ability to comprehensively "assess the true breadth and scope" of transnational drug trafficking entities would be severely limited, particularly identification of their U.S.-based cells. The DEA provided to ODAG several examples from prior [REDACTED] products to highlight that the same target numbers queried without the added value of the [REDACTED] data revealed substantially fewer links to other federal drug cases or connections between U.S.-based cells and their foreign sources and leadership network.<sup>45</sup>

The FBI has also stated that access to [REDACTED] data enhanced the "breadth and quality" of the FBI's investigations by prompt identification of unknown links within major drug organizations and interconnectivity with other federal drug investigations. In a February 2014 letter to ODAG advocating reinstatement of the [REDACTED] program, the FBI cited several investigations of major drug organizations where queries of known "command and control" target phone numbers in the [REDACTED] database, particularly the [REDACTED] data, resulted in the identification of other domestic connections to the organizations and many links to DEA or other federal agency investigations. The FBI stated that access to the [REDACTED] data aided federal drug enforcement agencies in their efforts to dismantle the most significant and violent drug trafficking organizations by identifying their leadership networks, which it believed otherwise would have been "substantially more" difficult.

#### **D. Use of [REDACTED] Data in Non-Drug Investigations**

[REDACTED]

[REDACTED]

---

<sup>45</sup> As discussed below, the DEA withdrew the request to reinstate the [REDACTED] collection in August 2014 in favor of the [REDACTED] program.



[REDACTED]

[REDACTED]

Patterson said that the standard applied for requests in non-drug investigations was essentially the same, but without the connection to a narcotics case.

[REDACTED]

Patterson said that this standard contained no particular limits beyond demonstrating that the request pertained to an active criminal investigation of the particular requesting agency. He said the level of specificity to justify the request in non-drug investigations would be the same as that required for DEA's requests in Title 21 cases.

Patterson told us that he did not believe there were many instances of such usage even though it had been done periodically in certain cases.

[REDACTED]

Patterson also based his belief on the fact that he never heard about any significant delays for products related to increases in requests in non-drug investigations.

[REDACTED]

[REDACTED]

The DEA reinstatement documents did not address the legal basis for using the [REDACTED] collection in this manner. The sample Speedway product excerpts that the DEA sent to ODAG in support of reinstating the program showed additional instances in which [REDACTED] data was apparently used in support of non-drug investigations. [REDACTED]

[REDACTED]

[REDACTED]

The FBI stated that access to [REDACTED] was legally permissible in these circumstances under the longstanding legal principle that evidence legally obtained by one law enforcement agency may be shared with another.<sup>46</sup> The FBI's letter did not cite any specific benefits derived from access to the [REDACTED] data in these non-drug nexus circumstances.

One instance of using the [REDACTED] collection in a non-drug investigation came to light in *United States v. Hassanshahi*, 145 F. Supp. 3d 75 (D.D.C. 2015). In *Hassanshahi*, a United States District Court described a use of the [REDACTED] collection on behalf of Homeland Security Investigations, a component of DHS ICE, to develop evidence of a criminal violation of the United States' trade embargo against Iran. DHS ICE was a participating agency in the [REDACTED] program. The DEA submitted a declaration from then-ASAC Patterson in which he set forth the standard, noted above, for requests in non-drug investigations, stating that the [REDACTED] database "could be used to query a telephone number where federal law enforcement officials had a reasonable articulable suspicion that the telephone number at issue was related to an ongoing federal criminal investigation," and stating further that this standard had been met with respect to the search that returned the defendant's telephone number.<sup>47</sup> Quoting *Jabara v. Webster*, 691 F.2d 272, 277 (6th Cir. 1982), the government argued that this use was consistent with the longstanding legal rule that

---

<sup>46</sup> As noted in Chapter Two, the FBI also has delegated authority to issue administrative subpoenas under 21 U.S.C. § 876(a) in FBI drug investigations. However, under Section 18.6.4 of the FBI's Domestic Investigations Operations Guide (DIOG), the FBI cannot issue an administrative subpoena unless it is relevant to an open investigation on a specific target. Accordingly, the DIOG would not permit the FBI to use its administrative subpoena authority for bulk collections like [REDACTED]. This issue is discussed in more detail in the next chapter regarding the National [REDACTED] Initiative.

<sup>47</sup> Although it did not rule on whether Homeland Security Investigations had established "reasonable articulable suspicion" for the database query request, the court reported the following facts regarding the request: Homeland Security Investigations received an unsolicited email from a source concerning an Iranian named "Sheikhi" who contacted the source by email, seeking assistance in procuring certain electrical equipment, and provided an Iranian telephone number and business address in Tehran, Iran, and the [REDACTED] product request was for calls to that telephone number. 145 F. Supp. 3d at 79; 75 F. Supp. 3d 101, 105 (D.D.C. 2014) (citing affidavit from Homeland Security Investigations agent).

"[e]vidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken."<sup>48</sup>

As noted in subsection E.1.b., below, we found other examples that appeared to show similar usage of ██████ products in non-drug investigations during the ██████ era. However, as explained below, the written descriptions of RAS submitted by requesters were often supplemented by more detailed information provided orally or by email to SOD. This additional information might have established a drug connection not made clear in the written submission. According to the DEA, it had the ability in individual cases to determine RAS and the Title 21 nexus of individual requests. However, the DEA told us that it lacked an automated accounting capability to assess the collective use of ██████ in non-drug cases, and could only do so by undertaking a burdensome manual examination of all ██████ records. Thus, we were unable to determine the extent of this practice and whether it was consistent with the DEA's and the FBI's general statements, noted above, that requests for ██████ products in non-drug investigations during the ██████ era was uncommon.<sup>49</sup>

## **E. Programmatic Safeguards**

In 2007, in response to questions from a congressional oversight committee regarding the ██████ program and its ██████ component, the DEA identified the following as "programmatic safeguards to ensure that the legitimate privacy and civil liberty interests of U.S. citizens were properly protected and respected:"

---

<sup>48</sup> 145 F. Supp. 3d 75, 83 (D.D.C. 2015). The government made this argument even though such use may not have been consistent with representations made to the subpoena recipients. As noted above, in each ██████ subpoena, the Department and the DEA affirmed to the company-recipient that the bulk metadata was being sought "in connection with ongoing criminal investigative activities" of the DEA and "other U.S. federal drug law enforcement authorities as authorized by law," and the responsive metadata provided by the recipient "shall be used for that purpose only." The court did not address substantive issues regarding the underlying ██████ subpoena or subsequent use of the responsive data because the court found that the Homeland Security Investigations's discovery of the evidence that supported Hassanshahi's arrest was sufficiently attenuated from the database query that initially identified him. See *United States v. Hassanshahi*, 75 F. Supp. 3d 101 (D.D.C. 2014) (order denying defendant's motion to suppress certain evidence discovered during a forensic examination of laptop computer); *United States v. Hassanshahi*, 145 F. Supp. 3d 75 (D.D.C. 2015) (denying motion for reconsideration to suppress the evidence based on new information regarding the DEA's database because such information did not alter prior ruling regarding the evidence being sufficiently attenuated from the query, and suppression of the evidence was not an available statutory remedy under 21 U.S.C. § 876(a) in any event).

<sup>49</sup> In response to a draft version of this report, the DEA stated that in June 2017 it added features to the automated request process that now enables it to account for the total number of Title 21 and non-Title 21 requests received in connection with ██████ successor program. We did not evaluate these new features as a part of this review, but will assess them later in connection with the DEA's responses to our recommendations.

1. Information that identifies a particular individual, entity or address, such as names, dates of birth, Social Security account numbers, was not sought, accepted or maintained as part of [REDACTED]. Rather, the DEA only sought and maintained the specific items of call metadata, described above, that were collected via [REDACTED] subpoenas (the originating telephone number, the receiving telephone number, call date and time information, call duration information, and type of payment).
2. [REDACTED]
3. A very limited number of personnel [in NS] who were specifically trained for participation in [REDACTED] were granted access to the [REDACTED] collection.
4. All requests for [REDACTED] products and the responses thereto were routed through SOD "to ensure that the requests originate[d] from a legitimate requestor and [were] supported by 'reasonable and articulable suspicion.'"
5. Only upon receipt of a valid request received through proper program channels were NS personnel permitted to query the [REDACTED] database and use the results as part of a [REDACTED] product.
6. The DEA maintained a detailed audit trail of all requests, queries and responses received, conducted and prepared by the [REDACTED] program.

[REDACTED]

[REDACTED]

---

<sup>50</sup> In fact, as detailed above in subsection D, the requirement of linkage to a "drug trafficking investigation" for [REDACTED] product requests was not always observed.



As detailed below, the [REDACTED] program was suspended in 2013, and it was beyond the scope of this review to determine whether the safeguards described above were consistently and strictly enforced during the period that the [REDACTED] program was in operation. From our interviews and the documents the DEA provided to us, we found no evidence that the DEA's general description of these safeguards was incorrect (apart from the indication that all target numbers in product requests were linked to drug trafficking investigations); many of these safeguards remain in place today with respect to the current version of the [REDACTED] program involving [REDACTED], as discussed below. However, we identified two safeguards during the [REDACTED] era to be of particular interest because of DEA's claim that they provided a safeguard against the misuse of the data that could implicate privacy or civil liberties of telephone service subscribers: the requirement that each request for a [REDACTED] product be vetted by SOD to ensure they were supported by RAS and the existence of an "audit trail" for all requests.

### **1. Reasonable Articulable Suspicion (RAS)**

According to DEA testimony and records, during the period that [REDACTED] was in operation, [REDACTED]

[REDACTED] As noted in the prior section, the DEA described the SOD's review of this information as an important safeguard to prevent misuse of the [REDACTED] collection and ensure the protection of the "legitimate privacy and civil liberty interests of U.S. citizens." Therefore, we discuss below the training and standards to show RAS, and examine sample SOD-approved products.

#### **a. Training and Standards**

A demonstration of RAS was required for obtaining [REDACTED] products containing [REDACTED] data, and is also required today in connection with [REDACTED] (as discussed below). Although this concept is not addressed in the DEA Agents Manual, according to the DEA, it is addressed during Basic Agent Training and other classes.<sup>51</sup> According to the DEA, SOD Staff Coordinators informed investigators in general training sessions or coordination meetings that any requests to SOD had to involve an active case or investigation and contain a "justification" or "basis" (or essentially RAS) on how their requests related to the respective active case or investigation. [REDACTED]

[REDACTED] Patterson equated

---

<sup>51</sup> In response to a draft version of this report, the DEA commented that the DEA Agents Manual is not the proper venue to discuss legal concepts. However, as discussed in Chapter Two, the Manual discusses several legal guidelines on appropriate use of the DEA's administrative subpoena power [REDACTED], which provides that administrative subpoenas may be used to compel many types of records that are "relevant or material to a drug investigation."

the RAS standard to the same level of support that field investigators had to demonstrate to their field supervisors with signatory authority on a conventional administrative subpoena. Patterson said that investigators understood the process and what information was required after submitting one or two product requests to SOD.

[REDACTED]

For example, Patterson said he would deny a request that only stated "number from pocket trash" without stating whose pocket the number came from and how it connected to the associated case. [REDACTED]

[REDACTED] SOD managers told us that, although the RAS justification (previously referred to as "remarks") auto-populated in the finished products from NS pre- and post-DARTS, the RAS justification contained in the finished products may not necessarily reflect an SOD Staff Coordinator's comprehensive understanding of the factual basis for the request, which was often clarified through informal communications with the requester not reflected in the written request.

#### **b. Sample Products**

The DEA provided the OIG with sample [REDACTED] products created during the [REDACTED] era, which contain the information provided by the requesters in their formal written requests. The DEA described these samples to us as being representative of the results of queries that were accepted [REDACTED]

[REDACTED]

---

<sup>52</sup> DARTS will not permit a requester to enter a case number unless it pertains to an active case number in the DEA's case system.

<sup>53</sup> Patterson told us that prior to 2006, SOD maintained a "very hard line" that no requests would be approved without a Title 21 nexus. However, as discussed above, other participating federal agencies were sometimes permitted to make requests for [REDACTED] products in non-drug investigations after 2006.

[REDACTED]

[REDACTED]

[REDACTED]

## **2. Auditability of Queries**

According to the DEA's records and testimony, each query of the [REDACTED] database, including the [REDACTED] component, left a record trail for potential audit purposes. [REDACTED]

[REDACTED]



## **F. Legal and Legislative Oversight**

In this section we describe the legal and legislative oversight of the ██████ program during the ██████ era by the DEA and the Department. As detailed below, there is no evidence that the DEA or the Department ever fully addressed the question of whether the ██████ bulk collection was permissible under 21 U.S.C. § 876(a).

### **1. Early Years**

According to DEA and FBI memoranda and other contemporaneous records, senior Department officials sanctioned the development of ██████ in the early 1990s. The DEA's historical records reflect that in January 1992 Attorney General William Barr provided approval for the ██████ program, including ██████, after receiving a program briefing, which the Deputy Attorney General also attended. The FBI Director also received a program briefing during that same time period. The DEA did not provide us with any formal document codifying the Department's approval of the program (besides implicit approval in the Memorandum of Understanding (MOU) discussed below). Nor did the DEA provide us with any formal document discussing the legal basis for what were then novel aspects of the program regarding the proposed use of the DEA administrative subpoena authority for collecting bulk data through ██████.

In June 1992, 5 months after the Attorney General's briefing, the DEA Administrator, the FBI Director, the Assistant Attorney General for the Criminal Division, and a senior Department of Defense official executed the ██████ program MOU, which set forth the terms of program's operations, including that the DEA's Deputy Assistant Administrator for NS served as the Program Manager, and the Department (without specifying a particular DOJ component) had legal oversight authority over the program. Contemporaneous documents showed that the Criminal Division filled this oversight role, which included signing the MOU on behalf of the Department.

We determined that over the years since 1992, the DEA, in its role as Program Manager, briefed numerous incoming senior Department officials about the ██████ program over the course of its existence, including most of the Attorneys General and Deputy Attorneys General serving during that period. Although these briefings noted that the ██████ collection was obtained by administrative subpoena, we found no evidence that these briefings included a discussion of any legal issues raised by the DEA's use of its administrative subpoena authority to collect bulk data through the ██████ program.<sup>56</sup> Available

---

<sup>56</sup> In response to a draft version of this report, the DEA commented that various DOJ officials over the years had many questions on this usage. To the extent this occurred, we saw no evidence of it. According to one DEA manager who provided multiple "read on" briefings to senior Department managers over several years, the ██████ portion of the ██████ briefing typically lasted only 3 to 4 minutes, and he did not recall any senior managers raising any questions regarding the ██████ collection. This DEA manager noted that the ██████ briefings were





was disseminated beyond a few people at the DEA and the Criminal Division, let alone formally adopted as the Department's analysis of these issues.

The August 1999 Memorandum did not address key published court decisions available at the time, and at the time ██████ began, which raised potential challenges to the validity of the DEA's use of Section 876(a) to amass the ██████ collection. Most significant of these omissions was the Supreme Court's decision in *United States v. Bisceglia*, 420 U.S. 141 (1975), which upheld the Internal Revenue Service's use of its administrative summons authority to require a bank to produce documents evidencing transactions of a certain type during a 1-month period to aid in identifying the individual who had engaged in the transactions and might be liable for unpaid taxes. However, two concurring and two dissenting justices expressed deep concern about the permissibility of "exploratory" subpoenas lacking a connection to a genuine, extant investigation.<sup>60</sup> In addition, the August 1999 Memorandum failed to discuss *Peters v. United States*, 853 F.2d 692 (9th Cir. 1988), in which the Ninth Circuit rejected a subpoena issued by the Immigration and Naturalization Service to a farm labor camp manager for all records pertaining to residents of the camp, which had been issued in support of a criminal investigation of unknown residents who might have been undocumented aliens. The court held that "we are reluctant to assume the existence of the power to issue third-party subpoenas directed at unidentified targets where Congress has not provided for them specifically, nor provided procedural safeguards."<sup>61</sup> 853 F.2d at 696.

---

authority to collect the ██████ data was "legally defensible" but "founded on uncertain legal ground." The FBI General Counsel's memorandum was shared with the DEA's Chief Counsel, who strongly disagreed with several of the FBI General Counsel's characterizations of the issues raised by the ██████ program, particularly that the program may lack a solid legal foundation, and noted that the Department endorsed the manner in which the subpoenas were used for the ██████ collection. After attempting unsuccessfully to locate any analyses of the legal underpinnings of the ██████ program that might have been prepared by the DOJ Criminal Division or the DEA, the DEA's then-Acting Administrator directed the then-CCI Section Chief to prepare "a memorandum addressing the administrative subpoena issue, on the theory that such a memorandum could act as a counter to any similar but dissenting memorandum that the FBI may produce" to the Department on this issue. We found no evidence that the FBI's proposed program was ever activated or that the DEA ever transferred bulk ██████ data to the FBI for such a program. However, as detailed below, notwithstanding the concerns raised by the FBI General Counsel, the FBI ultimately supported reinstatement of the ██████ program after it was suspended.

<sup>60</sup> The August 1999 Memorandum cited the *Bisceglia* decision only in a footnote for the proposition that "Congress has provided protection from arbitrary or capricious action [from an agency's subpoena powers] by placing federal courts between the Government and the person summoned." 420 U.S. at 151. As noted earlier, the DEA did not intend to enforce the ██████ subpoenas judicially, and thus the "protection" from "arbitrary or capricious action" would not exist in practice.

<sup>61</sup> The August 1999 Memorandum cited in a footnote the then nine reported court decisions regarding the DEA's administrative subpoena authority, which included *United States v. Moffett*, 84 F.3d 1291 (10th Cir. 1996). The August 1999 Memorandum noted parenthetically that the Tenth Circuit in *Moffett* held that the defendant lacked standing to challenge a DEA administrative subpoena issued to Amtrak. However, the August 1999 Memorandum did not include any facts regarding that case or the basis for the ruling. In particular, the Tenth Circuit

### 3. [REDACTED]

The first written evidence that we found in which the Department (or the DEA) specifically considered legal vulnerabilities posed by the use of "exploratory" subpoenas, as done in [REDACTED], occurred in 2005, [REDACTED]

[REDACTED]<sup>62</sup> In 2005, DOJ Criminal Division attorneys in the Narcotic and Dangerous Drug Section (NDDS) and the Asset Forfeiture and Money Laundering Section (AFMLS)<sup>63</sup> prepared legal analyses of [REDACTED] that highlighted the relevance of the *Bisceglia* and *Peters* opinions to the question of whether the DEA's subpoena authority would permit the collection of bulk, non-target-specific data for "exploratory purposes." The NDDS memorandum highlighted in bold text that the *Bisceglia* and *Peters* opinions raised "the question whether any subpoena requesting information on all customers transacting certain business with a third-party corporation would be interpreted as within the government's investigatory authority." Likewise, the AFMLS memorandum stated that "upon consideration of applicable law, and the objectives of [REDACTED], and available alternatives," DEA's proposed use of administrative subpoenas for exploratory purposes "would unnecessarily place one of DEA's most important information gathering tools in serious jeopardy of adverse judicial, and possibly legislative, reaction which could drastically reduce its usefulness . . . ."

Additionally, in July 2005, an AFMLS attorney contacted the then-CCI Section Chief to notify him that the AFMLS Chief intended to meet with the DEA's NS Chief to advise against the use of administrative subpoenas for exploratory purposes as proposed for [REDACTED]. The CCI Section Chief summarized AFMLS's concerns in a high priority email to then-Chief Counsel Wendy Goggin, then-Deputy Chief Counsel Michael Ciminelli, and other managers. In particular, the CCI Section Chief noted AFMLS's concern that any public disclosure of the proposed use of exploratory subpoenas in [REDACTED] "could have a negative if not devastating effect on SOD and 5th floor projects," even if such exploratory usage survived a court challenge. The AFMLS attorney

---

ruled that the defendant lacked standing to challenge the DEA's non-target-specific administrative subpoena, issued to Amtrak, seeking reservation records for a 1-month period, which DEA Special Agents analyzed to identify the defendant, who paid cash for his ticket, and subsequently found him traveling with a large amount of illicit drugs. See *Moffett*, 84 F.3d 1291 (10th Cir. 1996). Accordingly, the Tenth Circuit did "not reach the statutory construction issue defendant presses" on whether the DEA exceeded the scope of its statutory subpoena power in 21 U.S.C. § 876(a) by issuing a non-target-specific subpoena. *Id.* at 1293-94.

<sup>62</sup> [REDACTED]

<sup>63</sup> In November 2017, this Section was renamed the Money Laundering and Asset Recovery Section.

who contacted the CCI Section Chief told us that AFMLS was concerned about “negative effects” on [REDACTED].

The AFMLS attorney told us that he became “a sort of Cassandra” figure to the DEA and warned them that they “ran a serious risk” of Congress subsequently restricting their subpoena authority, as done to the Internal Revenue Service following the Supreme Court’s ruling in *Bisceglia*, if the DEA persisted in their proposed use of exploratory subpoenas in [REDACTED]. Three months later, he expounded on these risks in the AFMLS memorandum, stating:

[REDACTED]

(Emphasis added.) We determined that the memorandum’s reference to “the use of exploratory Section 876 subpoenas” to acquire this data was a reference to the [REDACTED] collection. The AFMLS attorney told us that a negative court ruling on the DEAs’ proposed use of exploratory subpoenas in [REDACTED] risked undercutting the whole [REDACTED] effort and would be “throw[ing]” the baby out with the bath water.”

Through in-person meetings and emails, AFMLS and NDDS warned DEA senior managers in the Intelligence Division and OCC about their concerns, stemming from the *Bisceglia* and *Peters* opinions, regarding the DEA’s proposed use of its subpoena authority to collect bulk, non-target-specific [REDACTED]. Ultimately, the Criminal Division convinced the DEA to obtain the equivalent information through alternative means.

The [REDACTED] controversy demonstrates that the Department and the DEA were aware of the existence of case law casting doubt on the use of administrative subpoenas to collect bulk data for exploratory purposes, including the [REDACTED] collection, at least as of 2005. However, we found no evidence that the [REDACTED] proposal caused anyone in the Department or the DEA to prepare a legal analysis of [REDACTED] addressing these issues, or to revisit the propriety of the continued use of the [REDACTED] administrative subpoenas.

#### **4. Congressional Oversight**

Our review found that a small number of Members of Congress or their staff knew of the ██████████ program prior to 2007.<sup>64</sup> Briefings provided by the DEA touched only superficially on the ██████████ program. Following a Senate Select Committee on Intelligence oversight hearing in 2007, which included the ██████████ program, the DEA's written responses to questions for the record addressed several oversight issues on the ██████████ collection, such as scope of collection, data retention, internal controls (consistent with those described above), and external disputes or judicial review. We found no evidence that the DEA provided to Congress a legal analysis of whether the ██████████ collection was authorized under 21 U.S.C. § 876, or that it was asked to do so during the period ██████████ was in operation.

##### **G. Termination of the ██████████ Collection**

Shortly after the Snowden leaks in June 2013, senior DEA managers from the Intelligence Division, the Operations Division, SOD, and OCC convened to discuss the effect of these leaks on the DEA's bulk data collection activities, including the ██████████ program. In July 2013, the DEA leadership met with Department senior leadership, including then-Attorney General Eric Holder and then-Deputy Attorney General James Cole, to discuss the ██████████ component of ██████████, among other programs. In the following months, the DEA briefed White House staff and Members of Congress and their staff on ██████████ and other DEA programs involving bulk collection. The DEA also continued working closely with ODAG on issues related to bulk collection.

DEA documents establish that, at the direction of the Department, the DEA suspended the ██████████ component of ██████████ on August 5, 2013. We found no documents, however, stating the reasons for this decision or identifying who made it. DEA witnesses involved with the program told us that they understood the decision was made by ODAG, but told us they did not know the reasons. While we believe that the individuals who made this decision are no longer with the Department, based on the timing of the decision (made in the aftermath of the Snowden disclosures), the questions presented by ODAG when the DEA sought reinstatement (discussed below), and the fact that ODAG directed that any replacement program must be target-specific, we believe that reasons for the decision likely included concerns about whether the non-target-specific ██████████ bulk collection was within the authority granted to the DEA under 21 U.S.C. § 876(a) as well as the controversy and privacy concerns generated by the Snowden disclosures about the NSA's bulk telephone metadata collection.

The ██████████ program continued, but Quick Checks and Formal Products were processed without the use of the ██████████ data tank. On September 25,

---

<sup>64</sup> Available records showed that only four Members of Congress received briefings between 1996 and 1997, 3 years *after* the program began, and then none until 10 years later in committee oversight hearings in 2007. From 1993 to 2006, we found that approximately 35 congressional committee staff received briefings.



2013, the DEA submitted a formal written request to the Office of the Attorney General (OAG) and ODAG to reinstate the ██████ program, which included among the several attachments a legal analysis in support of ██████ ("DEA Reinstatement Memorandum").

The DEA Reinstatement Memorandum contained a more detailed legal analysis of the legal authority for the ██████ collection under 21 U.S.C. § 876(a) than was prepared before or during the operation of the ██████ program.<sup>65</sup> However, like the August 1999 Memorandum, the Reinstatement Memorandum did not address the issues raised by the collection of bulk data by means of a subpoena that was unconnected to any specific suspect or investigation, and failed to identify or analyze several relevant court opinions, including *Bisceglia* and *Peters*. In defending the legality of the ██████ collection, the DEA Reinstatement Memorandum asserted that Section 876(a) provides broad subpoena power for "any investigation," without elaboration, related to a Title 21 drug nexus. The DEA Reinstatement Memorandum stated that the bulk ██████ data obtained was consistent with the type of "records" that can be obtained with an administrative subpoena and that the bulk ██████ data met the legal tests for "relevance" or "materiality" under the statute. With respect to "relevance," the DEA Reinstatement Memorandum detailed that courts have employed a broad standard to include any records that directly bear on the subject matter or could reasonably lead to other information that bears on a subject matter. The DEA Reinstatement Memorandum asserted that this broad standard does not have defined volume limits and detailed that courts have permitted production of voluminous data in circumstances where doing so requires identification of the precise information within that mass production that directly bears upon the matter being investigated.

The DEA Reinstatement Memorandum noted that this broad standard of "relevance" did not mean the DEA's subpoena power to obtain bulk records was boundless. Rather, it stated that if "there is no substantial nexus to international drug trafficking activity with a connection to the United States, DEA would not seek (and DOJ would not approve) collecting telephone transactional records in bulk under its administrative subpoena authority."<sup>66</sup>

---

<sup>65</sup> The DEA's Reinstatement Memorandum provided to OAG and ODAG did not reference the August 1999 Memorandum at all, much less as the prior official legal opinion on this matter. Nor did we find any evidence that the August 1999 Memorandum was later supplied to the Office of Legal Counsel for its review as discussed below.

<sup>66</sup> The expression "substantial nexus" apparently refers to the evidence tying a particular country on the list to drug trafficking as, earlier in the Memorandum, it states: "The ██████ program gathers large amounts of data about telephone transactions that take place between telephones in the United States and telephones in countries that have been determined by DOJ and DEA to have a significant nexus to drug trafficking." The DEA's use of the expression "substantial nexus" (and earlier in the document "significant nexus") appears to be a shorthand reference to the criteria used to add or remove countries. However, we saw no use of this expression in any ██████ country reviews or in the documents discussing the ██████ country review process in the DEA's Request for Reinstatement to which the Reinstatement Memorandum was an attachment.

The DEA Reinstatement Memorandum further noted that the [REDACTED] data fell within the scope of permissible transactional data that government entities can obtain by administrative subpoena under Section 2703(c)(2) of ECPA. Additionally, the DEA Reinstatement Memorandum pointed out that the DEA's administrative subpoenas are subject to court oversight any time a subpoena recipient decided not to comply and DEA sought to judicially enforce a subpoena. However, the DEA Reinstatement Memorandum also noted the DEA has opted not to pursue court enforcement against non-cooperating providers to preserve "the security of the program."

In early 2014, ODAG requested assistance from the Department's Office of Legal Counsel (OLC) in considering the structure of the [REDACTED] program in connection with the DEA's proposed reinstatement. On March 20, 2014, after reviewing the DEA's Reinstatement Memorandum, OLC transmitted a list of more than 30 "Follow-up Questions" to the DEA. Among other things, OLC requested the DEA to provide its understanding of the meaning and scope of the terms "relevant or material to [an] investigation" in Section 876(a) and to identify case law shedding light on the meaning of these terms. On July 1, the DEA's OCC provided partial responses to the questions. OCC's partial response did not answer OLC's (or ODAG's) questions about the meaning and scope of "relevant or material" in Section 876(a), stating instead that such questions "require a thorough review of case law" and would take "a couple of months" to complete.

The DEA never completed these responses. [REDACTED]

[REDACTED] The Department then terminated the OLC review. [REDACTED]

## II. [REDACTED]

---

<sup>67</sup> As noted above, we were not able to determine the precise reasons that were given by the Department to the DEA for the suspension of the [REDACTED] program. It appears from the DEA's documents and the testimony of witnesses, however, that DEA officials understood that any new program to fill the void from the [REDACTED] suspension would require ODAG approval and would have to involve target-specific subpoenas for telephone metadata rather than the non-targeted bulk collection approach of [REDACTED]. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED]

<sup>68</sup> At the time, Wallace was serving as a contract consultant to the DEA.

[REDACTED]

[REDACTED]

A. [REDACTED]

[REDACTED]

B. [REDACTED]

[REDACTED]

---

<sup>69</sup> [REDACTED] DEA documents sometimes use the term "reasonable articulated suspicion" (emphasis added). As discussed below, we believe the correct term is "articulable" as expressed by the Supreme Court.

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>70</sup> As noted earlier, SOD organizationally is classified by the DEA as a component of the Operations Division in DEA headquarters. ASACs serving at components of DEA headquarters are not currently listed as officials to whom the DEA has redelegated the authority to issue subpoenas (as opposed to ASACs at field offices) under the DEA's implementing regulations or the Agents Manual. See 28 C.F.R. Part 0, § 0.104; App. to Subpart R, Sec. 4; DEA Agents Manual Section 6614.21. According to the DEA, SOD and the Special Projects Section in particular "frequently perform DEA field operational missions and responsibilities" that "are consistent with subpoena issuance authority" in DEA's regulations and Agents Manual. Nevertheless, the DEA has not formally delegated the authority to such positions in DEA headquarters, and we recommend below that it do so if it intends that these officials execute such responsibilities. See Chapter Six, Recommendation 15.



[REDACTED]

[REDACTED]

D. [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>71</sup> SOD operations include coordinating multi-national investigations against the major drug trafficking organizations responsible for the flow of illicit drugs into the United States [REDACTED]

[REDACTED]

E. [REDACTED]

[REDACTED]

During the [REDACTED] era, compliance with the Section 876(a) requirement that records sought by the subpoena be relevant or material to Title 21 narcotics cases was plausibly accomplished at the subpoena issuance stage by limiting the collection to “drug nexus” countries. The DEA’s theory was that, once collected, this data could be shared for other matters pursuant to *Jabara v. Webster*, 691 F.2d 272, 277 (6th Cir. 1982). [REDACTED]

[REDACTED]

F. [REDACTED]

[REDACTED]

---

72 [REDACTED]

[REDACTED]

[REDACTED]

\_\_\_\_\_

## 1. Relevance and Reasonable Articulated Suspicion (RAS)

As noted above, Section 876(a) requires that any information sought by an administrative subpoena be “relevant or material” to a Title 21 investigation. There are two important dimensions of this requirement: first, that there be an adequate evidentiary connection between the information requested and the criminal activity being investigated, and second, that the investigation be of the correct type, *i.e.*, an authorized Title 21 (narcotics) investigation.

\_\_\_\_\_

[REDACTED] the standard applicable when law enforcement agents stop and question an individual or make a traffic stop. In *Terry v. Ohio*, 392 U.S. 1, 19-23 (1968), the Supreme Court held that a police officer's investigative stop of an individual for purposes of criminal prevention and detection is permissible under the Fourth Amendment if supported by "reasonable suspicion." The Supreme Court stated that a "police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that [particular] intrusion" upon constitutionally protected interests of the private citizen. *Id.* at 20-21. The Supreme Court expounded later that "reasonable suspicion" is simply "a particularized and objective basis for suspecting the person stopped of criminal activity." *Ornelas v. United States*, 517 U.S. 690, 696 (1996) (quoting *United States v. Cortez*, 449 U.S. 411, 417-18 (1981)).

[REDACTED]

**a. DARTS/DICE Procedure**

[REDACTED]

[REDACTED]

[REDACTED]

76

[REDACTED]

Below the free-text "remarks" box, the requester is instructed to "select justification" by choosing a selection from a drop-down menu of the following choices:

---

75

[REDACTED]

76 According to the DEA, in June 2017,

[REDACTED]

77

[REDACTED]

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]
7. [REDACTED]
8. [REDACTED]
9. [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>78</sup> By contrast, during the [REDACTED] era and prior to the adoption of the drop-down menu, requesters were required to demonstrate RAS in a free text box.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]  
79

[REDACTED]

b.

[REDACTED]

[REDACTED]

---

79

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

80

[REDACTED]

81

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**G. Legal Oversight**

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

## CHAPTER FOUR

The second program, after [REDACTED], in which the DEA used administrative subpoenas to amass and exploit bulk data was the [REDACTED]. [REDACTED] involved the use of administrative subpoenas to collect bulk purchase data for [REDACTED] sold by selected vendors.<sup>82</sup> [REDACTED] was initiated in 2008 as a result of a DEA Chicago Field Division operation in which an administrative subpoena was served on a local store for the records of all [REDACTED] purchases during a 3-month period. The subpoena was issued after the Field Division discovered in a different case that members of a major drug trafficking organization had purchased [REDACTED] of the same [REDACTED] there. The information provided in response to the subpoena led to two arrests and significant seizures of drugs and related proceeds.

In response to this success, DEA headquarters established a national program, known as [REDACTED], modeled on the Chicago regional operation.

[REDACTED]<sup>83</sup> [REDACTED] thus fit within a longstanding DEA strategic objective of attacking the financial infrastructure of drug trafficking organizations. As detailed below, the DEA stopped issuing [REDACTED] subpoenas in 2013, shortly after the [REDACTED] program was terminated.

### I. The [REDACTED] Collection

The purpose of the [REDACTED] bulk data collection was to develop potential targets associated with drug trafficking by cross-referencing the purchaser data through various law enforcement databases, such as the DEA's Narcotics and Dangerous Drugs Information System (NADDIS), an internal database for reporting drug enforcement activity. The Office of Financial Operations (FO), a component of DEA headquarters, formally announced [REDACTED] as a headquarters program under general file [REDACTED] in [REDACTED]<sup>84</sup>

FO informed the field divisions that FO would obtain the bulk purchaser data from companies by administrative subpoena, develop investigative intelligence

---

<sup>82</sup> [REDACTED]

<sup>83</sup> [REDACTED]

<sup>84</sup> FO's mission includes providing headquarters expertise in and oversight of the DEA's financial investigations of drug trafficking, particularly drug-money laundering activities, and leading national program initiatives targeting these illicit acts. FO's Chief reports to the DEA Operations Division Chief, who serves as the principal advisor to the DEA Administrator and Deputy Administrator on all operational matters and programs.

packages with other DEA offices, and disseminate these packages to the field for follow-up investigation. Jennings told the OIG that the Chicago Field Division's enforcement results "really opened our eyes to what we already thought was happening" and provided the DEA with a successful example of how to use [REDACTED] as another method to target the major drug trafficking organizations.

During most of the time that [REDACTED] was in operation, the DEA used administrative subpoenas to collect information about each [REDACTED] [REDACTED] from the recipient vendors during a designated period, and disseminated the raw information to the field offices where the purchasers were located. The field offices then were responsible for establishing connections to illicit drug activity, typically by running the data through NADDIS or other law enforcement databases. [REDACTED]

[REDACTED] The DEA collected the bulk [REDACTED] data on a continuous basis (bi-weekly, quarterly, or bi-annually) until the program was suspended indefinitely in August 2013 for reasons we discuss below.

#### **A. The [REDACTED] Subpoenas**

The administrative subpoenas for the [REDACTED] were not directed at or related to a particular identifiable investigation or target. Instead, the [REDACTED] subpoenas were issued periodically to [REDACTED] under a "general file" number as described below and required production of the following customer information for each [REDACTED]: (1) last name, (2) first name, (3) customer's company (if applicable), (4) billing address, (5) shipping address, (6) telephone number(s), and (7) date of purchase. The first [REDACTED] Staff Coordinator told us that he identified the five largest [REDACTED] based on "open-source" research and secured each company's advance consent to provide the requested bulk data, without any payment, in response to a subpoena.<sup>85</sup> He said that none of the companies raised any issues or concerns regarding the volume of information requested or the frequency of the DEA's requests. We saw no evidence that any company objected to the subpoenas.

From the [REDACTED] program's inception in 2008 to August 2013, the [REDACTED] subpoenas were generated and signed by the Assistant Special Agent-in-Charge (or a Group Supervisor) at the Washington, D.C., Field Division (Washington Field Division). As discussed in Chapter Two, the DEA has not delegated the authority to issue administrative subpoenas to positions in FO, an office in DEA headquarters. After the Assistant Special Agent-in-Charge (or a Group Supervisor) signed the subpoenas, a DEA Special Agent in the Washington Field

---

<sup>85</sup> FO Staff Coordinators are DEA Special Agents who serve as the staff lead on FO's programs and provide operational support to the DEA field offices, among other duties. There were three [REDACTED] Staff Coordinators in FO over the life of the program.

Division sent the originals and copies to the [REDACTED] Staff Coordinator to issue to the companies.

The first subpoena for [REDACTED] was issued shortly after the [REDACTED] cable of June 3, 2008. Consistent with the [REDACTED] cable, the subpoena stated that it was issued “[i]n the matter of the investigation of Case No: [REDACTED].” The ending code [REDACTED] referred to the headquarters general file code that was created for [REDACTED] and was unrelated to a specific drug trafficking investigation or target. Jennings told the OIG that [REDACTED] was the first time that he used administrative subpoenas to request information under a general file that was not particularized to a specific target. Similarly, Kevin J. Powers, the DEA Division Counsel in the Chicago Field Division, told the OIG that Chicago’s regional operation and its national counterpart, [REDACTED], represented “the first occasion that I ever had . . . where we were operating under a general file and sort of using the admin subpoena as a form of target development.” Powers said that “in all other instances” that he could recall the DEA already had an open investigative or general file on a particular target when it issued an administrative subpoena. Other DEA managers and Special Agents gave similar accounts.

The standard [REDACTED] subpoenas stated that the [REDACTED] purchase data was being sought “[p]ursuant to an official criminal investigation being conducted by the Drug Enforcement Administration of a suspected felony.” As discussed below, the DEA’s Office of Chief Counsel (OCC) reviewed and approved a sample [REDACTED] subpoena with this language in mid-September 2008. Witnesses told us that the DEA’s view was that there was an open criminal investigation under the general file—general investigation of [REDACTED] used to facilitate illicit drug/money laundering offenses.

However, DEA witnesses acknowledged that at the time any [REDACTED] subpoena was served, there was no open “criminal investigation” on an identifiable subject or specific “suspected felony” to which the subpoena related. We were unable to determine who developed this language or mandated its use, but as discussed in more detail below, it already was present in a sample [REDACTED] subpoena when OCC approved it and the DEA required its inclusion in [REDACTED] subpoenas in September 2008. When asked about the meaning of the phrase “pursuant to an official criminal investigation,” the first [REDACTED] Staff Coordinator stated “that’s a legal question” that was “beyond [his] scope,” though he believed that the [REDACTED] subpoenas either used standard language or language approved by OCC.<sup>86</sup>

---

<sup>86</sup> However, other witnesses, including Powers (the DEA Chicago Division Counsel) and the DEA’s head of the Domestic Criminal Law Section, a component of OCC which has responsibility for addressing internal questions on administrative subpoenas, told us they had not seen the [REDACTED] subpoena language on other subpoenas. As noted in Chapter Two, conventional administrative subpoenas reference a specific case number and target by name, phone number or some other identifier, even if they contain the phrase “pursuant to an investigation” or similar language.

Former FO Acting Chief Jennings told us that the “official criminal investigation” language referred to the general file because the DEA can open a general file on activity and seek to develop information related to suspected criminal activity. He said that the “suspected felony” would be money laundering or drug trafficking, and thus, [REDACTED] is “the investigation into the use of [REDACTED] for money laundering or drug trafficking activities.”

Powers told us that the “official criminal investigation” at the time the subpoena is issued refers to the general file in the heading “In the Matter of Investigation [REDACTED].” He noted that it is “absolutely not the [DEA’s] traditional use of the administrative subpoena” but the “general file covers it.” Like Jennings, Powers said that the [REDACTED] general file was for “developing targets” of drug traffickers and money launderers who use [REDACTED]. Maura Quinn, then-DEA Deputy Chief Counsel for International and Intelligence law, gave similar testimony and noted that, except for [REDACTED] and [REDACTED], the DEA’s administrative subpoena authority is “typically used narrowly” without collecting large amounts of information and is “typically connected to a specific case.”

## **B. Receipt of Data and Dissemination of Leads to Field**

As detailed below, the DEA primarily sent all of the raw data received from the vendors regarding thousands of purchases of [REDACTED] directly to the field offices, notwithstanding [REDACTED] cable that investigative packages would be developed by FO and then disseminated to the field for follow-up investigation. In practice, the DEA left it to the field offices to determine how to use the raw information. After field offices reported that this information was too voluminous to use efficiently, or simply disregarded it, in 2013 DEA began comparing the raw purchaser information with other criminal databases to identify “hits” and develop intelligence products for dissemination to the field for further investigation. This substantially reduced the number of leads sent to the field while increasing their potential value.

### **1. Dissemination of Raw Data (2008–2013)**

The first [REDACTED] Staff Coordinator told the OIG that he received the bulk [REDACTED] data responsive to the DEA’s administrative subpoenas. He provided the incoming bulk [REDACTED] data to an FO Program Analyst for formatting without any review of it. He told us that he had assumed the companies would not produce non-responsive data because the DEA only requested “limited things.” However, the Program Analyst explained to us that she reviewed the incoming data and removed items that were not [REDACTED], such as [REDACTED], before uploading the bulk data to DEA databases.

Initially, FO was responsible for disseminating the bulk [REDACTED] data to the field divisions where the purchases had occurred for follow-up action. FO sent these “raw lists” of data to the Special Agents-in-Charge by cover memoranda from [REDACTED] (the “[REDACTED] cover memoranda”), which stated that FO would

subsequently send a target list for follow-up action after running database checks on the data. As detailed below, however, we found little evidence that such target lists were regularly prepared by FO.

The Program Analyst told us that the "raw lists" received from the vendors contained too much information for her to continually format. The first [REDACTED] Staff Coordinator told us that the field divisions did not have the time to review it all, and further explained that Jennings asked the DEA's Office of Special Intelligence (NS) technical support staff to create a computer program that could manage the [REDACTED] data and automatically disseminate it to the field divisions. As a result, sometime between late 2008 and early 2009, NS technical support staff created the [REDACTED] module in the [REDACTED], which automatically disseminated the bulk data as leads, after FO uploaded it, to the relevant DEA field division contact, typically the Field Intelligence Manager. The [REDACTED] module also provided a means for the field divisions to electronically report results from the leads. Access to the bulk [REDACTED] data in the [REDACTED] module was limited to FO personnel who uploaded data, the [REDACTED] Staff Coordinator, and NS technical support staff.

We received conflicting information regarding the extent to which FO or other DEA offices actually generated target lists for dissemination to the field by comparing the raw [REDACTED] data with NADDIS or other law enforcement databases during the early years of the program, as promised in the [REDACTED] cover memoranda. The first [REDACTED] Staff Coordinator told us [REDACTED]

[REDACTED] He told us that this process existed until he left FO in 2010.

The first [REDACTED] Staff Coordinator's account on this subject was not consistent with the other information that the DEA provided to the OIG. Nor did he have a recollection of the [REDACTED] module generally, which was developed during his tenure as Staff Coordinator. While the [REDACTED] module in [REDACTED] may have had the capability to send NADDIS "hits" to the DEA field divisions, as we found was implied in some DEA records, we did not find any evidence that this actually occurred.

To the contrary, the DEA's responses to the OIG's information requests unequivocally stated that raw data was disseminated to the field divisions to conduct checks in NADDIS and other law enforcement databases before and after the creation of the [REDACTED] module. DEA records provided to the OIG included only one memorandum disseminating a target list of NADDIS hits sent to a field division along the lines set forth in Jennings cable during the period before the initiation of the [REDACTED] module. In contrast, the DEA provided us with several hundred pages of "raw lists" sent to field divisions through the Jennings cover memoranda prior to the [REDACTED] module. Further, the Program Analyst and the second [REDACTED] Staff Coordinator both told us that only raw data was disseminated to the field divisions from the [REDACTED] module in [REDACTED].



The first [REDACTED] Staff Coordinator stated that after FO sent [REDACTED] leads to the field his role was mainly to obtain division reports of any successes—arrests, drug seizures, or any other asset seizures obtained from the [REDACTED] information. He told us that field divisions sent emails or significant activity reports to him in which they reported the number of arrests, amount of drugs seized, amount of drug-related cash seized, and other property seizures.<sup>87</sup> FO compiled the statistical results reported to them in a spreadsheet using the following metrics: (1) number of arrests, (2) value of cash seized, (3) number/value of vehicles seized, (4) value of dollar of real property seized, (5) number of firearms seized, (6) amount of crack seized, (7) amount of cocaine seized, (8) amount of ecstasy seized, (9) amount of methamphetamine seized, (10) amount of marijuana seized, and (11) amount of heroin seized. FO's spreadsheet showed results on fiscal year (FY) and cumulative basis from FY 2008 through FY 2014.<sup>88</sup> The first [REDACTED] Staff Coordinator told us that Jennings frequently contacted field division management to find out why some offices did not send any responses on results to FO. However, the first [REDACTED] Staff Coordinator stated that FO took "a hands-off approach to these things, g[ave] information to the field, and it [was] up to the field to either do or not do."

In October 2010, the first [REDACTED] Staff Coordinator left FO and a new one replaced him. The second [REDACTED] Staff Coordinator told us that he did not receive any written protocols or checklists for the program from his predecessor or elsewhere. The second [REDACTED] Staff Coordinator said that he learned about the mechanics of [REDACTED] through discussions with the first Staff Coordinator before his departure.

The second Staff Coordinator told us that, after he started, the automated process of disseminating all raw purchaser data, by zip code, through [REDACTED] to the relevant field divisions continued for several years. He said that, prior to August 2013, FO did not perform any review of the raw data for matches in NADDIS or other law enforcement databases before it was automatically disseminated to the field. Rather, he said that FO expected the field divisions to do that work and determine "if there's something there."<sup>89</sup> The second [REDACTED] Staff Coordinator told us that he was not aware of any official directive for the field divisions to report results. He said that he endeavored to check for results

---

<sup>87</sup> As noted above, the first [REDACTED] Staff Coordinator had no recollection of an [REDACTED] Module in [REDACTED], and thus did not recall obtaining any results that might have been reported in the [REDACTED] Module from field divisions.

<sup>88</sup> However, the DEA informed the OIG that FY 2010 through FY 2013 contained the combined totals of *both* [REDACTED] and the non-subpoena operational component of the [REDACTED], which could not be separately reported.

<sup>89</sup> However, the second [REDACTED] Staff Coordinator noted that he initiated some review of the raw data earlier in his tenure. Specifically, by the end of 2010 or early 2011, he began reviewing the voluminous raw data more closely after he noticed that it contained purchase data for federal credit unions, churches, and colleges. He said that from that point on he tried to sift through every upload and remove obvious "dead-end leads" from the raw data before it was disseminated to the field divisions.

in the [REDACTED] module at least on a quarterly basis, but that he found the process cumbersome and that it was not easy to access the results.

[REDACTED]

Some field offices raised concerns with the quality of the leads from [REDACTED] data given the large volume. For example, a DEA manager in one field division wrote in an email to FO that "the field has limited resources to conduct the proper investigative follow-up on the voluminous [REDACTED] leads received from FO each month. The [REDACTED] leads should be about quality, not quantity." Likewise, the second [REDACTED] Staff Coordinator acknowledged in an email to a DEA colleague in July 2012 that: "[T]here are so many [leads] we put out, we don't know what's being done, and why some are better than others."

Other field offices expressed related concerns regarding the poor quality of the leads. For instance, Brian McKnight was a Group Supervisor in the Miami Field Division from approximately 2006 to 2011, and later served as an FO Section Chief and then Acting Chief of FO between August 2012 and January 2014. He told us that [REDACTED] leads were not "a high priority" if the purchasers were not active targets. Specifically, he stated:

[A]gents are very busy [and] unless it directly relates to an [active] case. . .there wasn't a lot of well, let's just go knock on his door because the person bought a [REDACTED]. That's, you know, you have to have some reasonable suspicion that a person was involved in illicit activity [before doing that]. [But] it all kind of was put in the [REDACTED] system. . . .

McKnight told us that, after he became Acting Chief of FO, he tried to improve [REDACTED] by establishing protocols for sending out quality leads, as described in the next subsection, versus simply sending a name to the field because someone bought a [REDACTED].

McKnight also stated that the information could be many months old before his field office received it. McKnight told us that FO was insufficiently staffed to process the large volume of bulk data when he first arrived as an FO Section Chief in August 2012. Powers, the DEA Division Counsel in Chicago where the [REDACTED] concept began, stated that his agents thought [REDACTED] "was a resounding failure at the headquarters level," in part, because of delays in purchase information reaching the field. Powers said that the Chicago Field

Division started issuing its own subpoenas shortly after [REDACTED] began because "headquarters was so slow" and the "national [program] wasn't working."<sup>90</sup>

## **2. Expanded Headquarters Efforts to Enhance the Value of [REDACTED] Data (2013-2014)**

Beginning in May 2013, DEA headquarters made efforts to enhance the value of the data it was receiving pursuant to [REDACTED] subpoenas by creating intelligence products for the field rather than disseminating raw data.

### **a. Organized Crime Drug Enforcement Task Forces Fusion Center (May to August 2013)**

From May 2013 through August 2013, FO arranged for the Organized Crime Drug Enforcement Task Forces (OCDETF) Fusion Center to query the incoming bulk [REDACTED] data for possible matches to information in the Fusion Center's database, which contains over 500 million records of investigative data from member agencies.

The Fusion Center is a multi-agency operational intelligence center that was established under the OCDETF program in 2004 to support member agencies in their cases against the most significant drug trafficking and money laundering organizations by providing "fused" intelligence products.<sup>91</sup> More than 15 federal agencies are Fusion Center members each of whom provide their respective criminal case reporting data, pursuant to Memoranda of Understanding, for incorporation into the Fusion Center database. These federal member agencies include the: DEA; FBI; Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Prisons; the U.S. Marshals Service; Department of Homeland Security Immigration and Customs Enforcement (DHS ICE); Department of the Treasury Financial Crimes Enforcement Network; and the U.S. Secret Service. According to the Chief Counsel for the Fusion Center, most fused intelligence products are generated for use in open investigations as requested by member agencies. [REDACTED]

[REDACTED] During the period these checks were done with regard to [REDACTED], FO stopped sending [REDACTED] data indiscriminately to the field divisions where the purchases took place.

---

<sup>90</sup> Powers told the OIG that he was unaware that his field division had been issuing administrative subpoenas locally for records of [REDACTED] purchases due to significant delays until shortly before his interview with us. He also discovered, shortly before his interview with us, that the Chicago Field Division continued to issue these subpoenas even after the Washington Field Division stopped issuing them for FO, as detailed below.

<sup>91</sup> See U.S. Department of Justice Office of the Inspector General, *Review of the Organized Crime Drug Enforcement Task Forces Fusion Center*, I-2014-002, March 2014 at 1-2 (discussing background, mission, and organization of Fusion Center).

McKnight told us that both he (as an FO Section Chief) and his then-FO Chief thought that running checks of the [REDACTED] in the Fusion Center database would produce the highest quality leads with limited resources because the [REDACTED]

[REDACTED] The DEA told the OIG that the Fusion Center subsequently generated 62 intelligence products for DEA and other member agencies based on its querying of the [REDACTED] purchase data in the Fusion Center database from May through August 2013.

The Fusion Center intelligence products provided a narrative summary regarding the "match" between the [REDACTED] and information in the Fusion Center database, and provided [REDACTED]

We found at least five instances where the Fusion Center created intelligence products for non-DEA member agencies based on "matches" of [REDACTED] with investigative material in the Fusion Center database that had no apparent drug nexus. Specifically, the Fusion Center created four intelligence products for DHS ICE on "matches" of [REDACTED] in the Fusion Center database with DHS ICE investigations on [REDACTED]

[REDACTED] Thus, the [REDACTED]-subpoenaed data apparently was used without limitation to create intelligence products for member agencies in non-drug investigations whenever the [REDACTED]-subpoenaed [REDACTED]

[REDACTED] The Fusion Center Chief Counsel stated that the Fusion Center accepts member-agency supplied data and does not independently assess an agency's acquisition of data, which DEA officials represented orally was lawfully obtained by subpoena. We found no evidence that any guidance or training was provided to Fusion Center personnel limiting the use of [REDACTED] data to drug cases.

The Fusion Center's brief utilization of [REDACTED] data ended in August 2013, just 2 ½ months after it began, in large part due to the FBI's concerns about the legality of the program, which are detailed in Section II below on legal review of [REDACTED].

**b. Internal Review by FO (August 2013 to April 2014)**

Sometime between August and October 2013, after the Fusion Center stopped utilizing [REDACTED] data, the DEA began performing its own analysis of the [REDACTED] data before disseminating leads. FO queried the [REDACTED] in NADDIS and other law enforcement databases, [REDACTED]

[REDACTED] FO sent these investigative leads directly to the field divisions by email. McKnight told us that he instituted these practices because "you need to send the best product available" to field agents who "have enough to do" and not simply send the names of [REDACTED] without any connection to illicit activity. McKnight said he instructed his staff to send leads where [REDACTED] were identified in NADDIS, particularly as a target, or in other databases reflecting a criminal drug history.

[REDACTED]

A former DEA manager of a financial investigative group, who had a lead role developing investigative leads as an FO contractor, explained this protocol. He stated to us that agents "don't have time" to review random names unless the lead is meaningful, p [REDACTED]. Accordingly, he sought to send leads that "hit" a target in an active case or preferably had a "hit" in more than one law enforcement database. The second [REDACTED] Staff Coordinator and the third [REDACTED] Staff Coordinator (who began in August 2013) told us that they agreed with this approach. They also told us that they requested the field divisions provide responses on any results, positive or negative, on these leads and followed-up at least on a quarterly basis.

According to the DEA's records and testimony, FO sent the first lead by email in October 2013. As detailed below in subsection I.D., the DEA stopped serving [REDACTED] subpoenas in September 2013. However, FO finished reviewing the last [REDACTED] subpoena returns in April 2014. FO's statistical spreadsheet for [REDACTED] showed that the results for this 7-month period in FY 2014, containing FY results from [REDACTED] subpoenas only, exceeded or roughly equaled the results of several metrics for all of FY 2013, containing FY results from both [REDACTED] subpoenas and the other operational non-subpoena component. Specifically, FO reported that the refined leads that FO disseminated during this limited period

resulted in more arrests (10 versus 6), vehicles seized (5 versus 0), firearms seized (4 versus 2), and 80 per cent of the value of cash seized (\$1.2 million versus \$1.5 million). However, FY 2013 results were greater for seizures of cocaine (137 kilograms versus 2.2 kilograms) and marijuana (12 pounds versus 3.1 pounds). (No other drug seizures were attributed to ██████ leads during this period.)

### **C. Maintaining the Confidentiality of the ██████ Program**

DEA sought to prevent the ██████ program from becoming publicly known because they were concerned that criminals would take steps to conceal their ██████ if they knew that data regarding such ██████ was being collected. The ██████ cover memorandum that was used beginning in 2008 to disseminate the ██████ data to the field instructed DEA personnel "not to disclose the source of names" identified via ██████ subpoenas when documenting their investigations. The memorandum also stated that "[p]robable cause must be developed independently." The first ██████ Staff Coordinator told us that the first instruction was intended to protect the program's sources and methods; criminals would obtain money counters by other means if they knew that the DEA collected this data. He said that DEA personnel were therefore told not to write on a DEA Form 6 that the DEA received the names in response to ██████ subpoena.<sup>92</sup> DEA documents showed that DEA personnel were instructed to state in reports, such as a DEA Form 6, that they "received a lead from a source of information that indicated that the ██████ may be involved in drug trafficking and money laundering." The first ██████ Staff Coordinator told us that the directive on using independent sources to corroborate the tips from the ██████ ██████ ensured that the DEA pursued genuine illicit drug activities.

This instruction was maintained as the ██████ evolved. The cover email and cover page to the Fusion Center products contained standard caveats that the product was sent for lead purposes only, should be segregated from official files, and should not be used in court proceedings. The cover email and summary page to the FO-generated products did as well. FO therefore included as a standard practice caveats that the field should develop their own probable cause for the ██████ leads and not incorporate the ██████ leads data or source into official files.

As discussed above, the DEA typically searched for a ██████ ██████ potential connections to illicit drug activities through NADDIS and other law enforcement database checks. DEA documents and testimony showed that the DEA sought to determine whether those potential indicators of illicit drug activity could then be corroborated through traditional investigative techniques, such as plain-view surveillance, to warrant initiating a conventional

---

<sup>92</sup> A "DEA Form 6," as described in the Manual, is "a general purpose form used to report investigative activities and intelligence information to investigative files." ██████ of the Manual.

particularized investigation. In this manner, the DEA could use the same independent evidence that served as the basis to open specific cases as evidence in court without disclosing [REDACTED], which functioned essentially as an anonymous tip and not as evidentiary foundation for the case.<sup>93</sup> DEA documents also showed examples where DEA divisions had already targeted the [REDACTED] for investigation prior to receiving the [REDACTED] lead. In these circumstances, the [REDACTED] data could provide additional evidence regarding the nature and scope of illicit activities in addition to that which already existed. DEA witnesses told us that the requirement to develop “independent probable cause” ensured that the DEA did not randomly investigate innocent parties because [REDACTED] is not a criminal act.

#### **D. Storage and Retention**

The [REDACTED] bulk data (including documents incorporating such data) was stored in three primary areas: [REDACTED]

[REDACTED] elsewhere in the DEA, or the Fusion Center. In this section, we discuss how DEA addressed the question of retention of the [REDACTED] bulk data stored in these locations.

##### **1. Bulk Data on Original CDs**

The first and second [REDACTED] Staff Coordinators both told us they were unaware of any retention policies that the DEA developed for the [REDACTED] bulk data during their respective tenures. The first [REDACTED] Staff Coordinator told us that the DEA did not have any policies on retention of the [REDACTED]. He said that “we didn’t know what to do with them . . . they’re not evidence . . .” He told us that he kept [REDACTED] in a locked cabinet and informed the second [REDACTED] Staff Coordinator of [REDACTED] location until FO could figure out what to do with [REDACTED]. He stated that “we weren’t interested in establishing any kind of database of, you know, anything other than having this [data] to send leads to the field to investigate.” The second [REDACTED] Staff Coordinator stated that the [REDACTED]

After the OIG initiated this review, the DEA told us that no [REDACTED] subpoenaed information received by DEA had been purged or destroyed since the program began in 2008. In addition, the DEA stated that it was working to develop a retention and destruction schedule for such materials. One DEA

---

<sup>93</sup> However, FO notified field investigators that they would have to reveal the original source of information from [REDACTED] subpoenas if the question ever arose in actual testimony. We found no evidence that the DEA ever revealed [REDACTED] in live testimony or elsewhere. However, Powers told the OIG that in approximately three to four cases a judge required the government to disclose *in camera* how a defendant originally was targeted through [REDACTED] subpoenas without requiring disclosure to defense counsel.



attorney working on this issue told us that FO had not contemplated a retention schedule for the [REDACTED] bulk data until the OIG raised this issue.

In June 2015, the DEA received approval from the National Archives and Records Administration for a retention and destruction schedule, submitted in March 2015, relating to "non-actionable information obtained pursuant to service of a DEA Administrative Subpoena." Although the retention and destruction schedule description appears to apply to [REDACTED] data held in *all* locations without distinction, the DEA's testimony and information responses showed that the DEA intended for this schedule to pertain [REDACTED]. Under this disposition schedule, DEA received approval to destroy the original CDs within 3 years after date of receipt.

## **2. Bulk Data in [REDACTED] Module**

The second [REDACTED] Staff Coordinator stated that he had no knowledge of what the retention policy would be for the [REDACTED].

[REDACTED] Then-DEA Deputy Chief Counsel Quinn told the OIG that she did not know if the DEA had the resources or technical ability to identify the specific [REDACTED] data in [REDACTED] that has investigative value.

## **3. Bulk Data Stored Elsewhere**

The DEA stated in response to an OIG information request that headquarters program general files [REDACTED], are destroyed or deleted 25 years after the cutoff date (which is 6 years after the last activity or correspondence). Therefore, under current policy and practice, all non-case specific [REDACTED] data stored by FO or elsewhere at the DEA (other than in [REDACTED]), *i.e.*, purchaser data that was never connected to a specific investigation, will be retained for at least 25 more years (though Quinn did not think it would be accessed, in part due to the speed with which drug trafficking organizations change and the historical nature of the data).

# **II. Legal Review of [REDACTED]**

In this section we describe three occasions in which questions were raised regarding whether the [REDACTED] program was a permissible use of DEA's administrative subpoena authority under 21 U.S.C. § 876(a).

## **A. Initial Review in September 2008**

In early July 2008, 1 month after [REDACTED] began, Powers sent an email inquiry requesting a legal review of the [REDACTED] subpoenas to two OCC managers, Michael Ciminelli and Donna Sanger, who oversaw the Domestic Criminal Law

Section (referred to as CCM).<sup>94</sup> Powers's request arose after he briefed two Assistant U.S. Attorneys (AUSAs) in the Northern District of Illinois on [REDACTED]. Powers told us that he informed the AUSAs that the DEA's use of a general file to issue administrative subpoenas to develop targets was "out of the ordinary," but he was comfortable with the subpoena use based on Chicago's success before FO launched [REDACTED]. Powers's email request to Ciminelli and Sanger stated that the AUSAs inquired whether anyone at OCC "had consulted with FO on the scope of the administrative subpoenas to be sure that they were in compliance with 21 U.S.C. § 876."

Powers's email stated that "in my opinion" the DEA was "well within the statutory authority" because the program's concept stemmed [REDACTED]. Powers's email added that the Chicago Field Division decided to send the question from the AUSAs to Ciminelli and Sanger "to be on the safe side, given the recent scrutiny regarding admin[istrative] subpoenas." Powers told us that the "recent scrutiny" referred to an internal review of the DEA's use of administrative subpoenas in the wake of the OIG's report of the FBI's misuse of National Security Letters in 2007.<sup>95</sup> Ciminelli replied by email the next day that "we do not believe that CCM has ever reviewed the subpoena," and would obtain "a copy from FO to review it now."

Two months later, however, OCC had not responded to Powers's email inquiry. In early September 2008, Sanger notified Ciminelli that she assigned a senior attorney in CCM (Senior Attorney 1) to review the "subpoena question." Sanger also remarked that she saw "nothing wrong with it on the surface, but [hasn't] seen the actual subpoena."

---

<sup>94</sup> CCM is the unit within OCC responsible for addressing administrative subpoena issues.

<sup>95</sup> See U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, March 2007. Following this OIG report, OCC conducted an internal review in May 2007 of its documented legal advice and guidance regarding administrative subpoenas for the prior 5 years, including a review of training and materials in the DEA Agents Manual relating to administrative subpoenas. OCC's summary report concluded that its substantive legal advice regarding administrative subpoenas had been correct. However, OCC found that the DEA Agents Manual omitted some important procedural guidelines, such as restrictions imposed by other federal statutes on the use of administrative subpoenas, and actions to be taken if the DEA received unauthorized information in response to an administrative subpoena. OCC also found that its training academy failed to have OCC attorneys provide the training on legal rules for administrative subpoenas to new agents and new group supervisors who would have authority to sign subpoenas. OCC's internal report documented the measures taken or to be taken to address the deficiencies that were found. OCC's report noted, without discussion, that "specialized legal support for certain DEA intelligence programs utilizing administrative subpoenas," a description that possibly included [REDACTED], was supervised by the Deputy Chief Counsel for International and Intelligence Law. Significantly, the OCC report did not address the issue of whether Section 876(a) authorized DEA to collect bulk data by administrative subpoena for target development purposes as done in [REDACTED], or for subsequent exploitation in specific cases as done in [REDACTED].

On September 9, 2008, Sanger sent Powers's July 2008 email inquiry to Senior Attorney 1. Senior Attorney 1 responded 2 days later to Sanger, copying Ciminelli and Powers, stating that she had "no legal objections" after reviewing a sample subpoena. Senior Attorney 1's response, which attached a sample [REDACTED] subpoena, also noted that the subpoenas requested raw data from companies that was disseminated to the field divisions as leads to develop their own probable cause.<sup>96</sup> Senior Attorney 1 separately forwarded her legal conclusion to Jennings and a former FO Section Chief, who notified the first [REDACTED] Staff Coordinator by forwarding the email to him.

Senior Attorney 1 told us that she did not have an independent recollection of this issue.<sup>97</sup> However, she remarked that on current reflection the subpoena language appeared fine because it seemed to her that the DEA had a specific target or was investigating a specific crime. She added that if she had understood at the time that the DEA was merely issuing "blanket" subpoenas on [REDACTED] purchases between certain dates without connection to an open case then she likely would have advised against it (despite her email reflecting that she knew the raw data was being disseminated to the field as leads to develop their own probable cause).

After Senior Attorney 1 replied "no objection," Sanger emailed Powers that "my view is probably the same as yours. Unless a federal court tells us we can't do this, I think we can continue this project."

None of the 2008 emails regarding the legal underpinnings of [REDACTED] made reference to the fact that a very similar question had been raised 3 years earlier, in connection with a proposal to use administrative subpoenas to [REDACTED]. As detailed in Chapter Three, in 2005, the DOJ Criminal Division Narcotic and Dangerous Drug Section (NDDS) and Asset Forfeiture and Money Laundering Section (AFMLS) both prepared legal analyses of [REDACTED] that highlighted the relevance of *United States v. Bisceglia*, 420 U.S. 141 (1975), and *Peters v. United States*, 853 F.2d 692 (9th Cir. 1988), to the question of whether the DEA's administrative subpoena authority in 21 U.S.C § 876(a) permitted the collection of bulk, non-target-specific data for "exploratory purposes." The AFMLS memorandum opined that the DEA's proposed use of its administrative subpoena authority for exploratory purposes to gather bulk wire remitter records

---

<sup>96</sup> Senior Attorney 1's "no objection" response stated that she had conferred with a more senior CCM line attorney. Powers pointed out to us that the DEA headquarters delays on [REDACTED] even extended to his legal questions—noting that it took 2 months before headquarters responded with a "one-liner, yes."

<sup>97</sup> However, Senior Attorney 1 said she did recall advising FO to be careful on the scope of collection because [REDACTED], whereas in more recent Department projects she recalled much discussion on how to avoid "retain[ing] information on innocent people."

in [REDACTED] "entail[ed] significant risk of adverse consequences" from both courts and Congress to such use.

The absence of any reference to this analysis was particularly noteworthy given that Ciminelli and others in OCC had been alerted to the Criminal Division's concerns about [REDACTED]. In July 2005, the then-OCC Section Chief of International Law (CCI Section Chief) sent a high priority email to then-Chief Counsel Wendy Goggin, then-Deputy Chief Counsel Michael Ciminelli, and other managers to notify them that the AFMLS Chief intended to meet with the DEA's Office of Special Intelligence Chief to advise against the use of administrative subpoenas for exploratory purposes, like [REDACTED]. Among other concerns, the CCI Section Chief noted that AFMLS was concerned that Congress might substantially restrict the DEA's administrative subpoena authority, as it had done with the Internal Revenue Service after the *Bisceglia* opinion, even if such exploratory usage survived a court challenge. In any event, we found no evidence that Ciminelli or anyone else in OCC recognized that [REDACTED] raised the same issues about the scope of Section 876(a) that arose in the [REDACTED] proposed operation.

#### **B. FBI Concerns at the Fusion Center in May 2013**

As noted above, beginning in May 2013, DEA sent [REDACTED] data to the OCDETF Fusion Center for analysis. On May 15, 2013, then-FO Section Chief McKnight reported to OCC that FBI agents had raised questions to DEA management at the Fusion Center about "the legality" of the [REDACTED] subpoenas and utilization of the Fusion Center to query the [REDACTED] data, which FO recently had started to send there. McKnight requested guidance from OCC, noting that his then-FO Chief had received a telephone inquiry on this issue from Fusion Center Chief Counsel. One week later, a DEA attorney in CCM provided McKnight the September 2008 response to Powers's inquiry, discussed above.

The FBI agents we interviewed described their concerns at the time. First, they were concerned about the broad scope of the "blanket" [REDACTED] subpoenas to obtain information simply because somebody purchased a [REDACTED]. They told us that in their collective experience at the FBI they could not issue an administrative subpoena without it being based on a specific target or case. Some of them also noted that the FBI's policy governing use of administrative subpoenas did not permit "blanket" usage.<sup>98</sup> As one FBI agent explained the concern about the "blanket" [REDACTED] subpoenas:

---

<sup>98</sup> Under Section 18.6.4 of the FBI's Domestic Investigations Operations Guide (DIOG), the FBI cannot issue an administrative subpoena under 21 U.S.C. § 876(a) unless it is relevant to a predicated drug investigation. Also, under Section 6.9 of the DIOG, the FBI has authority to issue administrative subpoenas in Preliminary Investigations. Section 6.1 of the DIOG provides that a Preliminary Investigation "may be opened on the basis of any 'allegation or information' indicative of possible criminal activity or threats to national security." Section 6.5 of the DIOG describes the predication required in this circumstance as particularized to a specific criminal activity or national security threat and the involvement or role of specific individuals, groups, organizations, or entities in such activity.

[I]t wasn't predicated on individual cases or individual suspicions. Rather, it [was] just a general fishing expedition [because one had] a good sense that some people that [REDACTED] may also be using [them] for illicit purposes. . . . [But] you can't just take any [kind of] innocent activity that Americans engage in and go grab all their records knowing that a small percentage of it is potentially connected to illegal activity. And that sounded exactly like what DEA was looking to do.

Second, the FBI agents were concerned about the Fusion Center personnel running all [REDACTED] through the Fusion Center database to mine for potential connections to an actual investigation. They explained that running all of these names, which had been collected without foundation, through a massive government database and producing comprehensive intelligence products on any "hits," which included detailed information on family members and pictures, "didn't sit right with any of [them]."

The FBI agents' concerns were raised to the Fusion Center Deputy Director, an FBI employee (FBI Deputy), who told us that he shared the same concerns. The FBI Deputy told us that underlying part of the FBI's concerns was that DEA and Fusion Center management tried "to push [REDACTED] very quickly," but it "needed to be really vetted and looked at by [FBI headquarters management] seven ways to Sunday" to ensure that it was consistent with the FBI's policies and protocols. The FBI Deputy told us that he notified the Fusion Center Director that the FBI was not going to participate in [REDACTED] until he received approval from FBI headquarters because "it just didn't seem right" in his experience. The Fusion Center Chief Counsel stated that the FBI's dataset is a significant part of the Fusion Center database, but it was not included in the queries of the [REDACTED] data due to the FBI's objection to [REDACTED].

The FBI Deputy related to us that a meeting was held with then-FBI Deputy Assistant Director of the FBI's Criminal Investigative Division, after the FBI Deputy raised the collective concerns on [REDACTED] to the then-Section Chief of the FBI's Criminal Investigative Division and an FBI Office of General Counsel (OGC) attorney. The FBI OGC attorney told us that after reviewing the statute and the DIOG it was clear to her that in "the FBI world you have to have a specific predicated investigation" to issue an administrative subpoena, but the DEA was not necessarily subject to the same constraints.<sup>99</sup> The FBI OGC attorney said that she informed the FBI Deputy Assistant Director that the FBI could not have used its administrative subpoena authority for [REDACTED], if it was an FBI program, "unless we had an individual [or organization] that we're trying to target" because of the DIOG's requirements. However, the FBI OGC attorney stated that she also explained to the Deputy Assistant Director that the FBI

---

<sup>99</sup> The FBI OGC attorney told us that the FBI lawyers who wrote the DIOG interpreted the statute, 21 U.S.C. § 876(a), to require an open investigation, or in FBI policy a "predicated investigation" particularized to a target. However, she told us that she understood that the DEA did not have such policy constraints.

could use the █████-subpoenaed data because the DEA collected the data under its authority (and not at the FBI's direction).

The FBI OGC attorney told us that after hearing these points the FBI Deputy Assistant Director decided that the FBI would not participate in █████ at the Fusion Center.

The FBI Deputy said that he notified the Fusion Center management about the FBI's decision not to participate in █████ and it was "not received well," particularly by DEA as the "parent agency" pushing the initiative. According to Fusion Center Chief Counsel, the FBI's decision not to participate in █████ at the Fusion Center was the primary reason why the Fusion Center's then-Acting Director (not a DEA employee) decided not to make █████ a permanent part of the Fusion Center operations after the pilot project ended. FO ceased sending █████-subpoenaed data to the Fusion Center in August 2013. We turn next to the DEA's legal review of █████ in late July 2013 in response to the OIG's inquiries.

### **C. OCC's Review before OIG Meeting in August 2013**

Two months after McKnight reported the FBI's concerns on █████, OCC initiated a legal review of the program in response to inquiries that DEA had recently received about the program from the OIG. Specifically, in late July 2013, DEA's CCM Section Chief assigned a senior CCM attorney (Senior Attorney 2) to review whether the DEA's use of administrative subpoenas in █████ was overbroad in preparation for an upcoming meeting with the OIG. Senior Attorney 2 sent his legal assessment in two lengthy emails to the CCM Section Chief and OCC senior manager, Maura Quinn.<sup>100</sup>

In the first email, Senior Attorney 2 discussed at length the 2005 NDDS memorandum regarding █████ which, as described in Chapter Three, highlighted the relevance of the court opinions in *Bisceglia* and *Peters* to the question of whether the DEA's Section 876(a) authority would permit the collection of bulk, non-target-specific data for "exploratory purposes." Senior Attorney 2 noted that the 2005 NDDS memorandum was "directly on point" to analyze the use of "exploratory" or non-target-specific subpoenas in █████. His review of the memorandum's in-depth analysis of court rulings concluded that it was "unclear what a court would do with the █████ subpoenas" because of conflicting court rulings in the most comparable cases.

In the second email, Senior Attorney 2 addressed Quinn's question on whether the language in the █████ administrative subpoenas was "legally sufficient." He responded to Quinn that the DEA had a "good-faith belief that the █████ subpoenas are legally sustainable," even if not directed to a particular suspect, based on █████ found in prior drug trafficking investigations. However, he stated that he thought the █████ subpoenas "would be quashed" if

---

<sup>100</sup> At the time, Quinn was serving as Acting Deputy Chief Counsel for Operational Law, which oversaw CCM.

challenged in the Ninth Circuit Federal Court of Appeals, which issued the *Peters* opinion.

Quinn told us in her interview that she did not recall a specific discussion with Senior Attorney 2 or others about his legal assessment on [REDACTED]. She also told us that OCC did not issue a final assessment on the propriety of the [REDACTED] subpoenas after Senior Attorney 2's review because the DEA ceased issuing the [REDACTED] subpoenas in September 2013. However, she stated that "risks" were highlighted to senior managers if the program continued after the Washington Field Division stopped issuing the [REDACTED] subpoenas, as discussed below.

### **III. DEA Stops Issuing [REDACTED] Subpoenas**

The DEA told us that the Washington Field Division provided FO with the last administrative subpoenas for [REDACTED] on or about August 1, 2013, and these subpoenas were sent to the respective companies on September 16, 2013.

In July 2013, Kevin Carter became an Assistant Special Agent-in-Charge of the Washington Field Division and received an overview of the office's activities, including [REDACTED]. He told us that he assumed from the brief overview on [REDACTED] that his office's involvement related to active criminal investigations on specific targets being done by his office. However, he told us that sometime between late July and early August 2013 he learned that his office's involvement did not involve any specific cases when he was given a large stack of [REDACTED] subpoenas to sign. Carter told us that he did not feel comfortable signing subpoenas unrelated his office's specific cases and instructed the Special Agent assigned to [REDACTED] to notify FO that the August 2013 batch would be the last one signed by him.<sup>101</sup>

Nevertheless, FO sent the next batch of unsigned subpoenas to Carter in December 2013. Like prior batches, these were blanket subpoenas that did not relate to specific, identified cases. Carter told us he refused to sign these [REDACTED] administrative subpoenas requested by FO.

FO continued to seek reinstatement of the [REDACTED] program. In late March 2014, the then-FO Chief emailed Quinn inquiring whether the Washington Field Division or some other DEA office with delegated subpoena authority could issue [REDACTED] subpoenas. Quinn told us that she pointed out the risks with continuing [REDACTED] to the Acting Chief of Operations and others, which included legal risks on whether the statute permitted such use and the current environment (in which the NSA's bulk telephone metadata collection program had been criticized by privacy advocates and the Obama administration had outlined plans to end it).

---

<sup>101</sup> Carter told the OIG that he signed the batch in August because [REDACTED] was a recognized headquarters program, the subpoenas had already been prepared, and he had not an opportunity to instruct his staff to notify the FO point-of-contact that he would no longer sign them.



Quinn told us that the Acting Chief of Operations favored continuing with the [REDACTED] subpoenas notwithstanding the risks.

In May 2014, the then-DEA Deputy Administrator transferred [REDACTED] responsibility from FO to NS, which had been delegated administrative subpoena authority (and issued the [REDACTED] subpoenas discussed in Chapter Three). However, according to the DEA, NS has not issued any subpoenas for [REDACTED] and the program has not been reinitiated since it was transferred to NS. The DEA Special Assistant to the NS Chief told us that the NS Chief never gave him the “green light” to restart [REDACTED]. The Special Assistant told us that the NS Chief told him they would not restart the program until they received approval from senior DEA managers, which they have never received, and that the program remains dormant.

However, the Chicago Field Division (and possibly others) continued to issue their own administrative subpoenas related to local [REDACTED] purchases. We were told that the Chicago Field Division continued issuing such subpoenas until approximately November 2014, when field division personnel heard about the OIG review of the [REDACTED] program.<sup>102</sup> We found no evidence that any DEA field offices have continued to issue blanket subpoenas for local [REDACTED] purchase data since November 2014. Further, the DEA stated in information responses to the OIG that no DEA field offices are issuing administrative subpoenas on behalf of FO for [REDACTED].

#### **IV. DEA Assessments of Value of the Program**

Former FO managers and [REDACTED] Staff Coordinators uniformly told us that [REDACTED] was a valuable and worthwhile program. McKnight told us that it was a very successful program that brought benefit to DEA, notwithstanding his issues regarding resources and quality of leads. Similarly, the first and second [REDACTED] Staff Coordinators echoed that [REDACTED] was a resounding success, citing that it resulted in approximately \$50 million of drug proceeds seized, significant seizures of illegal drugs and drug-related assets, and arrests based on the spreadsheet that FO used to compile results.<sup>103</sup> Powers also said that the

---

<sup>102</sup> We obtained sample copies of administrative subpoenas issued by the Chicago Field Division after the Washington Field Division ceased issuing them on behalf of FO. Although these subpoenas contained different language, they were functionally equivalent in that they requested the same [REDACTED] information under the same general program file code of [REDACTED] for the national initiative.

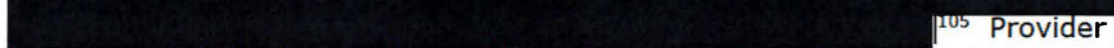
<sup>103</sup> FO’s spreadsheet showed the following cumulative results for [REDACTED] for FY 2008 through 2014: (1) 131 arrests, (2) \$48 million in drug-related cash seized, (3) 88 vehicles seized (worth approximately \$207,000), (4) \$4 million in real property seized, (5) 179 firearms seized, (6) 162 grams of crack seized, (7) 678 kilograms of cocaine seized, (8) 0 tablets of ecstasy seized, (9) 148 pounds of methamphetamine seized, (10) 21,381 pounds of marijuana seized, and (11) 22 kilograms of heroin seized. The OIG did not seek to test or corroborate these totals, particularly given the DEA’s acknowledgment, noted earlier, that the results for the majority of years reported, FY 2010 through FY 2013, are not attributed solely to [REDACTED], but rather include results from another operational component unrelated to use of the [REDACTED] subpoenas that cannot be separately reported.

program, as run locally by the Chicago Field Division, was viewed as a success that resulted in sizeable seizures of drugs, money, and guns. FO's results compiled for the Chicago Field Division showed that Chicago was in the top tier of divisional results for most metrics, including approximately 25 percent of all seizures of drug-related proceeds and 63 percent of all seizures of firearms attributable to █████ nationwide.

A former FO Section Chief from March 2014 to February 2015, told the OIG that the arrests and seizures attributable to █████ likely were under-reported because FO lacked a "standardized" and "consistent" process for field divisions to report results to FO on a set schedule. He added that "as a manager" the fact that FO personnel could not provide him with statistical results for █████ at any "given time" was a "problem." Indeed, as discussed earlier, the first █████ Staff Coordinator did not proactively monitor what field divisions did with the leads; rather, field divisions reported results to him as they happened and in their preferred reporting format. Additionally, the second █████ Staff Coordinator told us that he was not aware of any official reporting directive for the field divisions to report results. He said that he endeavored to check for results in the █████ module at least on a quarterly basis, but found the process cumbersome and not easy to access the results. Aside from the statistics noted above, the DEA Administrator's quarterly issue papers, used to keep the Administrator current on issues or congressional matters, routinely included a bulleted-reference to █████ as one of the important national financial initiatives targeting drug traffickers.

## CHAPTER FIVE THE HEMISPHERE PROGRAM

As noted in the Introduction, this report also addresses programs where the DEA uses its administrative subpoena authority to benefit from a company's ability to exploit its own bulk data, such as the Hemisphere program (initiated by the High Intensity Drug Trafficking Area (HIDTA) program).<sup>104</sup> Hemisphere is a contractual service program between law enforcement agencies and a telecommunications service provider (Provider B) under which Provider B maintains and exploits a vast collection of bulk telephone metadata to produce expedited or advanced telephone analytical products in response to target-specific administrative subpoenas or other compulsory legal process. Provider B developed this law enforcement sensitive program on its own initiative.

<sup>105</sup> Provider B has promoted Hemisphere's capability to aid narcotics enforcement by serving as an "intelligence pointer system" that could expeditiously identify leads in drug cases from a target's telephone calling activities. The DEA is a major customer for Hemisphere products, and some DEA employees have had a role in administering the use of the Hemisphere when detailed to HIDTA program offices, where Hemisphere is located, as discussed below.<sup>106</sup>

---

<sup>104</sup> The DEA stated that Hemisphere is not a DEA program and is target-specific, and thus should not be included within the purview of this report. We disagree. As noted above, the scope of the review included the DEA's employment of its administrative subpoena authority to obtain products from a private company that maintains and exploits its own private "bulk collection." The complex legal, policy, and privacy issues implicated in such a use of the DEA's subpoena authority may change but do not disappear by virtue of the fact that a private company is willing to maintain and mine its own bulk data collection on behalf of law enforcement agencies, such as the DEA, pursuant to contractual arrangements with them. Moreover, although Hemisphere may not be a "DEA Program," as shown in this Chapter, the DEA was the largest user of the program, and its employees at various times have had a significant role in its administering the use of Hemisphere when detailed to High Intensity Drug Trafficking Area (HIDTA) program offices through which the Hemisphere program is run.

<sup>105</sup> See U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records*, January 2010.

<sup>106</sup> The HIDTA program is a grant program administered by the Office of National Drug Control Policy (ONDCP), a component of the Executive Office of the President, established by the Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181 (1988). The HIDTA program aims to reduce drug trafficking in "high intensity" areas in the United States through specific initiatives, which are sponsored by federal, state, tribal, and local law enforcement agencies and funded by grants from ONDCP. See 21 U.S.C. § 1706; <https://www.whitehouse.gov/ondcp/grants> (accessed Sept. 13, 2016). The DEA assigns hundreds of special agents to the 28 HIDTA program offices in the United States, and senior DEA field division managers typically serve on the Executive Boards in each region that oversee individual HIDTA program offices. See <https://www.dea.gov/ops/hidta.shtml> (DEA Programs: High Intensity Drug Trafficking Areas) (accessed Sept. 12, 2016).



## **I. Elements of the Hemisphere Program**

### **A. The Data Used in the Hemisphere Program**

[REDACTED] Since the Hemisphere program began, Provider B has accrued billions of non-content calling records for more than 15 years of international and long distance calls. These call detail records or telephone metadata included the originating telephone number, the receiving number, and the date, time, and duration of the call.

### **B. The Hemisphere Analytical Products**

Provider B queries its proprietary database to create three different analytical products at the request of law enforcement customers, including the DEA: (1) a basic product that provides analysis of calls made or received on the target phone; [REDACTED]

The unique nature of Provider B's data collection and analytical capabilities enables it to offer products to law enforcement customers within hours or days of a request, and products that are derived from a database of more than 15 years of telephone metadata that is not limited to a particular telephone service provider.

#### **1. Basic Product**

The Hemisphere program's "basic product" prepared for law enforcement users is a report identifying the telephone numbers that were in direct contact with a particular target number, typically for the past 90 days, including the date, time, and duration of each call. The basic product contains similar metadata on a target's calling activity as can be obtained by a conventional subpoena for telephone records [REDACTED]

However, unlike standard subpoena returns, the basic product includes hours-old calling activities [REDACTED] The basic product

may also contain additional details regarding the telephone metadata that could aid law enforcement, such as identifying calls to or from a prison and calls made with prepaid calling cards.

Further, the basic product may include, when possible, the general location data (city or state or country) for cell phone calls made or received out of the target's home service area.<sup>108</sup> The Hemisphere program captures this general location data when long distance or international cell phone calls are [REDACTED] for the calls to reach their destination.

The basic product may also, if requested, include various analytical summary reports of a target's calling activities to spur investigatory activities, such as the 10 most frequently dialed numbers with date range and frequency rate, and the top 10 most recent outgoing or incoming calls by date.

## **2. Advanced Product**

If requested, Provider B is also able to provide an advanced product that analyzes calls [REDACTED]

[REDACTED] However, as detailed below, since 2008 DEA policy has prohibited its employees from obtaining such products through a single Hemisphere request.

## **3. [REDACTED] Products**

[REDACTED]

[REDACTED]



[REDACTED]

### **C. Value of Hemisphere Products to the DEA**

Historically, the DEA has been the most frequent federal agency user of Hemisphere. DEA personnel told us that the Hemisphere program enables the DEA to uncover unknown connections and leads in its drug investigations, particularly by providing quick responses and [REDACTED] DEA personnel told us that quick response time is important because DEA investigations generally are time-sensitive and event-driven, and under the Hemisphere program Provider B can respond in 48 hours versus other carriers who respond in 1 to 3 months. DEA personnel likewise stated that the program's [REDACTED] is the most significant service provided because it would be resource-intensive and challenging for the DEA to replicate that process using conventional subpoenas, a process that would require the in-house analysis of voluminous telephone metadata, and involve administrative subpoenas to more than one phone company, which could not respond as quickly. Witnesses told us that the ability of the Hemisphere program to reduce the time to [REDACTED] is a significant benefit for the DEA because the major drug trafficking organizations seek to evade DEA targeting [REDACTED]

Witnesses told us that the Hemisphere program does not necessarily provide precise results, but saves significant time by "pointing" to relevant telephone numbers on which to focus further attention. Hemisphere training materials that we reviewed similarly emphasized that the program should be used as a "pointer" system, and stated that the program "averages a strong success rate" without further description. One DEA analyst told us that his anecdotal experience was that it has about an 80 percent accuracy rate in identifying relevant telephone numbers, though we were unable to confirm this based on the available documentation. Further, witnesses told us that, [REDACTED]

[REDACTED] Hemisphere is not a substitute for obtaining a complete record of the target's calling activity from his or her direct service provider.

### **D. The Hemisphere Subpoenas**

Unlike [REDACTED] and [REDACTED] the DEA's administrative subpoenas for Hemisphere are issued for particular identifiable investigations or targets, as reflected by the case file numbers and target telephone numbers, listed in the body of the subpoenas. Besides the signed subpoena, a Hemisphere subpoena package also included a specific subpoena attachment (referred to as a rider) and a request form.

Hemisphere subpoenas are currently prepared using a Hemisphere-specific template, approved by the DEA's Office of Chief Counsel (OCC), and accessible on the DEA's Analysis and Response Tracking System (DARTS) only to a limited set of DEA personnel.<sup>109</sup> Once completed, the Hemisphere subpoenas are reviewed and approved at the field-level by those DEA managers with delegated subpoena authority, in the same manner that conventional administrative subpoenas are reviewed and approved.

The Hemisphere subpoena template is similar to a conventional administrative subpoena for telephone records, except that it provides specific instructions in an attached subpoena rider. One rider, known as a "basic" or "level 1" rider, is used for Hemisphere requests seeking only the target's direct calling activity—all calls placed and all calls received during a specified period. The other rider, known as an "advanced" or "level 2" rider, is used for Hemisphere requests seeking [REDACTED]

[REDACTED] The "advanced" rider has virtually the same language as the "basic" one, except that paragraph 3 of the "advanced" rider, as discussed in detail below, requests that the company produce for the particular target number:

[REDACTED] As detailed below, this language created much confusion during Department and DEA legal reviews of Hemisphere because Provider B does not [REDACTED]

Further, DEA requesters are also required to complete a standard "Hemisphere Project Request Form" that facilitates processing and includes the requester's contact information, type of request and special instructions, and level of priority.

## **E. Administration of the Hemisphere Program**

In this section we describe the evolution of the administration of the Hemisphere program over time. The Hemisphere program has largely been administered without a central managerial entity.<sup>110</sup>

---

<sup>109</sup> According to DEA documents and testimony, the DEA limits access to the Hemisphere subpoena template mainly to intelligence analysts or those assigned to HIDTA task forces given the sensitive, intelligence-nature of the program.

<sup>110</sup> A significant reason for the lack of a central managerial entity stems from the structure of the HIDTA program in which each HIDTA program office is located in a different region, and is controlled by a separate Executive Board, as noted above.

In 2007, the Hemisphere program was established in the [REDACTED] HIDTA program office to aid in targeted drug enforcement and to disrupt activities of major drug trafficking organizations. Since then, the Hemisphere program has been made available to those federal, state, local, and tribal law enforcement agencies participating in the HIDTA program, which includes on the federal level the DEA, the FBI, the Department of Homeland Security (DHS), and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

Hemisphere products were first made available to HIDTA program participants in March 2007, after the [REDACTED] HIDTA Director funded the Hemisphere program on a trial basis. Later in 2007, the [REDACTED] HIDTA Director obtained approximately \$1 million in funding from ONDCP to establish permanent Hemisphere program centers at the HIDTA Intelligence Support Centers in [REDACTED] and [REDACTED]. In 2008, ONDCP funded a third Hemisphere program center at the HIDTA Intelligence Support Center in [REDACTED]. The funding for the Hemisphere program covered the cost of two of Provider B's analysts at each location to expeditiously process requests from HIDTA program participants.

Although Hemisphere is funded through the HIDTA program, the HIDTA program is not an agency and does not exert any oversight over users of the Hemisphere program or over the on-site analysts who report to Provider B.

Additionally, the three Hemisphere program centers (located in the HIDTA Intelligence Support Centers) operated independently of one another without an overall program manager. DEA personnel who periodically worked at the Hemisphere program centers, including in supervisory roles, confirmed this independent nature. For example, a former DEA Group Supervisor, who established and oversaw the [REDACTED] Hemisphere program center for 5 years, told us that she had little interaction with her counterparts in [REDACTED] and [REDACTED]. Similarly, a former [REDACTED] Police Department sergeant, who oversaw the [REDACTED] Hemisphere program center for 5 years, told us that each center ran their Hemisphere program separately.

Notwithstanding the lack of a central administrative authority, the [REDACTED] HIDTA Intelligence Support Center, as the initial Hemisphere program center, took a lead role in establishing some consistent programmatic measures. For example, the [REDACTED] HIDTA Intelligence Support Center developed PowerPoint training materials and provided in-person tutorials on the Hemisphere program and the request process, which DEA personnel assigned to HIDTA program offices attended. The [REDACTED] and [REDACTED] Hemisphere program centers used these materials to adopt similar procedures to vet requests and to develop similar training documents in their regions. But, the Hemisphere program lacked standard written guidelines or operating procedures applicable to all of the program centers.

The HIDTA Intelligence Support Centers are dependent on grant money from ONDCP to support the Hemisphere program and other entities to receive



the funds.<sup>111</sup> The DEA provided significant stopgap funding to continue existing Hemisphere program services in 2011 and 2012. In 2011, for example, the then Executive Assistant to the DEA's Intelligence Chief, [REDACTED], noted internally that the DEA provided approximately \$150,000 to support Hemisphere program services because the "DEA is the largest user of Hemisphere" and is a "significant participant" at the HIDTA Intelligence Support Centers. Also, in 2012, the DEA provided funding of approximately \$200,000 to support Hemisphere program services.

ONDCP funding constraints in recent years led to the closure of the Hemisphere program center in [REDACTED] and reduced the number of on-site analysts from six to two.<sup>112</sup> As of 2016, HIDTA program offices collectively allocate a portion of their respective ONDCP grant funding to pay for these on-site analysts, one each in [REDACTED] and [REDACTED].

The relationship between Provider B and the Hemisphere program centers (HIDTA Intelligence Support Centers) has been managed as a business with its client/customer. Provider B's on-site analysts reported to off-site managers employed by Provider B who solicited feedback from users on the analysts' performance. For instance, the former [REDACTED] Police Department sergeant told us that when off-site managers of Provider B sought his input on whether as a "customer" the [REDACTED] HIDTA program was satisfied with the Provider B's on-site analysts' performance, he said he was because results were produced quickly. Similarly, the former DEA Group Supervisor stated Provider B's managers solicited feedback on the performance of their on-site analysts from the [REDACTED] HIDTA Director. She characterized the on-site analysts' performance as "very responsible and professional."

#### F. [REDACTED]

In order to protect the unique capabilities of the program from discovery, HIDTA program participants have been instructed not to use the information provided in Hemisphere reports in official files or court documents. Instead, users such as the DEA may [REDACTED]

[REDACTED] This typically requires issuing a "parallel subpoena" to the target's service provider for the relevant records in the investigation. [REDACTED]

---

<sup>111</sup> Because HIDTAs are not legal entities, ONDCP must provide HIDTA program funds to one or more legal entities, such as a state, local, or tribal agency, to act as the grantee(s) for agencies participating in the HIDTA program. See [http://www.nhac.org/hidta\\_guidance/guidance2012.pdf](http://www.nhac.org/hidta_guidance/guidance2012.pdf), p. 6-1, (accessed November 21, 2016).

<sup>112</sup> Requests previously sent to [REDACTED] are now sent to [REDACTED]

There are also important practical reasons for issuing “parallel subpoenas.” As discussed above, the Hemisphere program would only produce results for calls involving the target that were [REDACTED]. Additionally, the Hemisphere program caveated all of its products [REDACTED]. Therefore, the Hemisphere program instructed users that issuing parallel subpoenas to the official telecommunications service providers for the target phones would ensure that law enforcement personnel obtained all of the target’s calling activity during a particular timeframe.

### **G. Programmatic Safeguards**

The first programmatic safeguard for Hemisphere is that DEA requesters must demonstrate to their field supervisors that their Hemisphere-specific requests are “relevant or material” to narcotics investigations, as required under 21 U.S.C. § 876(a), before the Hemisphere-specific subpoena will be approved and signed. This demonstration is no different than that required for the DEA’s conventional administrative subpoenas to telephone companies, which do not require written justification. We were told that, as is the case for conventional subpoenas, the DEA does not require a particularly detailed demonstration of how the requested information is relevant or material to a Title 21 investigation in order to approve a Hemisphere subpoena.

A second safeguard is that access to the Hemisphere database is limited. In contrast to [REDACTED] and [REDACTED] the DEA does not control or maintain the bulk data in the Hemisphere program. The Hemisphere data is stored electronically at Provider B’s facilities where only Provider B’s analysts have direct access. Additionally, requests for Hemisphere products are only processed upon receipt of the required subpoena package through the proper program channels. Currently, subpoena packages are submitted through a secure virtual private network system accessed by user name and password.

We confirmed the existence of these safeguards from interviews and the documents obtained from the DEA and the FBI. For example, the Hemisphere program documents consistently state that no data will be provided without a subpoena and requests must be submitted to the Hemisphere program centers. DEA personnel involved with Hemisphere corroborated these statements in testimony. In particular, the former DEA Group Supervisor told us that when she oversaw the Hemisphere program center in [REDACTED] her staff always ensured that there was a signed subpoena in the required subpoena package before forwarding the request for processing. She also told us that the on-site analysts were located in a closed-door office space, physically separated from HIDTA Intelligence Support Center personnel, and used their own secure equipment and computers to query the Hemisphere database.<sup>113</sup> She further told us that

---

<sup>113</sup> According to the DEA, the Hemisphere on-site analysts no longer process requests for Hemisphere products at the HIDTA Intelligence Support Centers.

the on-site analysts were considered separate from the HIDTA program office personnel and did not attend staff meetings.

## **V. Legal Review of Hemisphere**

In this section, we describe four occasions in which questions were raised regarding whether the data provided from Hemisphere program was legally permissible to obtain through the DEA's administrative subpoena authority under 21 U.S.C. § 876(a) and 18 U.S.C. § 2703(c)(2).

### **A. Field Request for Legal Review in August 2007**

In August 2007, soon after the trial phase for Hemisphere ended, a DEA Group Supervisor from the [REDACTED] Division who was assigned to a [REDACTED] HITDA program office requested assurance from OCC that participation in the program had OCC approval. To facilitate that review, the DEA Group Supervisor emailed OCC a 122-page training document prepared by the [REDACTED] HIDTA Intelligence Support Center, which described the program in detail.

In response, OCC prepared a draft memorandum in September 2007 identifying the program's ability to provide [REDACTED] data for cell phones as a potential legal concern. The draft memorandum stated that it was unclear from the training document precisely what [REDACTED] was provided—[REDACTED]—or to what extent it would be available to be obtained by administrative subpoena under 18 U.S.C. § 2703(c)(2)(C) of ECPA (authorizing the carrier to disclose local and long distance connection records in response to administrative subpoenas).<sup>114</sup> The draft memorandum requested that the DEA's [REDACTED] Division provide more details on the geographic information being provided under the Hemisphere program in response to DEA's administrative subpoenas. Although OCC's Associate Chief Counsel, [REDACTED] signed a final memorandum without substantive changes, which was sent to the [REDACTED] Division on September 14, 2007, we found no evidence that the DEA's [REDACTED] Division ever provided the requested information or that OCC substantively addressed the issue raised in the memorandum at a later date.

### **B. Field Request for Legal Guidance in 2008**

In February 2008, a DEA Special Agent-in-Charge (SAC) sent an email requesting guidance from senior DEA officials on the DEA's use of Hemisphere after attending a Hemisphere program training session for federal, state, and local law enforcement personnel. The SAC expressed a major concern regarding the program's apparent practice of [REDACTED]

---

<sup>114</sup> The memorandum stated "because [REDACTED] data is typically available only with a § 2703(d) [court] order, we request that you provide this office more detail on the [REDACTED] information being provided under the authority of an administrative subpoena."



[REDACTED] He warned:

I do not know how many times they can or will do this, but I believe this may result in major problems for DEA in the future relative to our subpoena authority. I know how powerful an authority DEA has with admin subpoenas and I would not want to see the Hemisphere project harm that.

The SAC told senior DEA officials that he wanted to discuss this issue "as soon as possible to give proper guidance" to the DEA field division personnel.

Following several months of discussions among senior DEA officials and OCC, on August 4, 2008, [REDACTED] (Assistant Administrator of the Operational Support Division) issued a memorandum to all DEA field division managers that established the DEA's guidelines for use of the program ([REDACTED] Memorandum).<sup>116</sup> OCC concurred in the memorandum before it was issued. The [REDACTED] Memorandum provided that Hemisphere subpoenas may only be used for ongoing DEA cases and that all requests for Hemisphere products must use the specific Hemisphere administrative subpoena template in DARTS, approved by OCC. The [REDACTED] Memorandum also stated that most requests should use the "basic" rider, except for [REDACTED] which should use the "advanced" rider with the [REDACTED] language.<sup>117</sup> Additionally, the [REDACTED] Memorandum stated that any request for [REDACTED] [REDACTED] thereby effectively eliminating the "Advanced Product" request for such information absent a follow up subpoena.<sup>118</sup> The [REDACTED] Memorandum included as attachments sample Hemisphere request forms as well as a two-page protocol (Hemisphere Protocol) on completing the subpoena

---

<sup>116</sup> [REDACTED] was the DEA's SAC at the [REDACTED] Field Division during the Hemisphere trial phase at the [REDACTED] HIDTA Intelligence Support Center. Shortly thereafter, he became the Assistant Administrator for the Operational Support Division at DEA Headquarters.

<sup>117</sup> As detailed below, Provider B required the subpoena rider for [REDACTED]

<sup>118</sup> As an illustrative example, the [REDACTED] Memorandum stated that if a request on a target telephone number of [REDACTED] gave results of phone number [REDACTED] and several other numbers, then each subsequent request for calling data on the results would require a new subpoena, as if it were the first-time request.

and request form. The Hemisphere Protocol also instructed DEA personnel to send Hemisphere results to the DEA's central repository for telephone metadata as routinely done for all telephone metadata obtained by administrative subpoena in any case.<sup>119</sup>

We did not find evidence that the [REDACTED] Memorandum was widely disseminated to Hemisphere users at the DEA beyond initial distribution to then-existing field division management level (SACs, Associate SACs, Assistant SACs, and Field Division Intelligence Managers).<sup>120</sup> For example, several DEA personnel who had significant involvement with Hemisphere in their respective HIDTA program assignments, such as the former DEA Group Supervisor (who ran the [REDACTED] Hemisphere program center for 5 years), told us they had never seen the [REDACTED] Memorandum. Additionally, the evidence showed that DEA personnel were more familiar with the Hemisphere training guidelines not to mix Hemisphere data with official investigative data and treat it only as a "pointer" than the [REDACTED] Memorandum and attachments that instructed DEA personnel to upload Hemisphere data into the central repository.

### C. FBI Request for Legal Guidance in 2010

In early August 2010, then-FBI General Counsel [REDACTED] contacted then-DEA Chief Counsel [REDACTED] and then-Criminal Division Deputy Assistant Attorney General [REDACTED] with concerns regarding the Hemisphere program, particularly the "advanced" products, such as [REDACTED] that involve [REDACTED].<sup>121</sup> In August 2010, the FBI issued an Electronic Communication to all FBI SACs suspending use of the Hemisphere program until these concerns were resolved.

In response to the FBI's concerns, then-DEA Assistant Chief Counsel [REDACTED] contacted DEA field division personnel in [REDACTED] and [REDACTED] at [REDACTED] direction to "get a grasp on Operation Hemisphere" and understand what responsive information was provided with a [REDACTED] relayed to [REDACTED] that DEA field division personnel did not receive [REDACTED] even [REDACTED]

---

<sup>120</sup> Additionally, while it was beyond the scope of this review to try to review all DEA requests for Hemisphere products, our interviews and review of relevant materials did not uncover a practice by the DEA to [REDACTED] before or after the [REDACTED] Memorandum.

<sup>121</sup> The FBI General Counsel's concerns about Hemisphere were likely related to an OIG report on the FBI's use of National Security Letters to obtain certain telephone call records, which had been issued 8 months earlier. See U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records*, January 2010.



though the "advanced" rider for this request stated that such information should be provided.<sup>122</sup>

Around mid-August 2010, [REDACTED] met with DEA principals [REDACTED], [REDACTED], former DEA Deputy Chief Counsel for International and Intelligence Law), FBI principals ([REDACTED] and others), and designated principals from the ATF and DHS to discuss the FBI's concerns on the Hemisphere program.<sup>123</sup> According to an email summarizing the meeting, [REDACTED] requested the Criminal Division's opinion on: (1) whether law enforcement can obtain the identification of a new phone number for a subscriber [REDACTED], (2) whether law enforcement can obtain [REDACTED] and (3) whether law enforcement can obtain [REDACTED] with an administrative subpoena.

On August 26, 2010, [REDACTED] emailed the Criminal's Division "preliminary assessment" on these three issues, which [REDACTED] stated still required another meeting and additional facts before finalizing a view. First, [REDACTED] email stated that "there appears to be no clear *legal* impediment" (emphasis in original) to obtaining [REDACTED] but added that this practice should have some policy limits, such as [REDACTED]. Second, [REDACTED] email also stated that "there appears to be no clear *legal* impediment" (emphasis in original) to using a single administrative subpoena to obtain [REDACTED]. Once again, however, [REDACTED] email added that this practice should be bounded by policy considerations that could affect such usage. Third, [REDACTED] email stated that the [REDACTED] information for cell phones from Hemisphere [REDACTED] "does not clearly fall within the list of information" that can be obtained with an administrative subpoena under Section 2703(c)(2) of ECPA, 18 U.S.C. § 2703(c)(2), and thus this category of information required more discussion.

Between September and mid-October 2010, the Criminal Division arranged additional discussions with principals from the DEA, FBI, ATF, and DHS. According to emails, the group collectively agreed to revise the "advanced" rider for [REDACTED]

---

<sup>122</sup> As described above, the "advanced" rider containing [REDACTED]

[REDACTED] As noted, the [REDACTED] Memorandum did not permit the DEA to receive [REDACTED]. Even though the provisions of the [REDACTED] Memorandum were not widely known within DEA, witnesses told the OIG and that the advanced rider was not generally used to obtain such [REDACTED] information based on an initial subpoena.

<sup>123</sup> DHS was the next largest federal user of the Hemisphere program after the DEA. According to available data, the DEA's requests for Hemisphere products were approximately: 1.3 times greater than the DHS, 9 times greater than the FBI, and 60 times greater than ATF.



[REDACTED]

[REDACTED] The group also decided that it did not need to address "advanced" requests for [REDACTED] because their respective existing policies (such as the Memorandum for DEA) did not permit requests for such information. With respect to [REDACTED] information from Hemisphere [REDACTED], the Criminal Division's internal recommendation to the group was against receiving such information because the Criminal Division had not previously interpreted Section 2703(c)(2) of EPCA to permit [REDACTED] information by administrative subpoena. We found no evidence that the DEA communicated disagreement at that time with the Criminal Division.<sup>124</sup>

However, in November 2010, Provider B's counsel rejected the proposed revisions to the "advanced" rider for [REDACTED] on the basis that these advanced analytics were part of the Hemisphere program contract only and should not be referenced in the subpoena package, which could not compel this information. As memorialized by [REDACTED] Provider B's view was that the [REDACTED] demanded by the subpoena and attached rider in paragraph 3. The FBI found Provider B's response inadequate to address its initial concern that the rider should clearly state that [REDACTED]

Thereafter, the group's review of this matter ceased, in part because the Criminal Division attorney who had shepherded this issue on behalf of [REDACTED] announced her departure from the Department. [REDACTED] told us that he was not aware of any further Criminal Division assessment of the Hemisphere program after 2010.

In March 2011, the FBI issued its policy reauthorizing FBI use of the Hemisphere program. It contained the limitation that the FBI was not permitted to obtain any [REDACTED] with an administrative subpoena for Hemisphere products and that such information would be removed from products provided to the FBI. Additionally, the FBI policy did not permit the FBI to make requests for [REDACTED] so long as the existing subpoena rider still contained language requesting [REDACTED] (as it did in paragraph 3) as part of the analysis.

---

<sup>124</sup> In response to a draft version of this report, the DEA commented that it did not have the benefit of any written assessment from the Criminal Division that evaluated the permissibility of obtaining [REDACTED] derived from [REDACTED] in Hemisphere responses. Additionally, the DEA stated that it did not agree that such business records of Provider B were not permitted to be obtained by administrative subpoena. Notably, as discussed above, we found no evidence that the DEA itself completed a legal assessment on this issue when it was raised to OCC 3 years earlier in 2007.



The FBI's policy did not contain any written legal analysis that explained these policy decisions. According to an FBI email to the DEA, the FBI elected not to obtain [REDACTED] data for [REDACTED] from Hemisphere [REDACTED] due to the Criminal Division's recommendation that any actual [REDACTED] was not the proper subject of an administrative subpoena. Additionally, according to FBI testimony to the OIG, the FBI did not permit requests that sought [REDACTED] records with one administrative subpoena, or contained such language, because the FBI did not want to be associated with these requests, even in circumstances such as [REDACTED] requests where [REDACTED] in the rider language, but not provided in the response.<sup>125</sup>

In May 2011, the former [REDACTED] Police Department sergeant, who still ran the Hemisphere program center in [REDACTED] contacted [REDACTED] to determine if the DEA wanted [REDACTED] data removed from Hemisphere products consistent with the FBI's policy. He also inquired on status of a revised rider for [REDACTED] requests for both the FBI and the DEA to use, especially since the FBI attorney handling this issue had retired and a new one had recently taken over the issue. [REDACTED] responded that she was not aware that the FBI had issued its policy and the group that oversaw this matter had "faded away." [REDACTED] and the new FBI attorney made periodic efforts to discuss this issue, which we found ceased by June 2011.

#### **D. OCC Review in 2012-2013**

In September 2012, [REDACTED] assigned an attorney in the Technology Law Unit (Technology Attorney 1) to review one of the issues raised by the FBI in August 2010; namely, whether it was legally permissible for the DEA to use a single administrative subpoena (and the attached rider) to request [REDACTED]

[REDACTED] Technology Attorney 1 told us that [REDACTED] gave her this assignment at that time because the DEA intended to provide funding for the program. She added that no written legal analysis or formal assessments had emerged from the Department workgroup that reviewed these issues in August 2010 before it "just fell apart."

In early January 2013, Technology Attorney 1 completed her assessment in a draft memorandum she sent to [REDACTED]. The January 2013 draft memorandum addressed the question of whether the use of an administrative subpoena to [REDACTED] was legally permissible under ECPA. The draft memorandum noted that Section 2702(a)(3) of ECPA prohibits a communications service provider from knowingly divulging a record or other information pertaining to a subscriber to or customer of such

---

<sup>125</sup> The FBI also memorialized the restriction on obtaining records of [REDACTED] based on a [REDACTED] with one administrative subpoena in their Domestic Investigations Operations Guide (DIOG). See Section 18.6.4.3.3.2.3 of the DIOG.



service to any governmental authority, absent statutory authorization, such as a legally issued administrative subpoena. The memorandum concluded that this prohibition is applicable to Provider B when it accesses its own calling records "at the request of and for the benefit of" the government [REDACTED]

[REDACTED] even though the calling records analyzed by Provider B are not themselves given to the government. The memorandum stated: "The government cannot avoid the statutory prohibitions [against the provider divulging certain records] by working through private contractors." The memorandum therefore concluded that the government must issue a legally valid administrative subpoena in order to [REDACTED]

The draft memorandum concluded that the Hemisphere subpoenas, including the "advanced rider" language, are legally valid under 21 U.S.C. § 876(a) (which requires that the information be "relevant or material to" a narcotics investigation) and relevant case law (requiring among other things that the inquiry be within the authority of the agency, not too indefinite, and reasonably relevant). It stated: [REDACTED]

[REDACTED] are reasonably relevant to the legitimate investigative objective of [REDACTED] The memorandum found it significant that the call detail records on the [REDACTED] noting that these records are "relevant only insofar as [REDACTED]

The draft memorandum concluded that because the Hemisphere subpoenas for [REDACTED] are valid, Provider B is authorized to disclose that information and the government is authorized to compel its disclosure pursuant to a single subpoena under ECPA.

The draft memorandum noted that Provider B insisted that the subpoena rider used in [REDACTED] but stated "[w]e do not think this . . . is legally required to authorize" Provider B to access and analyze its own records. The memorandum recommended that the DEA eliminate this language. However, according to Technology Attorney 1, Provider B's counsel had rejected this proposal because Provider B decided, following an OIG report on the FBI's use of National Security Letters, that the rider must contain express language to reflect that the Provider B had been compelled under adequate legal authority to [REDACTED]

Technology Attorney 1's draft memorandum also addressed whether it is permissible under ECPA to obtain [REDACTED] for cell phones pursuant to a Hemisphere subpoena. It observed that, in general, [REDACTED] "pertaining to a subscriber to or customer of" an electronic



communications service typically requires a court order because it is not within the narrow list of information in Section 2703(c)(2) of ECPA, 18 U.S.C. § 2703(c)(2), that can be disclosed in response to an administrative subpoena. It noted, however, that an argument exists that the Hemisphere [REDACTED] data does not "pertain to" a subscriber or customer because such records reveal only the [REDACTED]

Thus, the memorandum stated that such information arguably falls outside of the customer or subscriber records protected by ECPA, and could therefore be obtained pursuant to the authority under 21 U.S.C. § 876(a). Nonetheless, the memorandum concluded that it "may be prudent as a matter of policy" not to obtain this information with an administrative subpoena because this area of law was unsettled.

The draft memorandum sent to [REDACTED] in January 2013 was never memorialized into a final product. [REDACTED] told us that she used the draft memorandum to ensure that the DEA's usage of Hemisphere was legally defensible and did not disseminate it further. Therefore, the DEA continued to make [REDACTED] requests with a single administrative subpoena and the existing "advanced" rider. Notwithstanding the draft memorandum's advice, as well as the concerns previously expressed by the DOJ working group, the DEA continued to obtain [REDACTED] when available via Hemisphere subpoenas. [REDACTED] told us that she did not confer with the Criminal Division on these issues because she believed that the Criminal Division had not done any formal analysis and had previously disregarded the issue.

After OCC's review, the DEA's use of Hemisphere remained different from the FBI in that FBI users were not permitted under FBI policy to receive [REDACTED] information for cell phones or [REDACTED] when the "advanced" rider still contained the [REDACTED] language. As noted above, the FBI elected not to obtain [REDACTED] data for cell phones from Hemisphere [REDACTED] due to the Criminal Division's recommendation that any actual [REDACTED] information was not the proper subject of an administrative subpoena. Additionally, according to FBI testimony to the OIG, the FBI did not permit requests that sought [REDACTED] records with one administrative subpoena, or contained such language, because the FBI did not want to be associated with these requests, even in circumstances such as [REDACTED]

[REDACTED] Technology Attorney 1 told us she viewed these usage differences as a probable cost-benefit policy choices, where the FBI may have opted for more restrictive use given their smaller drug investigation caseload. [REDACTED] concurred that it is a risk analysis assessment based on issues faced by the DEA and FBI in their respective enforcement operations. [REDACTED] said the DEA often has to address the issue of drug traffickers who [REDACTED] [REDACTED] is helpful to expeditiously address this issue—whereas this issue may be less of a concern for the FBI. As noted above, the DEA was the "largest user of

Hemisphere” and its requests for Hemisphere products were approximately nine times greater than the FBI.

## **CHAPTER SIX**

### **ANALYSIS AND RECOMMENDATIONS**

In this chapter the OIG presents our analysis and recommendations regarding the DEA's use of administrative subpoenas to exploit collections of bulk data. We focus on four main topics: (1) the sufficiency of legal reviews that have been conducted in connection with the bulk collection programs; (2) the adequacy of procedural safeguards that the DEA currently has in place to ensure, among other things, that DEA subpoenas are issued in full compliance with 21 U.S.C. § 876(a) and to prevent misuse of data collections; (3) the efficacy of audit procedures employed by the DEA with respect to ongoing bulk programs; and (4) the use of "parallel construction" to protect the programs from public disclosure.

#### **I. OIG Assessment of the Adequacy of Legal Review Conducted for the Bulk Collection Programs**

The [REDACTED] and [REDACTED] programs involved a uniquely expansive use of Section 876(a) authority to collect data in bulk without making a prior finding that the records were relevant to any specific defined investigation. The [REDACTED] program involved the collection of telephone call records for billions of telephone calls from the United States to many different countries. The DEA amassed this historical repository of information for future processing to later identify a tiny portion that would be relevant to actual drug investigations. In some respects, the [REDACTED] collection was even broader than [REDACTED]. [REDACTED], but was limited to the transactional details of the calls. Most or all of the [REDACTED] data was sent directly to the field offices for their use to develop new targets for investigation, without any pre-collection determination that a connection existed between the [REDACTED] and an existing investigation.

Both programs presented the question of whether a non-target-specific "exploratory" subpoena to collect bulk transactional data satisfied the requirement under 21 U.S.C. § 876(a) that the information sought be "relevant or material . . . to [an] investigation." The DEA's use of "exploratory" administrative subpoenas in [REDACTED] and [REDACTED] was not consistent with DEA's normal practice of issuing subpoenas in connection with a specific case or target. As a result, the language used in the [REDACTED] and [REDACTED] did not resemble standard DEA administrative subpoena language that Division counsel or OCC typically saw. In light of these circumstances, we would have expected a thorough legal analysis of this unique use before the DEA launched [REDACTED] or [REDACTED]. However, such was not the case.

Another issue raised by the bulk collection programs is whether the bulk collections, amassed pursuant to the DEA's authority to investigate narcotics cases, could permissibly be queried on behalf of other agencies in support of non-drug investigations. As detailed below, we did not find that the legal analysis of this issue was adequate either.

**A.** [REDACTED]

**1. Legal Validity under Section 876(a)**

We found no evidence that anyone in the Department or the DEA prepared a comprehensive legal analysis of [REDACTED], particularly the use of administrative subpoenas to amass a bulk collection of telephone metadata, prior to the program being established. The DEA did undertake a written legal analysis of the program in the August 1999 Memorandum. However, as far as we were able to determine, due to the close hold nature of the program, the August 1999 Memorandum had very limited distribution and was not intended to be the Department's "official legal review" regarding the permissibility of the [REDACTED] bulk collection. Therefore, it did not provide a comprehensive legal assessment on the statutory validity of the [REDACTED] subpoenas, which should have been prepared at program inception. Among other things, the August 1999 Memorandum did not address any of several published court decisions available at the time, (and at the time [REDACTED] began), clearly suggesting potential challenges to the validity of the DEA's use of Section 876(a) to amass the [REDACTED] collection. Among these decisions was *United States v. Bisceglia*, 420 U.S. 141 (1975), which upheld the Internal Revenue Service's use of its administrative summons authority to require a bank to produce documents evidencing all transactions of a certain type during a 1-month period, to aid in identifying the individual who had engaged in such transactions and might be liable for back taxes. Four concurring or dissenting justices in *Bisceglia* expressed deep concern about the permissibility of "exploratory" subpoenas lacking a connection to a genuine, extant investigation. In addition, the August 1999 Memorandum failed to discuss *Peters v. United States*, 853 F.2d 692 (9th Cir. 1988), in which the Ninth Circuit rejected a subpoena issued by the Immigration and Naturalization Service to a farm labor camp manager for all records pertaining to residents of the camp, which had been issued in support of a criminal investigation of unknown residents who might have been undocumented aliens. The court held that "we are reluctant to assume the existence of the power to issue third-party subpoenas directed at unidentified targets where Congress has not provided for them specifically, nor provided procedural safeguards." 853 F.2d at 696.

The earliest written evidence that we found in which the Department (or the DEA) specifically considered and assessed the legal vulnerabilities posed by the use of "exploratory" subpoenas, as done in [REDACTED], was in 2005 when the DEA proposed to use subpoenas to collect bulk, [REDACTED]

[REDACTED] Then, DOJ Criminal Division attorneys in NDDS and AFMLS prepared legal analyses of [REDACTED] that highlighted the relevance of the *Bisceglia* and *Peters* opinions to the question of whether the DEA's subpoena authority would permit the collection of bulk, non-target-specific data for "exploratory purposes." As detailed in Chapter Three, we determined that the AFMLS memorandum explicitly linked the potential legal vulnerabilities of the [REDACTED] proposal as creating risks to the DEA's use of "exploratory" subpoenas to amass the [REDACTED] collection, and ultimately to the



[REDACTED]. In light of these risks, the Criminal Division convinced the DEA to obtain the equivalent information through alternative means.

The [REDACTED] controversy demonstrates that the Department and the DEA were aware of the existence of case law casting doubt on the use of administrative subpoenas to collect bulk data for exploratory purposes, including the [REDACTED] collection, at least as of 2005.<sup>126</sup> Yet we found no evidence that anyone in the Department or the DEA prepared a comprehensive legal analysis of [REDACTED] at any time during its operation, including after the issue was squarely raised in connection with [REDACTED] in 2005.

A more detailed legal analysis of the statutory basis for the [REDACTED] collection was OCC's 2013 Reinstatement Memorandum, which was prepared expressly for Department leadership after the Department suspended the program. In that document, the DEA cited numerous cases in support of an argument that the "relevant or material" standard under 21 U.S.C. § 876(a) is extremely broad and permits requests for the production of large collections of records. However, even the DEA's Reinstatement Memorandum failed to address the unique issues raised by the collection of bulk non-target-specific data by means of an exploratory subpoena that was unconnected to any specific suspect or investigation. In particular, it never addressed the concurring or dissenting opinions by the four Justices in *Bisceglia* or the Ninth Circuit's decision in *Peters*, even though the Criminal Division had pointed out the relevance of those decisions to DEA managers eight years earlier in connection with the analysis of [REDACTED].

It appears that one reason the Department and the DEA did not see the need for a critical legal analysis of the statutory validity of [REDACTED] subpoenas was its understanding that the issue was unlikely to be litigated because the DEA never intended to serve a subpoena on an unwilling carrier so that judicial enforcement would never be required.<sup>127</sup> [REDACTED]

---

<sup>126</sup> The Department and the DEA were also likely aware of such case law in the early years of [REDACTED] after a failed attempt to challenge the DEA's authority to issue a non-target-specific subpoena under 21 U.S.C. § 876(a) on the basis of the rulings in *Bisceglia* and *Peters*. Specifically, in 1996, the Tenth Circuit ruled that the defendant lacked standing to challenge the DEA's non-target-specific administrative subpoena, issued to Amtrak, seeking reservation records for a 1-month period, which DEA Special Agents analyzed to identify the defendant, who paid cash for his ticket, and subsequently found him traveling with a large amount of illicit drugs. See *United States v. Moffett*, 84 F.3d 1291 (10th Cir. 1996). Accordingly, the Tenth Circuit did "not reach the statutory construction issue defendant presses" on whether the DEA exceeded the scope of its statutory subpoena power in 21 U.S.C. § 876(a) by issuing a non-target-specific subpoena. *Id.* at 1293-94.

<sup>127</sup> The *Moffett* case would have provided additional support for the notion that no such review was required because the Department and the DEA could assert lack of standing to deflect most challenges, given that the DEA had the cooperation of the subpoena recipients as they had with Amtrak in *Moffett*.

[REDACTED] The DEA paid the carriers to comply with the subpoenas expeditiously and on an ongoing basis, and the Department reassured the carriers that their compliance was legal in letters.

We do believe, however, that even assuming the absence of litigation risk, there still should have been a thorough legal review to ensure that the Department was utilizing its authorities properly. Indeed, we believe that the intentional absence of effective judicial review made it more important that a careful internal analysis of the legal validity of the program be conducted to ensure that the program was conceived and operated in compliance with the law.<sup>128</sup>

Additionally, the issues underlying the Second Circuit's decision in *Am. Civil Liberties Union, et al., v. Clapper, et al.*, 785 F.3d 787 (2d Cir. 2015), provide further confirmation that the [REDACTED] program raised difficult issues that warranted careful examination by Department or DEA attorneys. Although *Clapper* was decided 2 years after the [REDACTED] program had been suspended and 20 years after it began, it is probative in our analysis of the legal authority for the [REDACTED] program because the bulk data collection addressed in *Clapper* was comparable to the [REDACTED] program and the legal issues confronted by the *Clapper* court were essentially the same issues that were relevant to and foreseeably raised by the Department's operation of the [REDACTED] program years earlier.

The NSA program at issue in *Clapper* involved the use of court-approved orders from the Foreign Intelligence Surveillance Court (FISC) to a U.S. telephone service provider for telephone metadata for virtually every call made through its systems or using its services, where one or both ends of the call were located in the United States. The orders were issued under the authority of Section 215 of Foreign Intelligence Surveillance Act (FISA), which at that time authorized the government to obtain a court order requiring the production of records, including metadata, upon a showing that the records are "relevant to an authorized investigation" to protect against international terrorism or clandestine intelligence activities. See 50 U.S.C. § 1861(a)(1), (b)(2)(A) (2014). Thus, the relevancy standard under Section 215 was similar to the requirement in Section 876(a) that records be "relevant or material to [an] investigation" relating to controlled substances and other listed subjects. 21 U.S.C. § 876(a).

The data collected included originating and terminating phone numbers, time and duration of the calls, and other metadata—data nearly identical to that collected through the [REDACTED] subpoenas but for an even larger set of calls,

---

<sup>128</sup> Indeed, as part of its brief and aborted internal review of [REDACTED] in 2014, OLC transmitted many follow-up requests to the DEA, including a request to identify case law shedding light on the meaning and scope of the terms "relevant or material to [an] investigation" in Section 876(a), to which the DEA responded that it would need "a couple of months" to complete, and never did because the program was discontinued.

unrestricted by the “drug nexus” requirement. Like the ██████ program, the NSA program involved the subsequent exploitation of the data collected by querying the collection with seed numbers that were believed, based on “reasonable articulable suspicion” (RAS), to be associated with a foreign terrorist organization. However, unlike the ██████ program, the RAS determination under the NSA program was not made unilaterally by the agency, but rather was subject to approval by the FISC in an ex parte proceeding.

The Second Circuit held that the NSA program was not authorized under Section 215 of FISA because the data being demanded initially did not satisfy the requirement that it be “relevant to an authorized investigation.” The court observed that “[t]he records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contacts with others who are in contact with such subjects.” 785 F.3d at 813. The government conceded that vast amount of metadata collected did not contain directly “relevant” information, but argued that such data was “nevertheless ‘relevant’ because they may allow the NSA at some unknown time in the future, to utilize its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant.” *Id.* at 812 (emphasis in original).

The court rejected this interpretation of “relevance” as defying “any limiting principle,” as it could be applied to collect and store in bulk any other sets of metadata available anywhere in the private sector, including metadata associated with financial records, emails, and social media relating to all Americans. *Id.* at 818. The court stated that “such an expansive development of government repositories of formerly private records would be an unprecedented contraction of privacy of all Americans.” *Id.* at 818.

As a result of the *Hassanshahi* case (discussed in Chapter Three), the Second Circuit was made aware of the DEA’s use of administrative subpoenas for the ██████ bulk data collection and observed that the ██████ program “may have demanded an interpretation approaching the breadth of the government’s interpretation of similar language [in Section 215]” that the court rejected in *Clapper*. *Id.* at 812, n.6. However, the court did not opine on whether the language of Section 876(a) permitted the DEA’s ██████ bulk data collection because the issue was not before it and the program had been discontinued. *Id.* Nevertheless, we believe that most or all of the reasoning found in *Clapper* would have likely applied with similar force in any judicial assessment of whether the DEA’s use of its subpoena authority to amass the ██████ collection was consistent with 21 U.S.C. § 876(a).<sup>129</sup> Indeed, some of the differences

---

<sup>129</sup> We are not opining that the Second Circuit’s ruling in *Clapper* would have ultimately meant that ██████ would have been found to be beyond the bounds of Section 876(a). The Department disagreed with the Second Circuit’s ruling in *Clapper* and was appealing it, but the case was mooted by the USA FREEDOM Act of 2015, which prohibited “bulk collection” under Section 215 of FISA. Additionally, as we note next, many judges had previously ruled that the NSA’s bulk telephone metadata program was consistent with Section 215 of FISA.

between the programs—such as the effective lack of independent judicial oversight for █████—might have made a challenge even more compelling.

To be clear, we are not opining that a thorough legal analysis of the █████ program would inevitably have concluded that the program was inconsistent with Section 876(a). There are arguments to the contrary and case law to support them, as reflected in the DEA's Reinstatement Memorandum. First, many of the cases the DEA cited and the arguments made regarding the broad concept of "relevance"—including "bulk collection" of records to identify the "relevant" data—were accepted by several FISC judges with respect to the NSA's bulk telephone metadata collection program prior to the amendments to Section 215 of FISA, and one federal district court judge from the Southern District of New York, prior to being overruled by the Second Circuit. See *Am. Civil Liberties Union, et al., v. Clapper, et al.*, 959 F. Supp. 2d 724, 746-49, (S.D.N.Y. 2013), rev'd, 785 F.3d 787 (2d Cir. 2015). Thus, reasonable minds may differ on at least this aspect of the issue. Second, it is unclear if the statutory term "investigation" in 21 U.S.C. § 876(a) countenances a "general investigation," consistent with Title 21 duties, that would permit the scope of administrative subpoenas issued for █████ or █████. E.g., *United States v. Oncology Servs. Corp.*, 60 F.3d 1015, 1020 (3d Cir. 1995) (finding that administrative subpoena could be issued for "general investigation" within agency's statutory authority) (citations omitted). Third, the government's burden in obtaining a court order to enforce compliance with an administrative subpoena is not significant, particularly with respect to "relevance" of the requested information. See, e.g., *Fed. Trade Comm'n v. Carter*, 636 F.2d 781, 788-89 (D.C. Cir. 1980) (citations omitted) (agency's determination of "relevance" satisfied "if the documents sought are 'not plainly irrelevant' to the investigative purpose" or not "'obviously wrong.'"); *Nat'l Labor Relations Bd. v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006) (noting that courts defer to an "agency's appraisal of relevancy" to its investigation "so long as it is not obviously wrong") (citations and internal quotations omitted). It is possible, therefore, that a court could conclude that the bulk collection obtained by █████ or █████ subpoenas was not "obviously wrong" to support the general investigative purposes of seeking evidence regarding illicit drug activities in the United States.

In sum, we observe that there were significant legal issues raised by the DEA's use of "exploratory subpoenas" that warranted a careful examination, and that this did not occur. In this regard, we previously concluded in our review of the Department's involvement with the President's Surveillance Program that "classified programs that press the bounds of established law" should be supported by a collaborative legal opinion of sufficient legal and technical expertise.<sup>130</sup> So too here.

---

<sup>130</sup> U.S. Department of Justice Office of the Inspector General, *A Review of the Department of Justice's Involvement with the President's Surveillance Program*, July 2009, at 395.

## 2. Querying the [REDACTED] Data for Non-Drug Investigations

We determined that on an unknown number of occasions, the [REDACTED] data collection that was created from 1993 through 2013 was queried in support of matters that had no known drug nexus, such as investigations of major terrorism events. As we have noted, the [REDACTED] collection was amassed pursuant to the DEA's authority to issue administrative subpoenas relevant to Title 21 drug investigations based on the theory that the countries to which the communications were directed had a sufficient nexus to illicit drug activities. In response to a specific OIG information request, the DEA told us it could not locate any legal reviews, analyses, or other documents that addressed the decision to allow the use of the [REDACTED] collection for non-drug cases, the criteria for allowing such uses, the volume of such cases, or the legal authority for such uses. Nor could we find any such documents among the materials provided from other DOJ components.

Moreover, as discussed above, it does not appear that the use of [REDACTED] in non-drug cases was limited to major terrorism investigations. In *United States v. Hassanshahi*, 145 F. Supp. 3d 75 (D.D.C. 2015), a United States District Court described a use of the [REDACTED] collection on behalf of Homeland Security Investigations, a DHS component, to develop evidence of a criminal violation of the United States' trade embargo against Iran. The DEA submitted a declaration stating that the [REDACTED] collection "could be used to query a telephone number where federal law enforcement officials had a reasonable articulable suspicion that the telephone number at issue was related to an *ongoing federal criminal investigation*." (Emphasis added). The defendant alleged that this use of the [REDACTED] data in a non-drug case violated 21 U.S.C. § 876(a). Quoting *Jabara v. Webster*, 691 F.2d 272, 277 (6th Cir. 1982), the government argued that this use was consistent with the longstanding legal rule that "[e]vidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken." 145 F. Supp. 3d at 83.

Although the Court in *Hassanshahi* did not rule on whether Homeland Security Investigations had established "reasonable articulable suspicion" for the database query request, the standard articulated by the government in that case implies that the DEA and the Department did not recognize any impediment to querying the [REDACTED] database, collected under the authority of Section 876(a), in support of *any* federal criminal investigation, without regard to whether the investigation related in any way to drug trafficking.

We believe that this theory of unlimited use raises difficult questions of law and policy that the DEA and the Department should have analyzed carefully. One of the DEA's justifications for using its Section 876(a) authority to collect metadata for billions of phone calls to scores of countries was that that the collection would be queried for *drug trafficking* investigations, thereby ensuring that the investigative products would be relevant and material to an investigation within the DEA's jurisdiction. Yet, this limit disappears if other

agencies, including agencies having no administrative subpoena authority of their own, can exploit this drug-derived collection for non-drug purposes.

Again, the OIG is not opining on whether the DEA's theory of the potentially unlimited sharing of the data collected through ██████ for non-drug investigations was or was not legally correct. We found only that neither the DEA nor the Department adequately framed or analyzed the issue in order to ensure that this vast collection of information was being used consistently with the law.<sup>131</sup>

**B. ██████**

The DEA likewise did not conduct or request any significant legal analysis to support its use of exploratory subpoenas before the ██████ program began. In July 2008, after the ██████ program had been initiated, Kevin J. Powers, the Division Counsel for DEA's Chicago office, asked whether anyone in OCC had addressed whether the ██████ subpoenas were in compliance with 21 U.S.C. § 876. Donna Sanger, an OCC manager, forwarded this request to Senior Attorney 1 who, after reviewing a sample subpoena, told Sanger 2 months later that she had "no legal objections" without elaboration. Sanger then emailed Powers, stating: "Unless a federal court tells us we can't do this, I think we can continue this project." However, as with ██████, a court review was unlikely because the subpoena recipient-companies agreed in advance to cooperate with the DEA, even if not paid, and had no real incentive to challenge the ██████ subpoenas.

We found that this conclusory email exchange did not reflect a timely or adequate review of whether the ██████ subpoenas were issued in compliance with Section 876(a). The substantive deficiency in the 2008 legal review should have been particularly apparent given the similar issues raised to senior managers in OCC regarding ██████ 3 years earlier, as discussed above. The DEA finally recognized the need for a more rigorous review of the legal underpinnings for ██████ after the OIG made inquiries about the program in 2013. In response to this inquiry, Senior Attorney 2 in OCC analyzed the ██████ program, noting that the 2005 NDDS memorandum about ██████ was "directly on point" to analyze the use of "exploratory" administrative subpoenas in ██████—though no one else in the OCC apparently recognized this in 2008. His review concluded that it was "unclear what a court would do with the ██████ subpoenas" because of conflicting court rulings, but thought they would be quashed if challenged in the Ninth Circuit Federal Court of Appeals pursuant to the *Peters* decision. Even without the benefit of the 2005 NDDS memorandum, the published judicial opinions discussed in the NDDS memorandum, including *Bisceglia* and *Peters*, existed long before ██████ began. Therefore, we believe

---

<sup>131</sup> The DEA maintains that the court ruling in *Jabara* resolved the issue of law enforcement's ability to share its data holdings without a warrant. This position assumes that the non-target-specific ██████ subpoenas used to amass the bulk data collection were consistent with Section 876(a) to fall under the *Jabara* principle that "evidence legally obtained" can be shared with other agencies. However, no court has so ruled.



that they should have factored into the 2008 legal review of whether the administrative subpoenas used for [REDACTED] were appropriate.

We determined that during part of 2013, data collected by means of [REDACTED] subpoenas was utilized on an unknown number of occasions to create Fusion Center products in support of investigations having no connection to drug crimes. For example, the Fusion Center created four intelligence products for DHS ICE using [REDACTED] data in support of investigations of alien smuggling, benefit fraud, trafficking in counterfeit merchandise, and firearms trafficking, as well as one intelligence product for the U.S. Secret Service relating to an investigation of false identification and alien registration cards. The [REDACTED]-subpoenaed data apparently could be used without limitation to create intelligence products for Fusion Center member agencies in support of non-drug investigations once the Fusion Center obtained member-agency supplied data.

As with the similar use of [REDACTED] data, we believe that the lack of limitations on the use of [REDACTED] data raised substantial questions of law and policy that the DEA and the Department (and potentially even other participating Fusion Center agencies utilizing such data) should have analyzed carefully.<sup>132</sup> The DEA's authority to collect detailed purchaser data for all purchases of [REDACTED] was based on the potential relevance of such data to drug investigations under the DEA's jurisdiction based on the belief that [REDACTED] were frequently used in connection with Title 21 offenses. Routinely transferring the collection to the Fusion Center for exploitation by other agencies in non-drug cases was arguably tantamount to the DEA lending out its subpoena authority to agencies lacking their own. We found no DEA or Department memoranda assessing the legality of this use, which again due to the nature of the program was unlikely to be otherwise tested through litigation.

As in our analysis of the [REDACTED] program, we are not opining that a thorough legal analysis of these issues would have concluded that [REDACTED] was inconsistent with Section 876(a) or that it could not be used in support of non-drug investigations. Rather, we note that the same serious and readily apparent legal issues raised by [REDACTED] were also raised by [REDACTED], and that likewise no thorough analysis of such issues occurred before or during the operation of the initiative.

**C.** [REDACTED]

[REDACTED]

---

<sup>132</sup> As detailed in Chapter Four, the FBI decided not to participate in the use of [REDACTED] data at the Fusion Center after FBI agents raised concerns regarding the broad scope of the non-target-specific [REDACTED] subpoenas, which was not consistent with the FBI's policy requirement of a "predicated investigation" to issue administrative subpoenas.

<sup>133</sup> [REDACTED]

[REDACTED]

[REDACTED]

135

D.

[REDACTED]

[REDACTED]

---

[REDACTED]

[REDACTED]

requires [REDACTED] to access and analyze [REDACTED] and (2) whether under 18 U.S.C. § 2703(c)(2) of ECPA, and 21 U.S.C. § 876(a), the DEA could use an administrative subpoena to obtain general information about the location of the Hemisphere [REDACTED] serving a target's cell phone, in addition to conventional call metadata.

As we noted above, Hemisphere is not a DEA program. However, the DEA is a major user and has invoked its administrative subpoena authority to obtain products from the exploitation of [REDACTED] bulk collection. The DEA had the obligation to ensure that its use of this authority was lawful and appropriate.

We found no evidence of any written legal analysis of the legal issues described above or of any other expected DEA use of Hemisphere in advance of the program. Indeed, it was not until January 2013, more than 5 years after the program began, that the DEA completed a robust written legal assessment, albeit in a draft memorandum that [REDACTED] never memorialized into a final product or distributed to users.<sup>136</sup> We believe that several earlier events should have alerted the DEA to the need for a careful legal review.

First, in August 2007, shortly after Hemisphere's trial phase ended, OCC received a field inquiry on the propriety of the DEA's participation in Hemisphere through the use of its administrative subpoena authority. In response, OCC only noted that obtaining general location information for cell phones by an administrative subpoena might not be consistent with Section 2703(c)(2)(C) of ECPA (authorizing the carrier to disclose local and long distance connection records in response to administrative subpoenas), and requested more information to analyze this issue. We found no evidence that the information was ever provided or that the analysis was ever completed.

Second, 1 year later in August 2008, the DEA issued the [REDACTED] Memorandum that prohibited the DEA's use of a single administrative subpoena to obtain telephone metadata beyond the target's direct calls [REDACTED] from target number, as would occur in the course of creating an [REDACTED] as described in Chapter Five), but permitted the DEA to use a single administrative subpoena to obtain a [REDACTED] which required accessing and analyzing such records.<sup>137</sup> However, the [REDACTED]

---

<sup>137</sup> We found that prior to the [REDACTED] Memorandum the DEA had not contemplated issuing a formal policy until senior DEA managers received reports that the program's purported practice of subpoena "recycling"—[REDACTED] upon request without a new administrative subpoena(s)—could cause "major problems" for DEA's administrative subpoena authority generally if the DEA did not issue guidance soon. We believe that such issues could have been addressed much earlier had the DEA performed adequate analysis and set policy limits

Memorandum did not contain any legal analysis that explained the basis for those policy decisions. Nor did the [REDACTED] Memorandum address the permissibility of obtaining general location information in Hemisphere responses to DEA administrative subpoenas. Additionally, while we did not find evidence of DEA seeking to obtain telephone metadata beyond a target's direct calls after the [REDACTED] Memorandum, we found that the [REDACTED] Memorandum was unknown to many DEA personnel that have (or had) significant involvement with the Hemisphere program. It is also not on the DEA's intranet or otherwise widely available, even though it provides other important guidelines for the DEA's collection and use of Hemisphere data. It is axiomatic that a policy cannot have meaning or effect if it is not widely known or accessible to those for whom it was designed to provide guidance, especially given turnover of DEA personnel and the loss of their institutional knowledge over time.

Third, 2 years thereafter in August 2010, the FBI raised legal concerns to the Criminal Division about Hemisphere products, including concerns about products containing [REDACTED] and general location information in response to administrative subpoenas. The Criminal Division's preliminary assessment then was that the former was legally permissible with some policy constraints, but the latter was not recommended. The DEA continued to rely on its previous guidance in the [REDACTED] Memorandum without any new written assessments and continued to obtain both [REDACTED] and general location information in Hemisphere products.<sup>138</sup>

We believe that the January 2013 OCC draft memorandum adequately addressed (albeit not in a finalized policy document) the first question about whether the DEA could obtain a [REDACTED] from [REDACTED] with a single administrative subpoena. The memorandum addressed the DEA's authority under both 21 U.S.C. § 876(a) and 18 U.S.C. § 2703(c)(2) of ECPA. It is, again, beyond the scope of the OIG's review to opine on whether the 2013 OCC analysis was legally correct. We found only that the relevant legal issues were sufficiently considered and assessed.

On the second issue, relating to the propriety of obtaining general location information for cell phones by administrative subpoena, we identified several

---

before initiating widespread use of the program, or done a more rigorous review following the field inquiry to OCC in August 2007.

<sup>138</sup> In contrast, the FBI subsequently prohibited its personnel from obtaining both in policy issued in March 2011. The FBI's policy contained no discussion on the underlying rationale for the prohibitions. Other FBI documents and testimony, however, showed that the FBI elected not to obtain general location data for cell phones from Hemisphere [REDACTED] due to the Criminal Division's recommendation, and not to permit requests for [REDACTED] or [REDACTED] records because it did not want to be associated with such requests even if [REDACTED] were not provided in response to administrative subpoena requests for [REDACTED]. The FBI's DIOG also expressly prohibits FBI personnel from obtaining records of [REDACTED] or [REDACTED] (the rider language for Hemisphere [REDACTED] with a single administrative subpoena. See Section 18.6.4.3.3.2.3 of the DIOG.



potentially relevant authorities that the January 2013 OCC draft memorandum did not address. First, it failed to specifically address Section 6632.1 of the DEA Agents Manual, which requires the DEA to seek a court order under Section 2703(d) of ECPA to obtain “any information” beyond the narrow list of non-content information available by subpoena in Section 2703(c)(2)(A)-(F) of ECPA.<sup>139</sup> Instead, it defended the practice of obtaining Hemisphere’s general location information (country, state, or city) based on the argument that such location records do not “pertain to” a subscriber or customer, but rather are used by [REDACTED] only for the purpose of billing other carriers for using its network, and thus fall outside the protection of ECPA.<sup>140</sup> Second, it failed to address an OLC opinion that imposed similar limits to those specified in Section 6632.1 of the Manual for the FBI’s use of National Security Letters under the Section 2709(b)(1) of ECPA, 18 U.S.C. § 2709(b)(1), to obtain virtually identical non-content telephone information.<sup>141</sup> The OLC opinion determined that the specific information listed in Section 2709(b)(1) of ECPA is exhaustive and not illustrative, notwithstanding the FBI’s arguments that it could seek any information kept by the service provider for its own business purposes that relates to similar information listed in Section 2709(b)(1).<sup>142</sup> Third, it failed to address the Criminal Division’s recommendation to the DEA in 2010 against receiving Hemisphere’s general location information from [REDACTED] because the Criminal Division had not previously interpreted Section 2703(c)(2) of ECPA to permit obtaining location-type information by administrative subpoena.<sup>143</sup> Thus, we found that the January 2013 OCC draft memorandum did not sufficiently address the second issue.

---

<sup>139</sup> The 2013 memorandum recognized that location data typically is only available by court order, but failed to reference or address the mandatory constraints imposed by Section 6632.1 of the Manual. The DEA commented that the point of the January 2013 OCC Memorandum was to pose an alternative legal theory that Hemisphere’s switch location information was a business record that could be obtained outside the constraints of ECPA if Section 876(a)’s relevance requirements were met.

<sup>140</sup> OCC’s analysis did not address or reconcile court rulings that have reached opposite conclusions for other business-related location data derived from a carrier’s network equipment. See, e.g., *United States v. Graham*, 824 F.3d 421, 425-428 (4th Cir. 2016) (en banc) (describing historical cell site location information as business records that identify the cell tower equipment needed to route calls and text messages across a carrier’s network, including whether roaming charges apply, which are nonetheless protected by ECPA).

<sup>141</sup> *Requests for Information under the Electronic Communications Privacy Act*, 32 Op. O.L.C. 145-149 (Nov. 5, 2008), <https://www.justice.gov/sites/default/files/olc/opinions/attachments/2015/06/23/op-olc-v032-p0145.pdf> (accessed Dec. 9, 2016) (concluding that the FBI’s use of National Security Letters to obtain telecommunication transactional records was limited to the information—name, address, length of service, and local and long distance toll billing records—expressly listed in Section 2709(b)(1)).

<sup>142</sup> See 32 Op. O.L.C. at 146-49, 156 (reaching a conclusion consistent with Section 6632.1 of Manual for similar ECPA exception and noting later that National Security Letters are similar to administrative subpoenas in function).

<sup>143</sup> OCC did not accord the Criminal Division’s recommendation any weight because it was made without any accompanying legal analysis. The DEA commented that it was therefore

As discussed above, the January 2013 OCC draft memorandum was never finalized or disseminated broadly. After reviewing a draft of this report, the DEA stated that the purpose of the January 2013 OCC draft memorandum was to ensure that its usage of Hemisphere was legally defensible. We do not believe this step goes far enough. Rather, we believe that OCC, in consultation with the Department, should issue a final legal opinion and updated, controlling policy to authoritatively analyze and document that its use of the Hemisphere program is consistent with applicable statutes, and to provide formal guidance to DEA personnel on these matters.

## **E. Recommendations Regarding Legal Review**

### **1. Bulk Collections by Administrative Subpoena**

Although the [REDACTED] and [REDACTED] bulk collection programs no longer exist, there is nothing preventing the DEA or the Department from seeking to start such a program at any time in the future. In order to ensure that any future "bulk collection" program utilizing the DEA's administrative subpoena authority is grounded in clear written legal guidance sufficient to ensure that Department personnel act consistently with applicable laws and to provide meaningful standards for effective oversight, we make the following recommendation to the Office of the Deputy Attorney General and the DEA:

**Recommendation 1: Establish a policy or directive sufficient to ensure that, if the DEA or the Department considers reinstating a version of [REDACTED] or [REDACTED], or initiating another "bulk collection" program by use of administrative subpoenas, the DEA, in consultation with relevant DOJ components (e.g., the Criminal Division and the OLC), conducts a rigorous, objective legal analysis, memorialized in writing, in advance of reinstating or initiating such "bulk collection" program by use of administrative subpoenas. The policy or directive should ensure that any such legal analysis specifically addresses whether 21 U.S.C. § 876(a) authorizes the issuance of subpoenas of the type contemplated (i.e., non-targeted, for exploratory or target-development purposes), as well as the permissible conditions under which such bulk data collected by non-targeted administrative subpoenas may be shared with other federal agencies for non-drug purposes.**

---

unclear as to what factual information and circumstances were relevant to the Criminal Division's general recommendation against receiving location information through Hemisphere requests. While that is true, the DEA could have requested clarification at the time, but there is no evidence that it did. In any event, the Criminal Division has specific expertise in ECPA, which we believe warrants considering their view on whether obtaining the location information contained in Hemisphere responses to DEA administrative subpoenas is legally permissible under ECPA, and not merely whether a legal argument could be raised to defend the practice.



## **2. Legal Issues Relating to Hemisphere**

In order to resolve the outstanding legal issues relating to the Hemisphere program, we make the following recommendation:

**Recommendation 2:** The DEA, in consultation with the Department, should issue a final legal opinion and updated policy on the Hemisphere program and its permissible uses, including addressing the following issues:

(1) whether it is legally permissible under 21 U.S.C. § 876(a) and ECPA, 18 U.S.C. § 2703(c)(2), for the DEA to use a single administrative subpoena to request that the relevant provider access and analyze

[REDACTED] and

(2) whether it is legally permissible under ECPA, 18 U.S.C. § 2703(c)(2), for the DEA to obtain location information for cell phones by administrative subpoena.

## **II. OIG Assessment of Procedural Safeguards**

In this section we assess the procedural safeguards that the DEA currently employs to ensure compliance with the “relevance” requirement of Section 876(a), to prevent the misuse of bulk collections, and to ensure that the DEA administrative subpoenas are only issued in connection with Title 21 investigations, among other things.

### **A. Safeguards to Ensure Compliance with Section 876(a) and to Prevent Misuse of Collections**

#### **1. Relevance and RAS in [REDACTED]**

As detailed above, Section 876(a) requires that any information sought by an administrative subpoena be “relevant or material” to a Title 21 investigation.

[REDACTED]

[REDACTED]

144

[REDACTED]

145

[REDACTED]

---

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

147

2.

[REDACTED]

[REDACTED]

---

<sup>146</sup> The scope of this review did not include assessment of the DEA's approval process for issuance of conventional administrative subpoenas.

<sup>147</sup> We will assess the sufficiency of these changes as part of following up on the recommendations in this report.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED]

[REDACTED]





[REDACTED]

[REDACTED]

### **3. Recommendations Regarding [REDACTED] Procedures for Establishing Relevance under Section 876(a)**

Based on the foregoing analysis, we make the following recommendations regarding [REDACTED] procedures for the purpose of ensuring compliance with 21 U.S.C. § 876(a):<sup>152</sup>

[REDACTED]

---

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED]

B.

[REDACTED]

1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED]

[REDACTED]

2. [REDACTED]

[REDACTED]

[REDACTED]

**C. Safeguards Regarding Retention of [REDACTED] Bulk Data**

The DEA collected by administrative subpoena more than [REDACTED] of [REDACTED] to develop potential investigative leads between 2008 and 2013. However, the DEA did not have a standardized practice for management of this bulk purchase data information. Although the DEA envisioned developing targeted investigative packages from the [REDACTED] bulk data, in practice the DEA sent raw information directly to field divisions during

the majority of █████ operation (or until mid-2013) for the field division's discretionary use.<sup>155</sup>

The DEA's protocols for management of the █████ bulk data were particularly deficient with respect to storage and retention. We found that the DEA failed to establish any policies on storage or retention of the █████ bulk data at any time before or during the operation of █████. Indeed, FO had not even contemplated a retention schedule for the █████ bulk data until the OIG raised this issue.

Although █████ is not active, the DEA still retains the bulk collection of █████ data. Besides the original subpoena returns on CDs, the DEA has no retention and disposition policy in place for the information regarding tens of thousands of purchases uploaded to servers in DARTS, elsewhere in the DEA, or the Fusion Center.<sup>156</sup> Nor has it purged any of this information since the initiation of █████ in 2008.

Under DEA policy, data uploaded to DARTS, including the █████ bulk data, is currently retained indefinitely. In addition, data that the DEA obtained under a "general file" can be held 25 years after the cutoff date (which is 6 years after the last activity or correspondence). Therefore, under current DEA policy and practice, all non-case specific █████ data stored by the DEA that was never connected to a specific investigation can likely be retained for at least 25 more years.

We believe that such long-term or indefinite retention in government electronic systems raises significant privacy issues given that the vast majority of █████ purchasers whose information was collected were never shown to be connected to illicit drug-related activities. In particular, FO's spreadsheet of cumulative results for █████ for fiscal years 2008 through 2014 showed only 131 arrests from the tens of thousands of records of individual █████ purchases.<sup>157</sup> We are therefore troubled that the DEA would be

---

<sup>155</sup> Before providing raw data to the field, FO failed to establish protocols to systematically review the incoming █████ bulk data and ensure that it was within the scope of the █████ subpoenas █████. The first █████ Staff Coordinator erroneously assumed that the companies would not provide non-responsive data, and the second █████ Staff Coordinator only screened the bulk data to remove what he considered to be "dead-end" leads █████ from the information sent to the field. However, as shown by an FO Program Analyst's periodic removal of █████ on her own initiative between 2008 and 2010, the DEA failed to systematically guard against retention and dissemination of █████ as potential criminal leads.

<sup>156</sup> In June 2015, the DEA received approval from the National Archives and Records Administration to destroy the original subpoena returns on CDs (but not the other copies of the data in DEA files or systems) within 3 years after date of receipt.

<sup>157</sup> The DEA informed the OIG that the cumulative data in the spreadsheet contains combined results for █████ and another operational component unrelated to the use of administrative subpoenas, which cannot be separately reported. Accordingly, the figure of 131 arrests likely overstates the results of █████, even if there also was under-reporting due to FO's

able to retain purchaser information unconnected to illicit activity in government electronic systems for such a long duration.

By contrast with [REDACTED], as discussed in Chapter Three, the DEA had established a plan for the accumulated bulk data in the [REDACTED] program whereby the data was retained in a secure off-site facility, only limited individuals within DEA had direct access, and the data was purged every 2 years. We do not conclude that the same requirements necessarily should have been applied to the [REDACTED] bulk data, but rather that the DEA needs to put in place measures that are appropriate given the nature and scope of the information that it gathered through this program.

Accordingly, we recommend the following:

**Recommendation 8: The DEA should develop legally supportable criteria for retention of all [REDACTED] bulk data collected by use of administrative subpoenas, and policies for the disposition of such [REDACTED] bulk data.**

### **III. OIG Assessments and Recommendations Regarding Audits**

#### **A. [REDACTED]**

[REDACTED]

[REDACTED]

[REDACTED]

---

failure to establish standardized procedures to report results on a set schedule. Moreover, the DEA's statistics failed to account for targets or investigations that were already active and would have been pursued irrespective of any leads regarding [REDACTED] purchase data.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**B.** [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ensuring that its HIDTA-affiliated customers remain satisfied with program services.

Third, Provider B has provided co-located analysts at the Hemisphere program offices, whom Provider B has described in promotional materials as “trained in telecommunications and law enforcement investigations” and “available as a resource for any telecom[munications] question.” However, these co-located analysts reported to off-site supervisors and were not overseen by personnel in their physical location. In fact, the Hemisphere program as a whole lacked a central oversight entity or program manager who monitored operations for potential misuse or other infractions.

In a prior review, we found that co-location of a provider’s analysts with FBI employees, without sufficient oversight and supervision, contributed to serious abuses—including the passing of provider information to the government without legal process.<sup>159</sup> In the past, Provider B offered to the DEA (and other HIDTA-affiliated customers) to “recycle” Hemisphere subpoenas by providing [REDACTED], and possibly more, to the DEA upon request, without a separate subpoena approved by DEA supervisors or personnel in the Hemisphere program offices. This practice would risk short-cutting the relevance determination required under Section 876(a). Although the DEA has prohibited this practice, and there may be good reasons to [REDACTED] Hemisphere program offices, both illustrate the potential risks arising from the [REDACTED]

In light of the above, we recommend:

**Recommendation 12: After all recommended legal assessments of Hemisphere are completed and memorialized in a final document, the DEA, with OCC assistance, should conduct periodic audits, on a set schedule, of its use of the Hemisphere program to ensure compliance with Section 876(a) and ECPA, and with DEA’s procedures and policies, including those updated as recommended in this report.**

---

<sup>159</sup> See U.S. Department of Justice Office of the Inspector General, *The Federal Bureau of Investigation’s Use of Exigent Letters and Other Informal Requests for Telephone Records*, January 2010. Indeed, in 2013, when the DEA contemplated [REDACTED], OCC notified Intelligence Division and SOD Chiefs about the potential “pitfalls” of such an arrangement by sending lengthy excerpts from the above OIG report. One of the excerpts that OCC included noted with special emphasis that, the “FBI leaders and managers also should have recognized early on . . . the necessity of establishing oversight mechanisms to ensure those [proper] procedures were followed.” The DEA never implemented the proposal to [REDACTED] and we concur with the “necessity of establishing oversight mechanisms” to ensure that proper procedures are observed and, to make sure this occurs where such co-location exists or has existed, recommend periodic DEA audits of the DEA’s use of the Hemisphere program.

We believe that the DEA's participation in programs like Hemisphere that are not government-run and yet provide access to unique law enforcement tools requires more vigorous oversight, not less, particularly when no other central oversight entity exists.

#### **IV. Parallel Construction**

In analyzing the use of "parallel construction" to protect the confidentiality of the bulk programs discussed in this report, we identified two issues that should not be conflated. The first is the question of whether it is permissible and appropriate to use parallel construction to generate evidence for use in court filings or other documents that otherwise might potentially reveal the program to the public. The second is whether parallel construction is being, or can permissibly be, used to prevent prosecutors from fully assessing their discovery and disclosure obligations in criminal cases under Rule 16 of the Federal Rules of Criminal Procedure or other authorities.<sup>160</sup> We believe that the first such use of parallel construction is a legitimate and appropriate means of protecting the confidentiality of programs like ██████████ and ██████████. However, we believe that the DEA (and other participating federal agencies) must take care to ensure that they comply with criminal discovery obligations, if any.

There is nothing inherently inappropriate about using parallel construction to re-create information originally derived from a confidential program like ██████████ or ██████████ for use as evidence in court filings, such as warrant applications, or even at trial. Agents are not required to disclose all evidence in their possession to support probable cause for a warrant, for example. Parallel construction is, in this regard, essentially just a process for obtaining the same evidence by other means. For example, in some cases, the communications links identified in ██████████ or ██████████ products can be "reconstructed" through a series of subpoenas to relevant carriers relying on the same factual predicate that was relied on to justify requesting a ██████████ or ██████████ product in the first instance. The conventional administrative subpoena return may then be submitted as evidence, without any violation of program requirements or substantive or procedural rights.

Evidence that has been reconstructed in this manner is obtained through alternative, but similar, legal process, and not inappropriate to use merely because the facts were previously known to the government by other legal means. This situation is essentially indistinguishable from the practice of using conventional investigative techniques to confirm a fact initially disclosed to a law enforcement agency in a confidential tip.

---

<sup>160</sup> Other authorities include Federal Rule of Criminal Procedure 26.2; 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*, 373 U.S. 83 (1963); and *Giglio v. United States*, 405 U.S. 150 (1972).

However, the question of what must be disclosed to a defendant in discovery or under questioning by defense counsel is a separate issue from what may permissibly be relied on affirmatively in a court pleading. Dealing with discovery questions calling for the disclosure of sensitive programs like ██████ is, in this sense, similar to difficult questions of discovery that may occur when an investigation was initiated or relies on classified or confidential information, such as an informant whose identity the government does not want to reveal.<sup>161</sup> The question of whether and what the government will be required to disclose in discovery in such cases is governed by the Rules of Criminal Procedure (in particular, Rule 16) and by a body of case law, which may be complex and dependent upon the particular facts and jurisdiction.<sup>162</sup>

As in these situations, parallel construction does not supersede the government's discovery obligations, if any. The DEA has represented that it does not use parallel construction to prevent prosecutors from fully assessing their discovery and disclosure obligations in criminal cases. It was beyond the scope of this review to attempt to confirm this assertion. Nevertheless, in any case in which a confidential sensitive program like ██████ or ██████ is used to develop evidence in an investigation, there is a possibility that the government will be asked to disclose the source of information used to assist in the development of its investigation. Discovery obligations may lead back to the program eventually, depending on how much disclosure a court requires. This possibility exists even if the government never relies on any information developed from the program at trial or in a court filing. If complying with a discovery obligation would cause irreparable harm to a sensitive program, the government's options include seeking a protective order in sealed pleadings (likely on an *ex parte* basis), dismissing the particular counts that rely on the sensitive information, or in the most extreme circumstance dismissing the entire case—not ignoring discovery obligations.

---

<sup>161</sup> Indeed, Department guidance regarding discovery obligations of federal prosecutors has noted that “[p]rosecutors must always be mindful of security issues that may arise with respect to disclosures from confidential sources files.” See David W. Ogden, Deputy Attorney General, memorandum for Department Prosecutors, Guidance for Prosecutors Regarding Criminal Discovery, January 4, 2010, at 5. Additionally, other Department guidance has noted that “litigating components should specifically state in their office-wide discovery policies that discovery in national security cases or cases involving classified information must account for special considerations that apply to those cases.” See Gary G. Grindler, Acting Deputy Attorney General, memorandum for the Associate Attorney General and the Assistant Attorneys General for the Criminal Division, National Security Division, Civil Rights Division, Antitrust Division, Environment and Natural Resources Division, Tax Division, and all United States Attorneys, Policy and Procedures Regarding Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations, September 29, 2010, at 2-3. As one example, this guidance observed that: “disclosure of *unclassified* information relating to a national security investigation may also pose a risk to national security if, for instance, the information reveals investigative steps taken, investigative techniques or tradecraft used, or the identities of the witnesses interviewed during a national security investigation.” Grindler, memorandum for the Associate Attorney General, *et al.*, at 2 (italics in original).

<sup>162</sup> See, e.g., Grindler, memorandum for the Associate Attorney General, *et al.*, at 3-4.

The DEA's training materials and other DEA documents provide that the main objective of the "parallel construction" process is to expeditiously provide actionable information to criminal investigators regarding existing investigative leads without unnecessarily risking disclosure of sensitive sources and methods. While they do not specifically address the issue, these materials do not instruct that parallel construction should be used to evade discovery. Rather, they focus on protecting disclosure of sensitive methods and tradecraft and state that the "ultimate sanction" for refusing to disclose the program is a motion to dismiss the case.

However, these materials also contain some troubling aspects. Most significantly, they expressly state that [REDACTED] investigative products cannot be shared with prosecutors.<sup>163</sup> The materials also expressly state that [REDACTED] investigative products may not be referenced in any potentially discoverable information.

The above guidance appears in tension with Department policy on a federal prosecutor's "duty to search" for discoverable information from all members of the "prosecution team," which typically includes federal law enforcement officers who participated in the investigation of the defendant.<sup>164</sup> In this regard, Department policy notes that prosecutors should review and be granted access to the substantive case file and non-investigative files, such as confidential source files, that may contain discoverable information related to the matter being prosecuted.<sup>165</sup> However, if the DEA (or any other participating federal agency) as a member of the "prosecutorial team," does not routinely disclose to a federal prosecutor the existence of a [REDACTED] investigative product that was subsequently parallel constructed, then the federal prosecutor who is ultimately responsible for compliance with discovery and disclosure obligations might not know of the existence of this information to assess if it is potentially discoverable, either initially or in response to questions that may arise during the course of litigation.

We recognize that these are difficult issues and, therefore, believe that the issue of parallel construction of evidence developed via [REDACTED] or [REDACTED] requires a comprehensive review by those DOJ components with expertise in this area, including the Office of the Deputy Attorney General (Associate Deputy Attorney General & National Criminal Discovery Coordinator), the Criminal Division, and the DEA.

In light of the above, we recommend:

---

<sup>163</sup> DEA guidance documents appear to suggest that the basis for this practice is because many prosecutors do not typically have security clearances to handle highly classified materials and some [REDACTED] investigative products might be so classified.

<sup>164</sup> Ogden, memorandum for Department Prosecutors, at 2, 4; Grindler, memorandum for the Associate Attorney General, *et al.*, at 3-8.

<sup>165</sup> Ogden, memorandum for Department Prosecutors, at 2, 4



**Recommendation 13:** The Office of the Deputy Attorney General should ensure that a comprehensive review is conducted of the DEA's "parallel construction" policies and practices with respect to [REDACTED] and [REDACTED] investigative products to ensure that these policies and practices do not conflict with the government's discovery and disclosure obligations in criminal cases, or Department policy on this subject.

**Recommendation 14:** In the interim, and subject to the results of the above review, the Department's and the DEA's guidance and training materials regarding "parallel construction," including SOD/[REDACTED] investigative products and [REDACTED] investigative products, should be clarified to clearly state that "parallel construction" does not negate adherence to discovery and disclosure obligations in criminal cases, if applicable. These guidance and training materials should further make explicit that, if discovery requirements threaten disclosure of the program, prosecutors may seek to protect the program through appropriate process, such as protective orders or *ex parte* proceedings, and that, depending on the circumstances, the government may eventually be required to choose between disclosure or dismissal, but that "parallel construction" cannot be utilized as a substantive substitute for otherwise applicable discovery and disclosure requirements.

## **V. General Updates to Policies and Training**

For the reasons discussed above, the OIG also makes the following additional recommendations with respect to updating policies and training:

**Recommendation 15:** The DEA should review and update its delegations to ensure that Section 876(a) authority has been properly delegated to the officials who are reviewing and signing [REDACTED] subpoenas.

**Recommendation 16:** The DEA should take steps to ensure that all changes to DEA policies, guidance, or procedures adopted as a result of implementing the foregoing recommendations are disseminated widely and readily available to DEA employees and other users of the programs, as appropriate, ([REDACTED] [REDACTED]). All such changes should be incorporated into the DEA Agents Manual and periodic training provided to users of the relevant programs and to SOD and NS personnel, as appropriate.

## **VI. Conclusion**

In this report, the OIG has described the DEA's use of its administrative subpoena authority under 21 U.S.C. § 876(a) to collect or exploit "bulk data" in the furtherance of narcotics investigations. We determined that the DEA has discontinued two programs that utilized this authority (██████ and ██████), but is utilizing an alternate approach under which bulk data collections are maintained and queried by private entities on behalf of the DEA and other agencies (██████ and ██████).

As detailed in this chapter, we found that the Department and DEA did not conduct an adequate review of the legal validity of the DEA's use of its administrative subpoena authority before initiating the ██████ program. We found a similar failure by the DEA before initiating the ██████ program, and that additional legal questions remain about its use of the ██████ program that require further legal assessment. Although the ██████ and ██████ bulk collection programs were discontinued, there is no formal restriction barring the DEA (or the Department) from initiating similar programs at any time in the future. Therefore, we recommended that, if the DEA or the Department considers initiating a "bulk collection" program by use of administrative subpoenas, the Department should conduct a rigorous, objective legal analysis, memorialized in writing, in advance of initiating such a program that specifically addresses whether 21 U.S.C. § 876(a) authorizes the issuance of subpoenas of the type contemplated (*i.e.*, non-targeted, for exploratory or target-development purposes), and addresses the permissible conditions under which such bulk data collected by non-targeted administrative subpoenas may be shared with other federal agencies for non-drug purposes.

Additionally, we found that the DEA has failed to develop a final disposition plan for the ██████ bulk data that resides on DEA or Fusion Center servers and recommended that the DEA develop policies for retention and disposition of all ██████ bulk data collected by use of administrative subpoenas.

We also found that the DEA's procedural safeguards and audit practices for the ██████ program are not sufficiently clear or strong to ensure compliance with the requirement under Section 876(a) that the information being demanded is relevant or material to a Title 21 investigation, and therefore made a total of eight recommendations to address these issues.

██  
██  
██

We also recommended that the Department undertake a comprehensive review of "parallel construction" policies and practices with respect to ██████ and ██████ investigative products to ensure that these policies and practices do not conflict with the government's discovery and disclosure obligations in criminal cases, or Department policy on this subject, and that the

Department's and DEA's guidance and training materials on this subject be clarified as warranted.

Finally, we recommended general updates to policies and training materials pertaining to the DEA's administrative subpoena authority.

In total, the OIG made 16 recommendations to the DEA for improving its programs and ensuring compliance with its obligations under Section 876(a) and criminal discovery requirements. We believe that compliance with these recommendations will assist DEA and the Department to utilize its significant authorities in this area appropriately and consistently with the law and the civil rights and civil liberties of those who are protected thereby.

## APPENDIX A

### TIMELINE OF KEY EVENTS

January 1992	The Attorney General approves the [REDACTED] Program, an interagency program involving the analysis of bulk telephone call records to combat drug trafficking. As part of [REDACTED], the DEA begins using administrative subpoenas to collect bulk telephone calling data for calls from the United States to a foreign country known to have a nexus to drug trafficking, or in some cases between those countries (the [REDACTED] collection). In subsequent years the number of countries vastly expands from the initial 1 country to many others.
June 1992	The DEA, FBI, Criminal Division, and Department of Defense enter into the first [REDACTED] Memorandum of Understanding (MOU). In subsequent years other DOJ or federal agency components sign MOUs and begin contributing law enforcement data to the [REDACTED] program and requesting [REDACTED] analytical products prepared by the DEA.
1993	First [REDACTED] subpoenas served on communications service providers.
August 1999	The DEA's Office of Chief Counsel (OCC) prepares a legal memorandum to "act as a counter" to legal concerns raised by the FBI's General Counsel regarding the legal validity of the [REDACTED] subpoenas (the first evidence of DEA legal analysis of the [REDACTED] collection). The August 1999 Memorandum does not discuss court decisions regarding the use of "exploratory" subpoenas lacking a connection to a specific authorized investigation.
2004-05	The DEA proposes the use of administrative subpoenas to [REDACTED] [REDACTED] DOJ Criminal Division attorneys question whether such subpoenas would be legally valid, and note that the proposed [REDACTED] subpoenas might place the [REDACTED] program in legal or legislative jeopardy, thereby undermining [REDACTED]. The DEA abandons the proposal [REDACTED]
March 2007	[REDACTED]

## APPENDIX A

June 2008 The DEA commences the [REDACTED], under which the DEA uses its administrative subpoena authority to collect bulk data regarding purchases of [REDACTED] in order to develop targets for investigations.

August 2008 [REDACTED]

September 2008 In response to an email from the DEA's Chicago Division Counsel requesting a legal review of an [REDACTED] subpoena, an attorney in OCC states that she sees "no legal objection."

August 2010 [REDACTED]

March 2011 [REDACTED]

January 2013 [REDACTED]

June 2013 Edward J. Snowden makes disclosures indicating that the National Security Agency has collected billions of telephone call records under Section 215 of the Foreign Intelligence Surveillance Act, encompassing every call made through the systems of certain telecommunications service providers where at least one end of the communication was located in the United States.

## APPENDIX A

June 2013	After the FBI's Office of General Counsel notes that FBI policy requires there to be a specific predicated investigation to issue an administrative subpoena, the FBI declines to participate in [REDACTED] at the Fusion Center.
July 2013	The DEA's OCC conducts another legal review of [REDACTED] in preparation for an upcoming meeting with the OIG, and finds prior Criminal Division analysis on [REDACTED] directly on point in assessing the issue.
August 2013	The Office of the Deputy Attorney General (ODAG) directs the DEA to suspend the [REDACTED] collection and conduct a reassessment, based on public concerns arising from the Snowden leaks and concerns about whether using subpoenas to amass the [REDACTED] bulk collection is within the authority granted to the DEA under 21 U.S.C. § 876(a).
September 2013	The DEA ceases issuing [REDACTED] subpoenas.
September 2013	The DEA completes its reassessment of the [REDACTED] collection and requests that the Attorney General and the Deputy Attorney General authorize reinstatement of the [REDACTED] collection, attaching a legal analysis that again does not discuss court decisions casting doubt on the validity of the proposed use of the DEA's subpoena authority.
January 2014	ODAG requests that the Office of Legal Counsel (OLC) review the DEA's legal assessment of the [REDACTED] collection.
January 2014	[REDACTED]
August 2014	The DEA modifies its automated system for requesting [REDACTED] products (including [REDACTED] data) to incorporate a drop-down list of generic categories of information sources to show "reasonable articula[ble]," also known as "RAS." In addition, the requester is instructed to describe the "significance" of the target number in a free-text "Remarks" box.



## APPENDIX A

August 2014	The DEA withdraws its request to reinstate █████, and OLC review of █████ ceases.
September 2014	The DEA prepares a draft guidance document for █████ that has served as the only written policy, protocol, or procedure for █████ to date. Among other things, the guidance states that █████ users must demonstrate that "specific reasonable articula[ble] suspicion exists that [the target numbers] are being used in the conduct of criminal activities."
July 2016	The DEA first begins audits of the █████ program (on a quarterly basis) including subpoena requests for █████ data.
Present	█████ and █████ remain operational. █████ and █████ are non-operational.



## APPENDIX B

U.S. Department of Justice

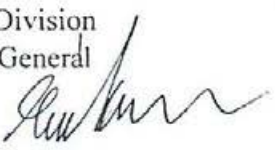
Office of the Deputy Attorney General

Associate Deputy Attorney General

Washington, D.C. 20530

### MEMORANDUM

**TO:** Michael S. O'Neill  
Assistant Inspector General  
Oversight and Review Division  
Office of the Inspector General

**FROM:** Bradley Weinsheimer   
Associate Deputy Attorney General  
Office of the Deputy Attorney General

**DATE:** March 22, 2019

**SUBJECT:** Response to OIG's Draft Report "A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas To Collect or Exploit Bulk Data"

The Office of the Deputy Attorney General (ODAG) appreciates the review undertaken by the Office of the Inspector General (OIG) and the opportunity to comment on the OIG's final draft report, "A Review of the Drug Enforcement Administration's (DEA) Use of Administrative Subpoenas To Collect or Exploit Bulk Data." Recommendations One, Thirteen, and Fourteen of the report are directed, in part, to ODAG. ODAG concurs with these recommendations and, working with the DEA, already has begun implementation of the recommendations.

In particular, while the Department and DEA have no plans to reinstate any of the discontinued bulk collection programs discussed in the OIG report, ODAG will ensure that the Department establishes a policy or directive sufficient to ensure that, if the DEA or the Department considers another bulk collection using administrative subpoenas, the DEA, in consultation with relevant DOJ components (e.g., the Criminal Division and the OLC), will conduct a rigorous, objective legal analysis, memorialized in writing, in advance of initiating such a program. ODAG also will ensure that a comprehensive review is conducted of the DEA's parallel construction policies and practices with respect to the programs covered in the OIG report to ensure that these policies and practices do not conflict with the government's criminal discovery obligations or Department policy on this subject. Finally, in the meantime, ODAG will work with the DEA to ensure its guidance and training materials regarding parallel construction, including investigative products relating to programs discussed in the OIG's report,

will be clarified to clearly state that parallel construction does not negate adherence to discovery obligations, where applicable.

ODAG and the DEA will provide to you a status update to report progress in meeting the recommendations contained in your report.



## APPENDIX C

### U. S. Department of Justice Drug Enforcement Administration


[www.dea.gov](http://www.dea.gov)

Washington, D.C. 20537

MAR 19 2019

#### MEMORANDUM

TO: Mr. M. Sean O'Neill  
Assistant Inspector General  
Oversight and Review Division  
Office of the Inspector General

FROM: Mary B. Schaefer   
Chief Compliance Officer  
Office of Compliance

SUBJECT: DEA Response to the OIG's Law Enforcement Sensitive Formal Draft Report:  
"Drug Enforcement Administration's Use of Administrative Subpoenas to Collect  
or Exploit Bulk Data"

The Drug Enforcement Administration (DEA) has reviewed the Law Enforcement Sensitive draft of the Department of Justice (DOJ) Office of the Inspector General's (OIG) Oversight and Review (O&R) Division report entitled, "*Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data.*"

DEA appreciates the OIG's assessment of the programs involved in the report and the opportunity to discuss improvements made over the years to those programs that DEA participates in, operates, or oversees. The OIG has identified sixteen recommendations in the report that are directed towards DOJ and DEA. DEA concurs with the OIG's recommendations for further improvement of its use of administrative subpoenas with respect to bulk data. Implementation is already underway; DEA will provide the OIG with a memorandum detailing its efforts under separate cover.

Thank you for the opportunity to review the OIG's report. We look forward to working with you and your staff to improve our processes.

If there are any questions regarding this response, please contact the DEA's Audit Liaison Section on 202-307-8200.





The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at [oig.justice.gov/hotline](https://oig.justice.gov/hotline) or (800) 869-4499.

**U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL**

950 Pennsylvania Avenue, Northwest  
Suite 4760  
Washington, DC 20530-0001

<b>Website</b>	<b>Twitter</b>	<b>YouTube</b>
<a href="https://oig.justice.gov">oig.justice.gov</a>	@JusticeOIG	JusticeOIG

Also at [Oversight.gov](https://Oversight.gov)