CLEAR is an online investigative platform used by ERO personnel to work more efficiently and effectively to:

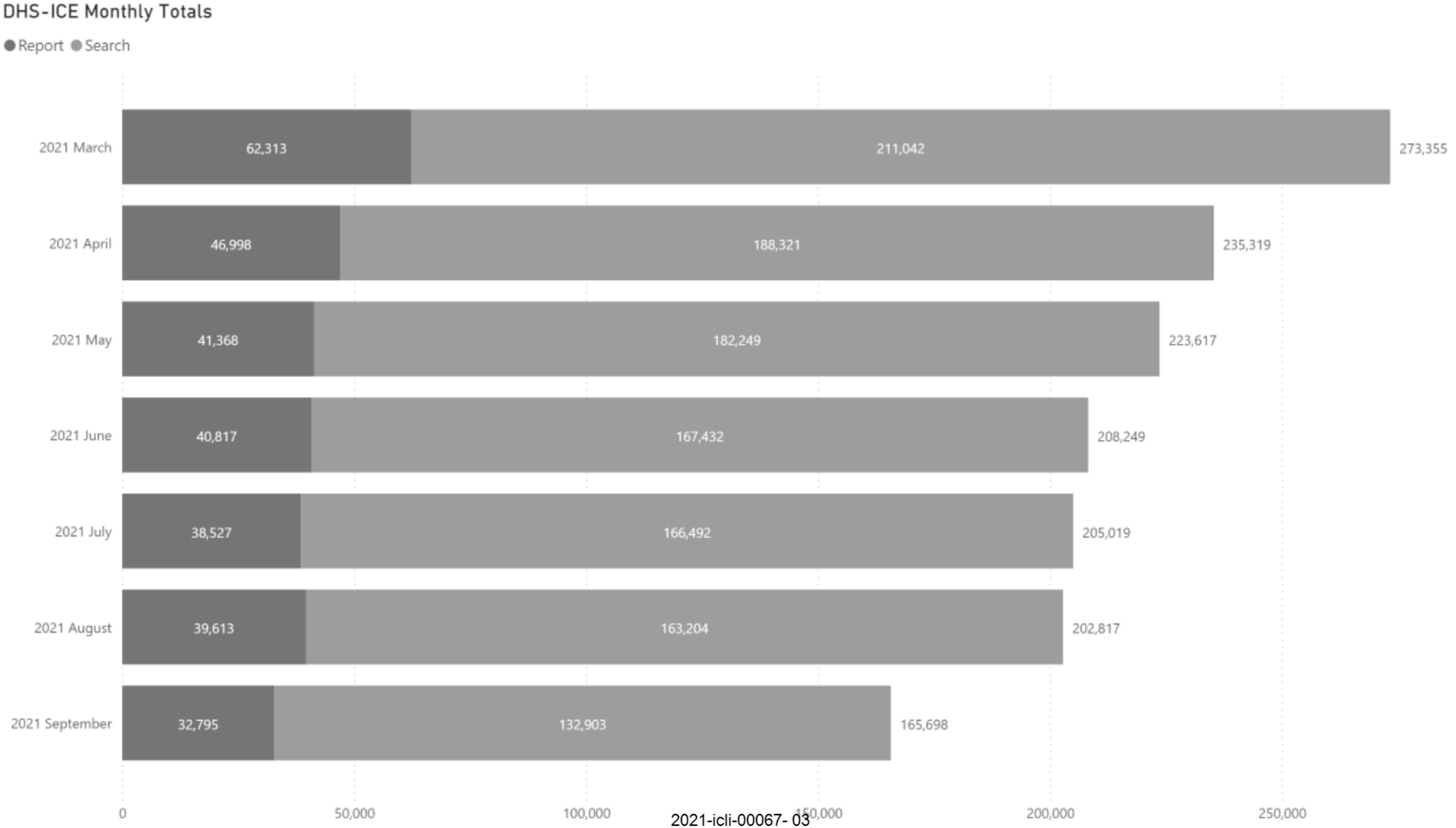
- Locate people, assets, businesses, affiliations, and other crucial facts;
- Make connections among individuals, incidents, activities, and locations; and
- Visualize, detect, and analyze patterns and trends in offenses and offenders.

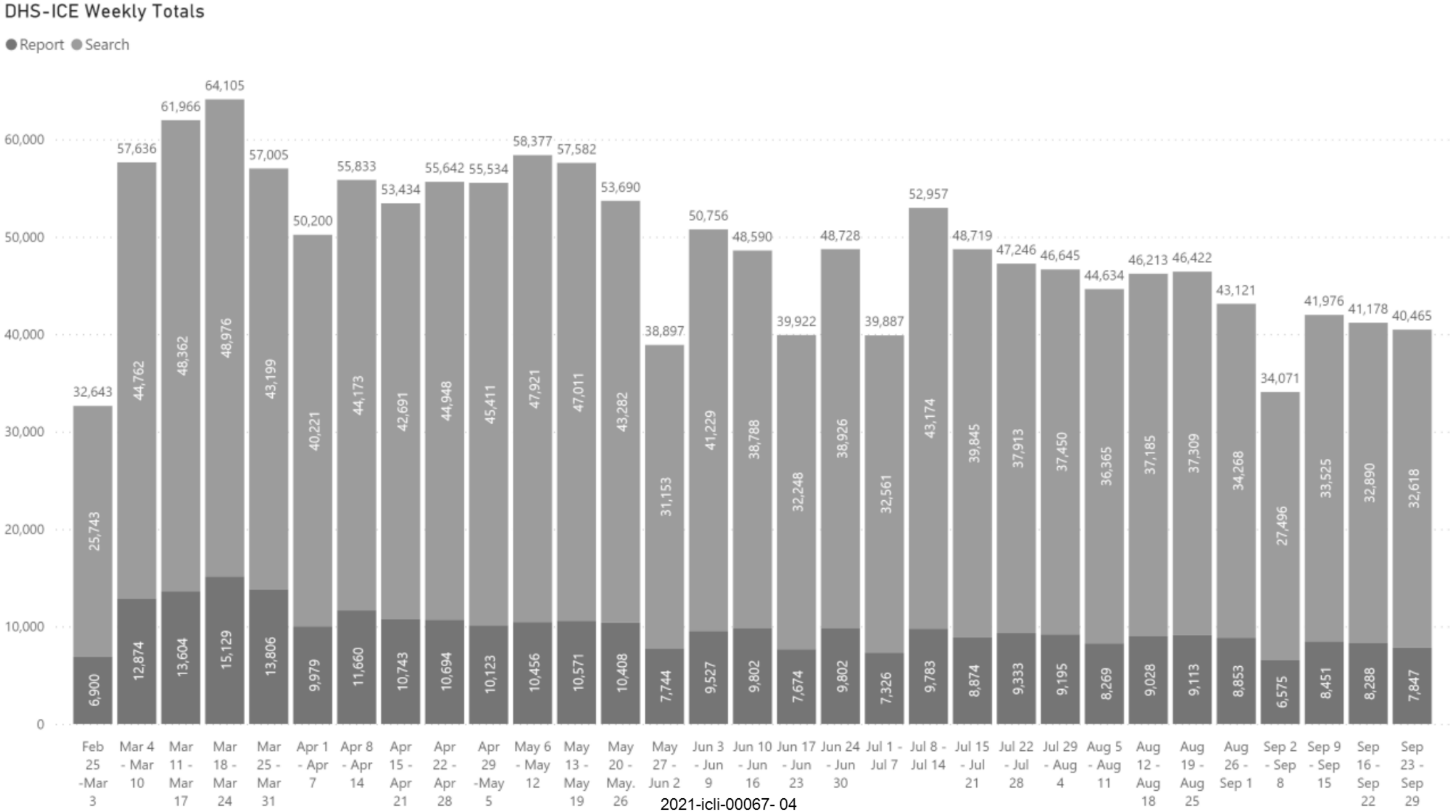
In addition, the CLEAR platform enables users to access **JusticeXchange**, an integrated justice solution, which provides an instant, up-to-date database of booking records, persons of interest, and other data from thousands of agencies across the country.

DHS-ICE AVCC USAGE
September 2021
Data through 30 Sept 2021

Last data refresh:

9/30/2021 4:57:04 PM UTC


DHS-ICE Monthly Totals
Report
Search
2021 March
62,313
211,042
273,355
2021 April
46,998
188,321
235,319
2021 May
41,368
182,249
223,617
2021 June
40,817
167,432
208,249
2021 July
38,527
166,492
205,019
2021 August
39,613
163,204
202,817
2021 September
32,795
132,903
165,698
0
50,000
100,000
150,000
200,000
250,000


DHS-ICE Weekly Totals
Report
Search
60,000
50,000
40,000
30,000
20,000
10,000
0
32,643
57,636
61,966
64,105
57,005
50,200
55,833
53,434
55,642
55,534
58,377
57,582
53,690
38,897
50,756
48,590
39,922
48,728
39,887
52,957
48,719
47,246
46,645
44,634
46,213
46,422
43,121
34,071
41,976
41,178
40,465
25,743
44,762
48,362
48,976
43,199
40,221
44,173
42,691
44,948
45,411
47,921
47,011
43,282
31,153
41,229
38,788
32,248
38,926
32,561
43,174
39,845
37,913
37,450
36,365
37,185
37,309
34,268
27,496
33,525
32,890
32,618
6,900
12,874
13,604
15,129
13,806
9,979
11,660
10,743
10,694
10,123
10,456
10,571
10,408
7,744
9,527
9,802
7,674
9,802
7,326
9,783
8,874
9,333
9,195
8,269
9,028
9,113
8,853
6,575
8,451
8,288
7,847
Feb 25 -Mar 3
Mar 4 - Mar 10
Mar 11 - Mar 17
Mar 18 - Mar 24
Mar 25 - Mar 31
Apr 1 - Apr 7
Apr 8 - Apr 14
Apr 15 - Apr 21
Apr 22 - Apr 28
Apr 29 -May 5
May 6 - May 12
May 13 - May 19
May 20 - May. 26
May 27 - Jun 2
Jun 3 - Jun 9
Jun 10 - Jun 16
Jun 17 - Jun 23
Jun 24 - Jun 30
Jul 1 - Jul 7
Jul 8 - Jul 14
Jul 15 - Jul 21
Jul 22 - Jul 28
Jul 29 - Aug 4
Aug 5 - Aug 11
Aug 12 - Aug 18
Aug 19 - Aug 25
Aug 26 - Sep 1
Sep 2 - Sep 8
Sep 9 - Sep 15
Sep 16 - Sep 22
Sep 23 - Sep 29

DHS-ICE-HSI

companyname	Search	Report	Total
DHS-ICE-HSI	373	43	416
DHS-ICE-HSI-HQ	18	11	29
DHS-ICE-HSI-HQ-GLOBAL TRADE INV	515	237	752
DHS-ICE-HSI-HQ-INTEL	15,971	4,368	20,339
DHS-ICE-HSI-HQ-INTL OPS	4,345	1,402	5,747
DHS-ICE-HSI-HQ-INTL OPS VSP	2,424	227	2,651
DHS-ICE-HSI-HQ-INV PRG INV SRVCS	629	198	827
DHS-ICE-HSI-HQ-INV PRG TOC I	6,111	666	6,777
DHS-ICE-HSI-HQ-INV PRG TOC II	557	136	693
DHS-ICE-HSI-HQ-NSID CTCEU	28,806	8,587	37,393
DHS-ICE-HSI-HQ-NSID NSP	1,919	792	2,711
DHS-ICE-HSI-HQ-OTCD C3	2,883	444	3,327
DHS-ICE-HSI-HQ-OTCD OSDM	10	1	11
DHS-ICE-HSI-SAC-Atlanta	10,740	2,848	13,588
DHS-ICE-HSI-SAC-Baltimore	12,461	3,934	16,395
DHS-ICE-HSI-SAC-Boston	18,371	4,686	23,057
DHS-ICE-HSI-SAC-Buffalo	8,170	1,617	9,787
DHS-ICE-HSI-SAC-Charlotte	10,922	3,703	14,625
DHS-ICE-HSI-SAC-Chicago	17,325	4,654	21,979
DHS-ICE-HSI-SAC-DALLAS	11,150	3,450	14,600
DHS-ICE-HSI-SAC-DALLAS DBA DEPARTMENT OF HOMELAND SECURITY	126	33	159
DHS-ICE-HSI-SAC-DENVER	8,245	2,869	11,114
DHS-ICE-HSI-SAC-DETROIT	18,203	5,017	23,220
DHS-ICE-HSI-SAC-DETROIT DBA DEPARTMENT OF HOMELAND SECURITY	331	44	375
DHS-ICE-HSI-SAC-El Paso	21,320	6,338	27,658
DHS-ICE-HSI-SAC-Honolulu	4,597	1,040	5,637
DHS-ICE-HSI-SAC-Houston	13,809	4,258	18,067
DHS-ICE-HSI-SAC-Kansas City	10,031	2,876	12,907
DHS-ICE-HSI-SAC-Las Vegas	3,381	1,020	4,401
Total	**500,000**	**132,095**	**632,095**

DHS-ICE-ERO

companyname	Search	Report	Total
DHS-ICE-ERO-FOD-Atlanta	8,639	1,422	10,061
DHS-ICE-ERO-FOD-Baltimore	2,193	352	2,545
DHS-ICE-ERO-FOD-Boston	3,532	780	4,312
DHS-ICE-ERO-FOD-Buffalo	2,585	418	3,003
DHS-ICE-ERO-FOD-Chicago	13,004	1,858	14,862
DHS-ICE-ERO-FOD-Dallas	4,266	1,051	5,317
DHS-ICE-ERO-FOD-Denver	8,271	967	9,238
DHS-ICE-ERO-FOD-Detroit	4,329	911	5,240
DHS-ICE-ERO-FOD-El Paso	6,704	1,481	8,185
DHS-ICE-ERO-FOD-Houston	3,895	567	4,462
DHS-ICE-ERO-FOD-Los Angeles	9,662	2,343	12,005
DHS-ICE-ERO-FOD-Miami	6,940	1,400	8,340
DHS-ICE-ERO-FOD-New Orleans	2,412	344	2,756
DHS-ICE-ERO-FOD-New York City	4,735	1,081	5,816
DHS-ICE-ERO-FOD-Newark	2,766	425	3,191
DHS-ICE-ERO-FOD-Philadelphia	4,069	581	4,650
DHS-ICE-ERO-FOD-Phoenix	4,904	937	5,841
DHS-ICE-ERO-FOD-Saint Paul	3,009	521	3,530
DHS-ICE-ERO-FOD-Salt Lake City	8,234	986	9,220
DHS-ICE-ERO-FOD-San Antonio	9,370	1,773	11,143
DHS-ICE-ERO-FOD-San Diego	16,527	2,173	18,700
DHS-ICE-ERO-FOD-San Francisco	7,984	1,495	9,479
DHS-ICE-ERO-FOD-Seattle	6,183	1,021	7,204
DHS-ICE-ERO-FOD-Washington DC	3,955	512	4,467
DHS-ICE-ERO-HQ-ERO	3,241	296	3,537
DHS-ICE-ERO-HQ-LESC	24,024	2,610	26,634
DHS-ICE-ERO-HQ-NCATC	45,785	10,682	56,467
DHS-ICE-ERO-HQ-PERC	544	146	690
Total	**221,762**	**39,133**	**260,895**

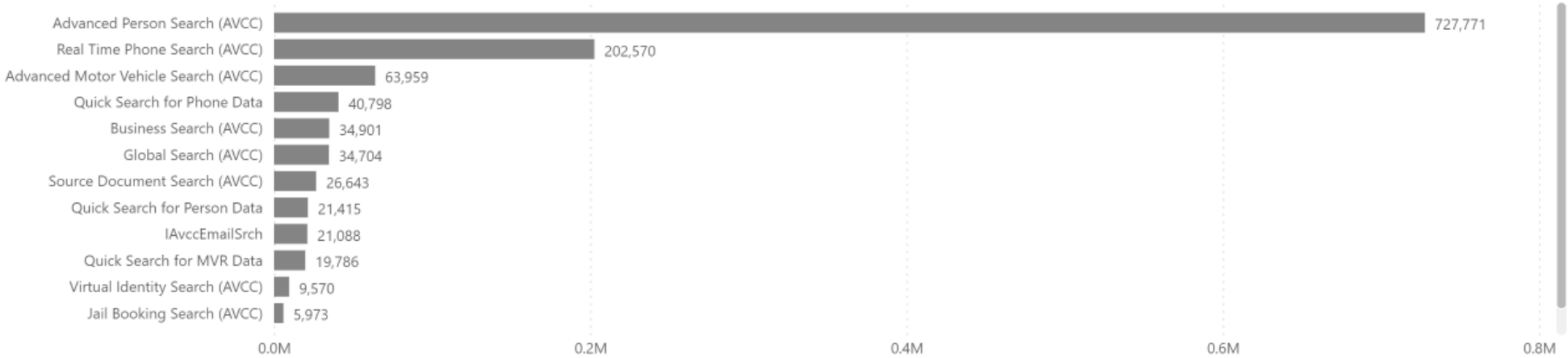
DHS-ICE-OPR

companyname	Search	Report	Total
DHS-ICE-OPR-HQ	1,224	383	1,607
Total	**1,224**	**383**	**1,607**

Total Searches and Reports

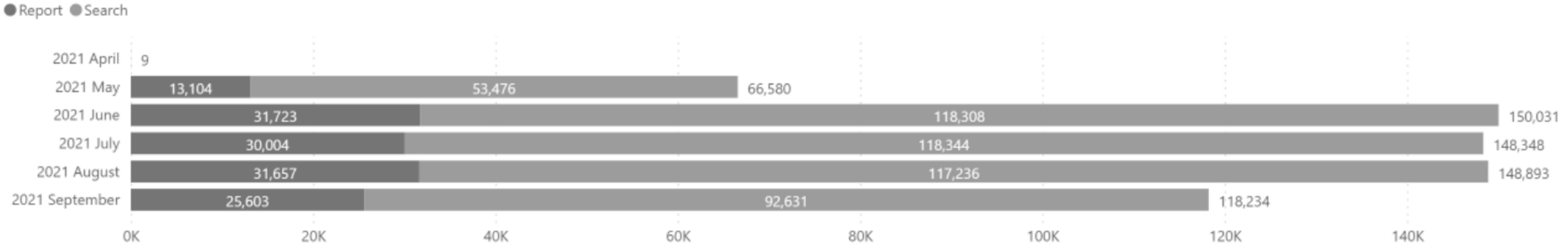
1,211,643	302,431
Searches	Report

Total Searches

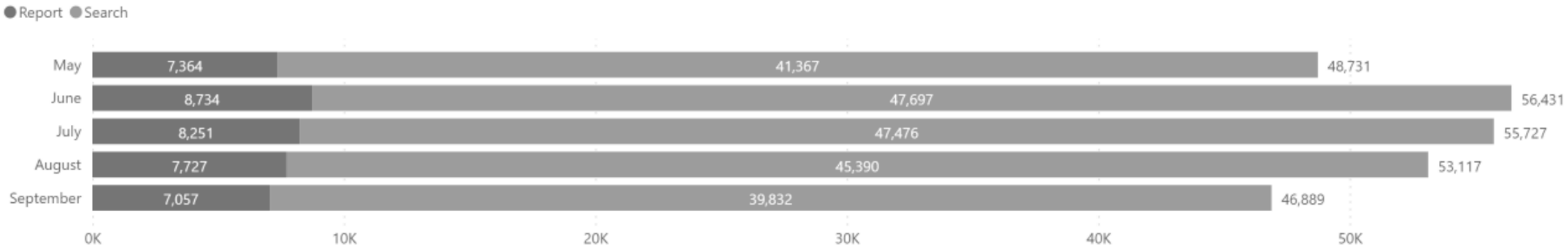


Total Reports

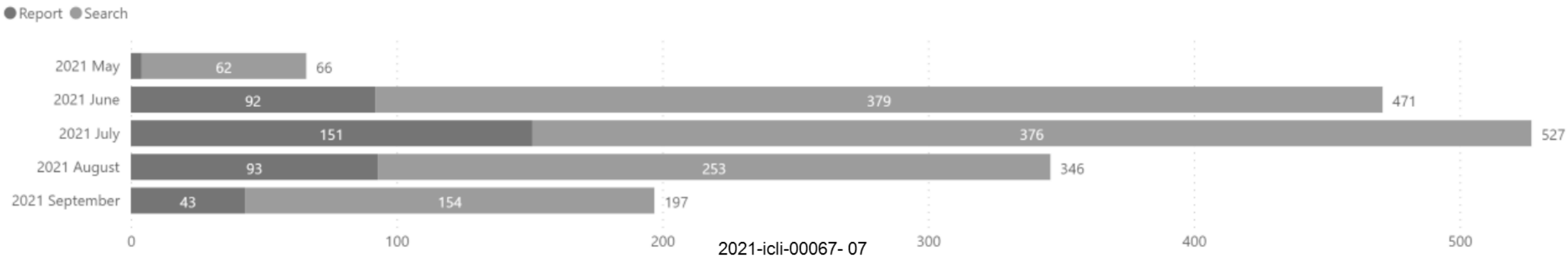
DHS-ICE-HSI Division

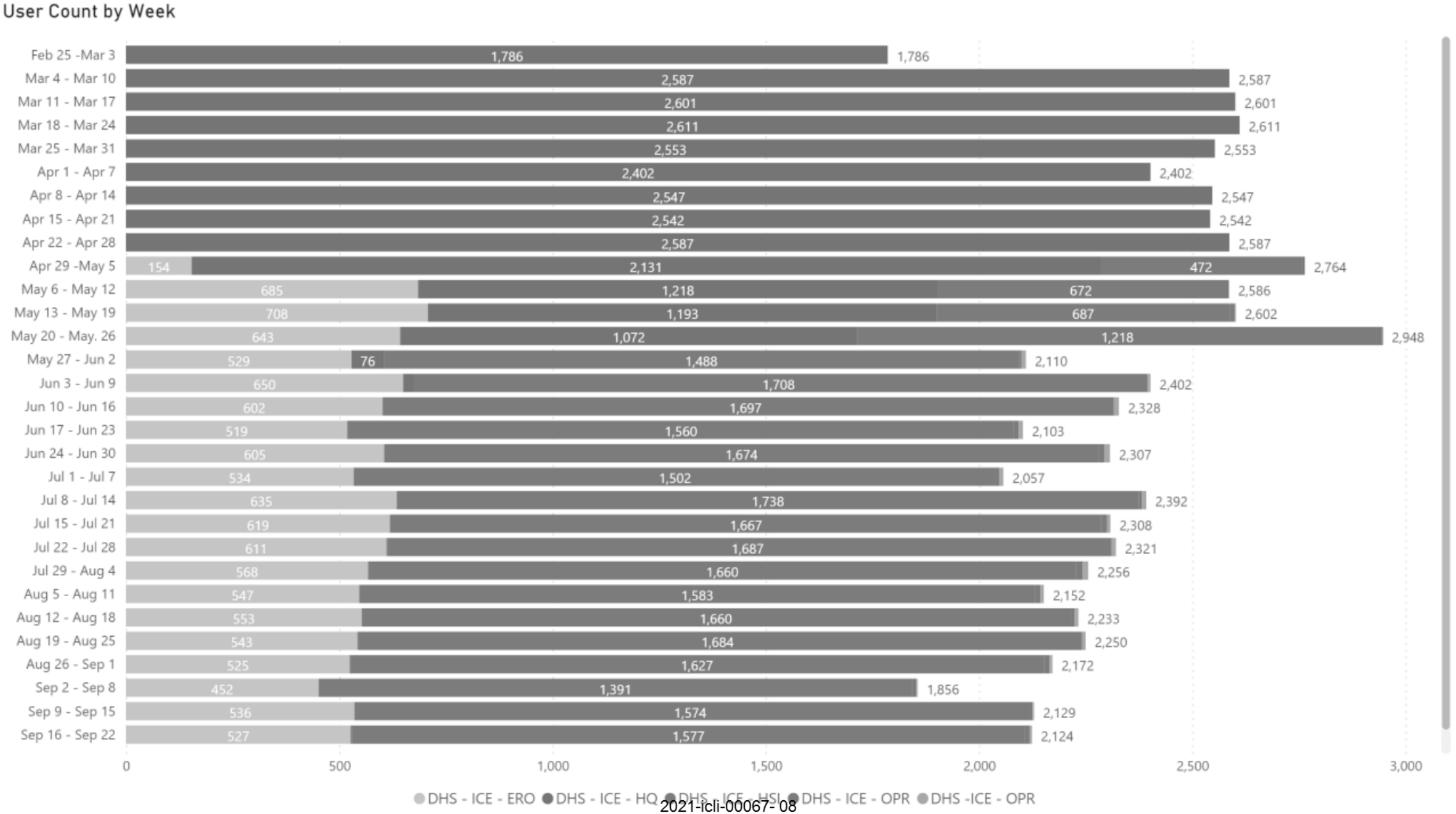


DHS-ICE-ERO Division



DHS-ICE-OPR Division




User Count by Week
Feb 25 -Mar 3
1,786
1,786
Mar 4 - Mar 10
2,587
2,587
Mar 11 - Mar 17
2,601
2,601
Mar 18 - Mar 24
2,611
2,611
Mar 25 - Mar 31
2,553
2,553
Apr 1 - Apr 7
2,402
2,402
Apr 8 - Apr 14
2,547
2,547
Apr 15 - Apr 21
2,542
2,542
Apr 22 - Apr 28
2,587
2,587
Apr 29 -May 5
154
2,131
472
2,764
May 6 - May 12
685
1,218
672
2,586
May 13 - May 19
708
1,193
687
2,602
May 20 - May. 26
643
1,072
1,218
2,948
May 27 - Jun 2
529
76
1,488
2,110
Jun 3 - Jun 9
650
1,708
2,402
Jun 10 - Jun 16
602
1,697
2,328
Jun 17 - Jun 23
519
1,560
2,103
Jun 24 - Jun 30
605
1,674
2,307
Jul 1 - Jul 7
534
1,502
2,057
Jul 8 - Jul 14
635
1,738
2,392
Jul 15 - Jul 21
619
1,667
2,308
Jul 22 - Jul 28
611
1,687
2,321
Jul 29 - Aug 4
568
1,660
2,256
Aug 5 - Aug 11
547
1,583
2,152
Aug 12 - Aug 18
553
1,660
2,233
Aug 19 - Aug 25
543
1,684
2,250
Aug 26 - Sep 1
525
1,627
2,172
Sep 2 - Sep 8
452
1,391
1,856
Sep 9 - Sep 15
536
1,574
2,129
Sep 16 - Sep 22
527
1,577
2,124
0
500
1,000
1,500
2,000
2,500
3,000
DHS - ICE - ERO
DHS - ICE - HQ
DHS - ICE - HSI
DHS - ICE - OPR
DHS -ICE - OPR

Overall Top 60 Users

loginid	lastname	firstname	Search	Report	Total
(b)(6); (b)(7)(C)			26,272	7	26,279
			4,141	753	4,894
			3,359	1,513	4,872
			4,182	178	4,360
			2,728	1,572	4,300
			3,023	1,123	4,146
			2,833	1,131	3,964
			3,944		3,944
			3,094	832	3,926
			3,682	92	3,774
			3,570	200	3,770
			2,622	1,121	3,743
			2,842	840	3,682
			2,231	1,328	3,559
			2,165	1,113	3,278
			2,600	666	3,266
			2,890	342	3,232
			2,603	540	3,143
			3,070	65	3,135
			2,089	1,034	3,123
			2,322	735	3,057
			2,348	663	3,011
			2,832	160	2,992
			2,920	48	2,968
			2,374	594	2,968
			2,776	88	2,864
			2,826	18	2,844
			2,485	353	2,838
			2,833	4	2,837
			1,768	1,043	2,811

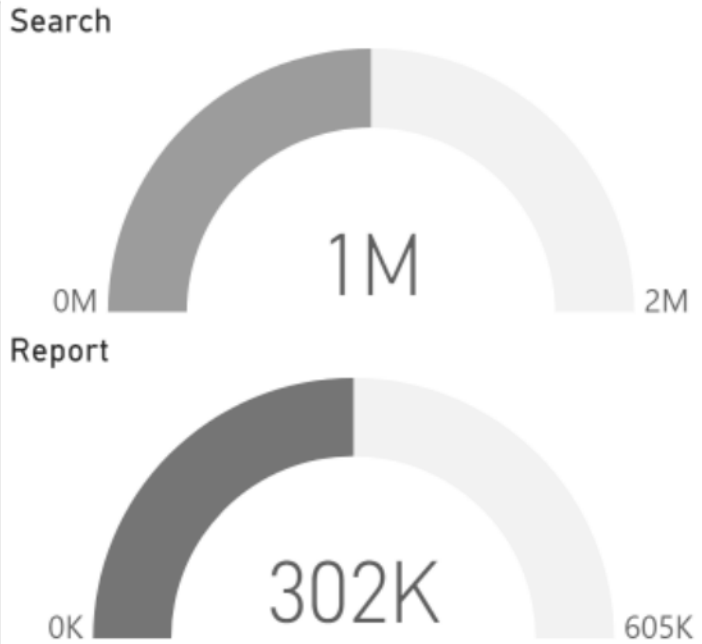
Previous 14 Days Top 60 Users

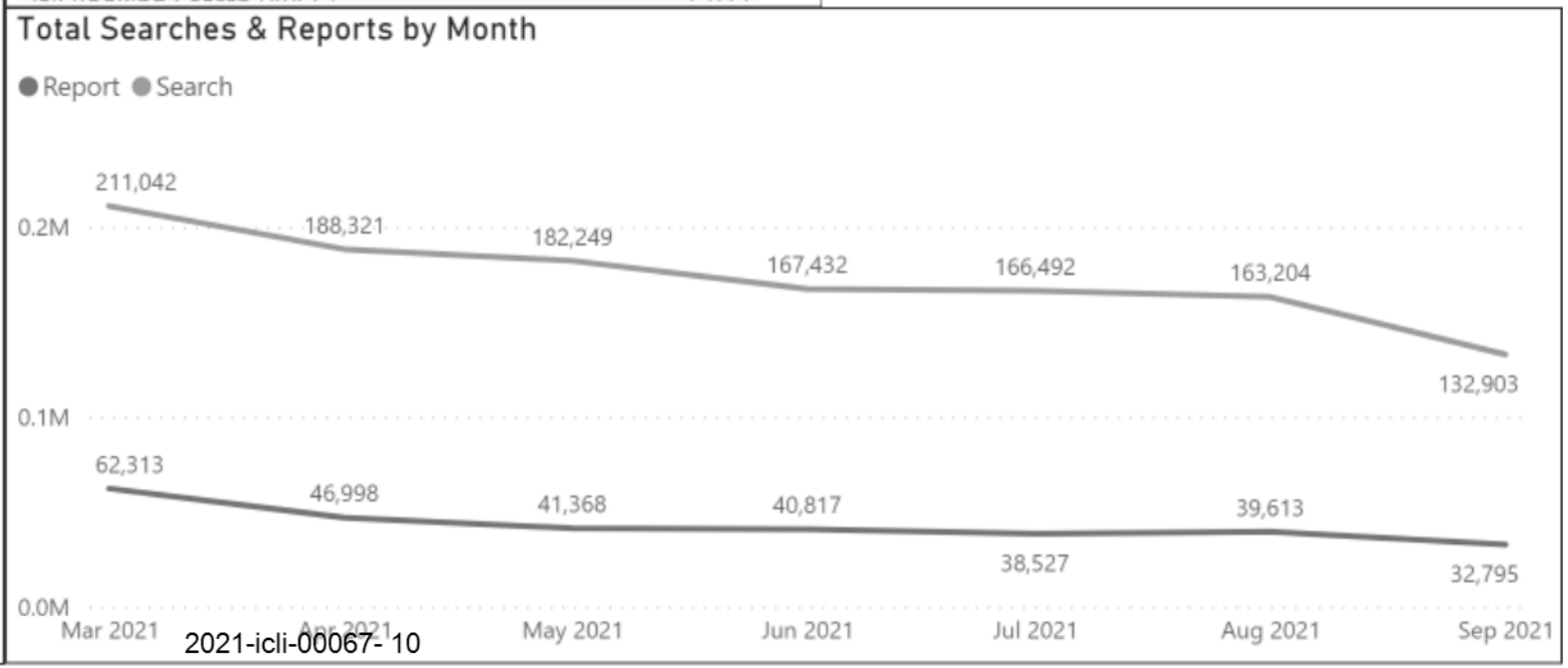
loginid	lastname	firstname	Search	Report	Total
(b)(6); (b)(7)(C)			130	8	138
			140	23	163
			122	32	154
			388		388
			92	30	122
			124	2	126
			178	18	196
			133	2	135
			134	1	135
			70	48	118
			76	43	119
			113	2	115
			167	1	168
			148		148
			212		212
			177	14	191
			95	38	133
			94	72	166
			150	39	189
			253	31	284
			157	2	159
			111	67	178
			144	80	224
			218	47	265
			221	15	236
			96	38	134
			122		122
			90	58	148
			206	66	272
			116	1	117

Overall Top 60 Users

loginid	lastname	firstname	Search	Report	Total
(b)(6); (b)(7)(C)			26,272	7	26,279
			4,141	753	4,894
			3,359	1,513	4,872
			4,182	178	4,360
			2,728	1,572	4,300
			3,023	1,123	4,146
			2,833	1,131	3,964
			3,944		3,944
			3,094	832	3,926
			3,682	92	3,774
			3,570	200	3,770
			2,622	1,121	3,743
			2,842	840	3,682
			2,231	1,328	3,559
			2,165	1,113	3,278
			2,600	666	3,266
			2,890	342	3,232
			2,603	540	3,143
			3,070	65	3,135
			2,089	1,034	3,123
			2,322	735	3,057
			2,348	663	3,011
			2,832	160	2,992
			2,920	48	2,968
			2,374	594	2,968
			2,776	88	2,864
			2,826	18	2,844
			2,485	353	2,838
			2,833	4	2,837
			1,768	1,043	2,811

Search/Report Description	Total Searches / Reports
Advanced Motor Vehicle Search (AVCC)	63,959
Advanced Person Search (AVCC)	727,771
AVCC Virtual Identity Report	21,085
Business Report (AVCC)	12,837
Business Search (AVCC)	34,901
Comprehensive Report - to Dashboard (AVCC)	8,644
Flat Rate Comprehensive Report (AVCC)	237,808
Global Search (AVCC)	34,704
IAvccBpsReportRR	1,382
IAvccEmailSrch	21,088
Jail Booking Report (AVCC)	919

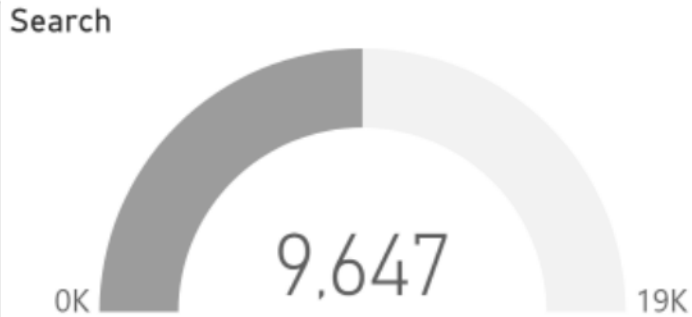




Previous 14 Days Top 60 Users

loginid	lastname	firstname	Search	Report	Total
(b)(6); (b)(7)(C)			406	82	488
			388		388
			368		368
			358		358
			329	14	343
			217	109	326
			323	1	324
			301	8	309
			184	100	284
			253	31	284
			206	66	272
			218	47	265
			218	25	243
			221	15	236
			169	55	224
			144	80	224
			153	66	219
			212		212
			131	66	197
			178	18	196
			162	33	195
			177	14	191
			150	40	190
			150	39	189
			111	67	178
			167	1	168
			94	72	166
			140	23	163
			151	11	162
			157	2	159

Search/Report Description	Total Searches / Reports
Advanced Motor Vehicle Search (AVCC)	268
Advanced Person Search (AVCC)	6,306
AVCC Virtual Identity Report	39
Business Report (AVCC)	36
Business Search (AVCC)	74
Comprehensive Report - to Dashboard (AVCC)	6
Flat Rate Comprehensive Report (AVCC)	1,728
Global Search (AVCC)	165
IAvccEmailSrch	39
Jail Booking Report (AVCC)	7
Jail Booking Search (AVCC)	70
MVR Wildcard Search (AVCC)	1
Quick Search for MVR Data	97
Quick Search for Person Data	101
Quick Search for Phone Data	227
Real Time Phone Detail Report (AVCC)	30
Real Time Phone Search (AVCC)	1,874
Source Document Search (AVCC)	410
Virtual Identity Search (AVCC)	15



From: ERO Assistant Directors
Sent: Mon, 1 Mar 2021 20:39:46 +0000
To: Undisclosed recipients:
Subject: Law Enforcement Investigative Database Subscription (LEIDS) Accurint Virtual Crime Center (AVCC) available on March 1, 2021
Attachments: LN AVCC ID for Sign-In.docx

Assistant Director for Enforcement

Enforcement and Removal Operations

U.S. Immigration and Customs Enforcement

To: All ERO Employees

ICE's Law Enforcement Investigative Database Subscription (LEIDS) contract was awarded to LexisNexis Risk Solutions. Effective March 1, 2021, all authorized users will transition from the Thomson Reuters Special Services (TRSS) Consolidated Lead evaluation and Reporting (CLEAR) database to the LexisNexis Accurint Virtual Crime Center (AVCC) database. The AVCC database provides access to public records and state and local record management systems (RMS) and computer-aided dispatch (CAD) data from over 1,500 agencies nationwide, all in one search. Users will also have mapping and link analysis capabilities to help locate non-obvious relationships between people, assets, and incidents.

In an effort to migrate all ICE authorized users seamlessly, it is anticipated that ICE users will be able to access AVCC via sign-in at (b)(7)(E) Information with their assigned username and password will be sent by LexisNexis to the user's ICE email address. Password will be sent in a separate email. Prior to logging in to the system, the user must concur with the agency's permissible uses of the system and affirmatively consent to these rules before proceeding further.

In the event that an automatic registration email is not received, and users need to register for access, please contact your local LEIDS database administrator for registration instructions.

With the migration from the incumbent platform (TRSS CLEAR), users will no longer be able to access the Vigilant Solutions - Law Enforcement Archival Reporting Network (LEARN) License Plate Reader (LPR) through CLEAR. Users may log into their current LPR accounts directly through the LEARN website at (b)(7)(E)

Potential Questions:

Q: What is Accurint Virtual Crime Center (AVCC)?
A: Access to Lexis Nexis AVCC will provide users with the information required to assist in investigations. Users will be able to access public records and state & local RMS and CAD data from over 1,500 agencies nationwide, all in one search.

Q: How do I login?
A: Users must log into Accurint via (b)(7)(E)

Q: What's my user id and password?
A: Users should have a seamless transition. Sign-in at Accurint.com with your username and password. The username and password will be provided to users via registration emails from LexisNexis to your assigned ICE email address. The password will be sent in a separate email.

Q: How do I use the platform?
A: Attached you will find the "Welcome to Accurint Virtual Crime Center (Part 1: ID for Sign-In)" quick instruction guide. Please review the training resources provided in 4 easy steps: (1) Video: a quick-start video to walk you through your first sign in. (2) Live Training via webinars, (3) Getting Started Guide: download getting started guide for basic information on searching and reports and (4) On-demand training: for more in-depth training, a series of courses available via LexisNexis University Public Safety Academy.

If you have any questions about Accurint Virtual Crime Center, please contact customer support at (b)(7)(E)
(b)(6); (b)(7)(C)
.

(b)(6); (b)(7)(C)
Assistant Director
Enforcement
Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement

This message was sent in concurrence with AD Field Operations.

This message expires one year from the date it was sent, pursuant to ERO policy.

Serving with Integrity.
Integrity • **C**ourage • **E**xcellence

U.S. Immigration and Customs Enforcement

Subject: Welcome to Accurint Virtual Crime Center (Part 1: ID for Sign-in)

View in the browser

LexisNexis® RISK SOLUTIONS | Public Safety & Law Enforcement

February 2021

LexisNexis Risk Solutions is pleased to have U.S. Immigration and Customs Enforcement as one of our valued Accurint® Virtual Crime Center Customers. **Below you will find information about signing into Accurint Virtual Crime Center and how to access training**.

With **Accurint Virtual Crime Center**, you will have access to **10,000 public records and state & local RMS and CAD data from over 1,500 agencies nationwide, all in one search**. You will also have mapping and link analysis capabilities to help you find non-obvious relationships between people, assets and incidents.

Sign-in at Accurint.com with the user name below, and the password that will be sent to you shortly. Use Chrome or Firefox browsers for best results. **A quick-start video to walk you through your first sign-in is here**.

User Name: (b)(7)(E)

(Password will be sent in a separate email)

It's easy to get started with Accurint Virtual Crime Center, simply type in the Quick Search box to easily search on both public records and law enforcement data. For Investigative searches on people, phones, vehicles or businesses, access the five search form icons shown below. For more information sign up for a live ICE training webinar **here**.

(b)(7)(E)

Training Resources

Get the most out of Accurint Virtual Crime Center in four easy steps:

Video: A quick-start video to walk you through your first sign in is **here**.

Live Training: Sign up for live ICE Quick Start and/or Core Competencies training webinars **here**.

Getting Started Guide: Download our **getting started guide** for basic information on searching and reports.

On-demand Training: For more in-depth training, a series of courses is available on the **LexisNexis University Public Safety Academy**.

LexisNexis continues to enhance its technology platforms in order to deliver exceptional service and value. If you have any questions about Accurint Virtual Crime Center, please contact customer support at (b)(7)(E)

Sincerely,

(b)(6); (b)(7)(C)
Strategic Sales Executive
Federal Government
LexisNexis Special Services. Inc.
(b)(6); (b)(7)(C) Direct
Mobile
(b)(6); (b)(7)(C) **@lnssi.com**

Quick Links

Contact the Team **Product Page**
Product Training

From: (b)(6); (b)(7)(C)
Sent: Fri, 17 Sep 2021 12:19:03 +0000
To: (b)(6); (b)(7)(C)
Subject: Accurint

Good Morning (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) sent me a dataset showing who made searches and reports. Via account this morning and I was able to put this together.

Just a quick explanation. Not all accounts were used. Since Atlanta is the first on the Sort by AOR chart we'll use that as an example. Of the 146 accounts only 55 were used to conduct searches and reports. So those 55 people made those 1,809 searches and the 318 reports.

Sort by AOR

AOR	Accounts	Users	Searches	Reports
ATL	146	55	1,809	318
BAL	71	22	493	68
BOS	82	27	359	88
BUF	124	31	463	71
CHI	191	67	2,425	346
DAL	100	32	816	201
DEN	114	46	1,626	258
DET	152	48	822	192
ELP	132	37	1,344	302
HOU	65	22	536	80
LOS	248	77	1,489	348
MIA	210	73	1,342	261
NEW	76	25	604	88
NOL	140	23	547	59
NYC	120	37	1,022	226
PHI	170	45	722	111
PHO	122	31	947	163
SEA	108	46	1,177	140
SFR	208	61	1,505	271
SLC	137	40	1,439	169
SNA	174	49	1,516	282
SND	124	38	2,566	298
SPM	156	29	669	128
WAS	102	25	961	89
HQ	101	15	668	40

LESC	90	56	5,552	600
NCATC	67	49	11,842	2,482
PERC	78	11	129	48
Total	3,608	1,117	45,390	7,727

Sorted By Searches

AOR	Accounts	Users	Searches	Reports
NCATC	67	49	11,842	2,482
LESC	90	56	5,552	600
SND	124	38	2,566	298
CHI	191	67	2,425	346
ATL	146	55	1,809	318
DEN	114	46	1,626	258
SNA	174	49	1,516	282
SFR	208	61	1,505	271
LOS	248	77	1,489	348
SLC	137	40	1,439	169
ELP	132	37	1,344	302
MIA	210	73	1,342	261
SEA	108	46	1,177	140
NYC	120	37	1,022	226
WAS	102	25	961	89
PHO	122	31	947	163
DET	152	48	822	192
DAL	100	32	816	201
PHI	170	45	722	111
SPM	156	29	669	128
HQ	101	15	668	40
NEW	76	25	604	88
NOL	140	23	547	59
HOU	65	22	536	80
BAL	71	22	493	68
BUF	124	31	463	71
BOS	82	27	359	88
PERC	78	11	129	48
Total	3,608	1,117	45,390	7,727

Sorted by Reports

AOR	Accounts	Users	Searches	Reports
NCATC	67	49	11,842	2,482
LESC	90	56	5,552	600
LOS	248	77	1,489	348
CHI	191	67	2,425	346
ATL	146	55	1,809	318
ELP	132	37	1,344	302
SND	124	38	2,566	298
SNA	174	49	1,516	282
SFR	208	61	1,505	271
MIA	210	73	1,342	261
DEN	114	46	1,626	258
NYC	120	37	1,022	226
DAL	100	32	816	201
DET	152	48	822	192
SLC	137	40	1,439	169
PHO	122	31	947	163
SEA	108	46	1,177	140
SPM	156	29	669	128
PHI	170	45	722	111
WAS	102	25	961	89
BOS	82	27	359	88
NEW	76	25	604	88
HOU	65	22	536	80
BUF	124	31	463	71
BAL	71	22	493	68
NOL	140	23	547	59
PERC	78	11	129	48
HQ	101	15	668	40
Total	3,608	1,117	45,390	7,727

(b)(6); (b)(7)(C)

Detention and Deportation Officer, **National Fugitive Operations Program**
Enforcement Division
Enforcement and Removal Operations
Immigration and Customs Enforcement
(202) 497-(b)(6);

United States Immigration and Customs Enforcement
ICE Targeting Operations Division
Data Subscription Services
Statement of Work

1.0 PURPOSE:

The purpose of this requirement is to obtain mission-critical subscription data services to conduct customized analysis, screening, and monitoring of Department of Homeland Security priority criminal alien information in support of the Targeting Operations Division (TOD) of the U.S. Immigration and Customs Enforcement (ICE), Enforcement and Removal Operations (ERO). The required support subscription services contract will support national ICE initiatives, maintain the efficiency of the TOD, and develop leads which permit ERO Field Offices and other ICE entities to focus resources on priority cases involving aliens that pose a threat to public safety and/or national security.

Successful law enforcement operations require adaptation to changing public safety threats and the ability to continually refine processes and modernize information technologies. Although ICE continues to make considerable progress in identifying and arresting criminal aliens, the continued use of proactive and modern enforcement tools and batch and alert capabilities remains an essential approach to achieve ICE enforcement goals. Other less comprehensive and less efficient approaches to the challenges associated with identifying and locating criminal aliens have resulted in limited success. Accordingly ICE-ERO-TOD is seeking a contract service provider to provide a continuous monitoring and alert service that provides real-time jail booking data to support the identification and location of aliens who pose a threat to public safety and/or national security. The TOD will provide targeting information for the service provider to set up a continuous monitoring and alert system to track 500,000 identities per month for specified new data, arrests, and activities

2.0 BACKGROUND

The arrest, detention, and removal of criminal aliens from the United States is one of ICE's current priorities. To address this priority, ICE formed the Targeting Operations Division (TOD) within Enforcement and Removal Operations (ERO). One of the primary missions of the TOD is to identify and locate illegal aliens that pose a threat to public safety and/or national security.

In 2006, ERO first obtained subscription access to commercial database aggregators provided through an agreement with the Federal Library and Information Network (FEDLINK), managed by the United States Library of Congress. At that same time, ERO also purchased a customized batch service with the capability to vet alien information through commercial databases in a batch process, and obtained access to a custom alert service designed to continuously monitor criminal alien information for recent credit or other commercial activities.

Similar services were acquired and managed by ERO from 2007 – 2009. In 2010, all subscription services obtained for ICE programs were managed by the DHS Library Program Management Division as part of a DHS efficiency initiative. However, the growing need for more criminal information and for more accuracy in the batch process prompted the TOD to seek alternatives to data service products currently available through the DHS Library.

3.0 GENERAL REQUIREMENTS

The continuous monitoring and alert system must be able to securely process and return aliens' information and addresses using the following types of specified data: FBI numbers; State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; vehicle registration information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN) data; and employer records.

The vendor must have a multi-tiered internal vetting system in place. Specifically, ERO's data must be analyzed internally by both automation and trained analysts with research support tools to provide the best leads possible and to reduce the number of false positives forwarded to the TOD.

Availability of the contracted services must be flexibly structured to adapt to changing priorities in the law enforcement continuum. This flexibility must allow for possible increases or decreases in the amount of the various services needed.

3.1 PERIOD OF PERFORMANCE

The period of performance will include a twelve (12) month base period, four (4) twelve (12) month option periods, and a six (6) month extension period. The anticipated period of performance can be seen below.

03/01/2018 – 02/28/2019 – Base Period
03/01/2019 – 02/29/2020 – Option Period 1
03/01/2020 – 02/28/2021 – Option Period 2
03/01/2021 – 02/28/2022 – Option Period 3
03/01/2022 – 02/28/2023 – Option Period 4

The Government reserves the right to modify performance standards and/or metrics during the life of this contract, in order to ensure that the right outcomes are being assessed and that the performance

standards are appropriate. Changes will be made via supplemental agreement within the changes clause.

3.2 Place of Performance

The primary place of performance will be the Contractor's facilities.

3.3 Contract Type

Firm Fixed Price (FFP) Purchase Order

3.4 Contract Line Items:

CLIN 0001 CLEAR / Justice Exchange Alert System (500,000 identities)

4.0 SPECIFIC REQUIREMENTS/ TASKS

4.1 Task One

The contractor shall track daily address changes and credit activities of targeted persons (i.e. new aliases, new addresses, new jail bookings, insurance claims, DOB changes, and SSNs, using information available from open sources and commercial data sources. Source listings for this information shall include, but is not limited to, the following: insurance/auto insurance, property, phones, employment, utilities, moving companies, renter information, drivers' licenses, credit checks, vehicle accident reports, Real Time Jail Bookings, pay day loans, check cashing, and death registries.

4.2 Task Two

The contractor shall securely return to ICE, from publicly available and commercial sources available to the contractor, any information that identifies the possible location of the target and changes in the target's identifiers, such as addresses, phone numbers, email addresses, user names, new aliases, date of birth changes, SSN changes, utility changes, arrests, credit checks, death registry information, employment changes, insurance changes, and affiliated organizations through which a location can be derived.

5.0 OTHER APPLICABLE CONDITIONS

5.1 Release of Information

Contractor access to proprietary and Privacy Act-protected information is required under this Statement of Work (SOW). Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the Privacy Act of 1974, and the *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*. Contractor and subcontractors shall not hold any discussions or release any information relating to this contract to anyone not having a direct interest in performance of this contract, without written consent of the Contract Officer (CO) and Contract Officer's Representation (COR). This

restriction applies to all news releases of information to the public, industry or Government agencies, except as follows: Information for actual or potential subcontractors or other individuals necessary for Contractor's performance of this contract. Contractor and subcontractors shall not issue advertisements about projects performed under this task without government review and approval. For the purposes of this paragraph, advertisement is considered to be Contractor-funded promotional brochures, posters, tradeshow handouts, world-wide-web pages, magazines, or any other similar type promotions.

5.2 Non-Disclosure

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of these tasks and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of these tasks. Contractors shall be required to sign Non-Disclosure statements

All information, including documents, workflows, products, training materials, or programs, created in support of ERO, at the request of the TOD management or staff, or generated as a result of this contract, will become the property of the ICE and the U.S. Government.

5.3 Data Use, Disclosure of Information and Handling of Sensitive Information

The contractor will not be provided with any classified information through this requirement. However, the contractor will be provided with law enforcement sensitive information. The Contractor shall maintain, transmit, retain in strictest confidence, and prevent the unauthorized duplication, use, and/or disclosure of information. The Contractor shall only provide information to employees, Contractors, and subcontractors having a bona fide "need to know" in the performance of their duties related to this project.

Information made available to the contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other manner without the written agreement and consent of the CO.

If public information is provided to the contractor for use in performance or administration of this effort, the contractor, except with the written permission of the CO, may not use such information for any other purpose. If the contractor is uncertain about the availability or proposed use of information provided for the performance or administration of the contract, the contractor will consult with the COR regarding use of that information for other purposes.

The contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each offeror or employee of the contractor to whom information may be made available or disclosed shall be notified in writing by the contractor that such information may be disclosed only for the purposes and to the extent authorized herein.

Performance of this effort may require the Contractor to access and utilize data and information proprietary to a Government agency or Government Contractor, which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others.

Contractor and/or Contract personnel shall not divulge or release data or information developed or obtained in performance of this effort, until such time as it is made public by the Government. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort.

Whether conducting publicly available or commercial source-based searches, the contractor shall not maintain any data, including the list of targets provided by ICE and search results provided to ICE after the analysis is complete, nor shall the contractor maintain any data on behalf of ICE after the data is no longer in a state of analysis. The contractor is also not permitted to use any law enforcement information provided by ICE for any outside commercial purpose.

5.4 Unauthorized Commitments (FAR 1.602.3)

The COR is designated by the CO to perform as a technical liaison between the Contractor's management and the CO in routine technical matters constituting general program direction within the scope of the contract. Under no circumstances is the COR authorized to effect any changes in the work required under this contract whatsoever or enter into any agreement that has the effect of changing the terms and conditions of this contract or that causes the Contractor to incur any cost.

Notwithstanding this provision, to the extent the Contractor accepts any direction that constitutes a change of this contract without prior written authorization of the CO; costs incurred in connection therewith are incurred at the sole risk of the Contractor and if invoiced under this contract will be disallowed. On all matters that pertain to the contract terms, the Contractor must communicate with the CO.

Whenever, in the opinion of the Contractor, the COR requests efforts beyond the terms of the contract, the Contractor shall so advise the CO. If the COR persists and there still exists a disagreement as to proper contractual coverage, the CO shall be notified immediately, preferably in writing. Proceeding with work without proper contractual coverage may result in nonpayment or necessitate submittal of a contract claim.

6.0 PRIVACY AND RECORDS REQUIREMENTS

ICE Information Governance and Privacy Requirements Clause (JUL 2017)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information
In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974 the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized

by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

(3) Prior Approval Required to Hire Subcontractors
The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

B. Privacy Training, Safeguarding, and Remediation

If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of this clause is deemed self- deleting.
(1) Required Security and Privacy Training for Contractors
Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or

transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the *Privacy at DHS: Protecting Personal Information* training course. This course, along with more information about DHS security and training requirements for Contractors, is available at www.dhs.gov/dhs-security-and-training-requirements-contractors. The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(2) Safeguarding Sensitive PII Requirement
Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

(3) Non-Disclosure Agreement Requirement
All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) Prohibition on Use of PII in Vendor Billing and Administrative Records
The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Suspected Loss of Sensitive PII
Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.

2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.

3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:

a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
b. Date, time, and location of the incident.
c. Type of information lost or compromised.
d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

(6) Victim Remediation

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates

as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the

Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.

(2) Requirements for Contractor IT Systems Hosting Government Data
The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under "Compliance." DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under "Key Personnel." The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Office, the Office of the Chief Information Officer, and the Records Management Branch to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion. The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

(c) If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

(End of Clause)

***** Clauses Incorporated by Reference *****

In reference to Federal Acquisition Regulation (FAR) 52.252-2, the following clauses are incorporated by reference with the same force and effect as if they were given in full text. The offeror is cautioned not to delete clauses from, nor add clauses to, the following contract clause list.

Such an action may cause your offer to be rejected. Note: The complete text of specific clauses is contained in Chapters (DHS FAR Supplement) of Title 48 of the Code of Federal Regulations (CFR) which are available at most law libraries. In addition, the full text of FAR and HSAR/HSAM clauses may be accessed electronically at http://www.arnet.gov/far/ and http://www.dhs.gov/dhspublic/ respectively.

- FAR 52.212-4, Contract Terms and Conditions (Jan 2017)
- FAR 52.223 5, Pollution Prevention and Right-To-Know Information, (AUG 2003)
- FAR 52.227-14, Rights In Data – General (Dec 2007)
- FAR 52.239-1, Privacy or Security Safeguards (AUG 1996)
- FAR 52.224-1, Privacy Act Notification (APR 1984)
- FAR 52.224-2, Privacy Act (APR 1984)
- HSAR 3052.204-71, Contractor employee access, and Alternate II
- HSAR 3052.209-70, Prohibition On Contract With Corporate Expatriates
- HSAR 3052.242-71, Dissemination of Contract Information
- HSAR 3052.242-72, Contracting Officer Technical Representative

52.217-7, Option For Increased Quantity – Separately Priced Line Item (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer

may exercise the option by written notice to the Contractor within **thirty (30) days prior** to the end of contract performance. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

52.217-8 -- Option to Extend Services ((Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within **thirty (30)** days.

52.217-9, Option To Extend The Term Of The Contract. (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within **fifteen (15) days prior** to the end of contract performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **thirty (30)** days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **sixty (60)** months.

52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items (Jan 2017)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

☒ 52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)
☒ 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)
☒ 52.233-3 Protest After Award (AUG 1996)
☒ 52.233-4 Applicable Law for Breach of Contract Claim (OCT 2004)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

☐ 52.203-6 Restrictions on Subcontractor Sales to the Government (SEPT 2006)
☐ Alternate I (OCT 1995)
☒ 52.203-13 Contractor Code of Business Ethics and Conduct (OCT 2015)
☐ 52.203-15 Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUNE 2010)
☒ 52.204-10 Reporting Executive Compensation and First-Tier Subcontract Awards (OCT 2016)
☐ [Reserved]
☒ 52.204-14 Service Contract Reporting Requirements (OCT 2016)
☐ 52.204-15 Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016)
☒ 52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (OCT 2015)
☒ 52.209-9 Updates of Publicly Available Information Regarding Responsibility Matters (JUL 2013)
☐ [Reserved]
☐ 52.219-3 Notice of Total HUBZone Set-Aside (NOV 2011)
☐ Alternate I (NOV 2011)
☐ 52.219-4 Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2014)
☐ Alternate I (JAN 2011)
☐ [Reserved]
☐ 52.219-6 Notice of Total Small Business Set-Aside (NOV 2011)
☐ Alternate I (NOV 2011)
☐ Alternate II (NOV 2011)
☐ 52.219-7 Notice of Partial Small Business Set-Aside (JUN 2003)
☐ Alternate I (OCT 1995)
☐ Alternate II (MAR 2004)
☐ 52.219-8 Utilization of Small Business Concerns (NOV 2016)
☐ 52.219-9 Small Business Subcontracting Plan (JAN 2017)
☐ Alternate I (NOV 2016)
☐ Alternate II (NOV 2016)
☐ Alternate III (NOV 2016)
☐ Alternate IV (NOV 2016)
☐ 52.219-13 Notice of Set-Aside of Orders (NOV 2011)
☒ 52.219-14 Limitations on Subcontracting (JAN 2017)
☐ 52.219-16 Liquidated Damages – Subcontracting Plan (JAN 1999)
☐ 52.219-27 Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011)
☐ 52.219-28 Post Award Small Business Program Rerepresentation (JUL 2013)
☐ 52.219-29 Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (DEC 2015)
☐ 52.219-30 Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (DEC 2015)
☒ 52.222-3 Convict Labor (JUN 2003)

☐ 52.222-19 Child Labor – Cooperation with Authorities and Remedies (OCT 2016)
☒ 52.222-21 Prohibition of Segregated Facilities (APR 2015)
☒ 52.222-26 Equal Opportunity (SEPT 2016)
☒ 52.222-35 Equal Opportunity for Veterans (OCT 2015)
☒ 52.222-36 Equal Opportunity for Workers with Disabilities (JUL 2014)
☒ 52.222-37 Employment Reports on Veterans (FEB 2016)
☒ 52.222-40 Notification of Employee Rights Under the National Labor Relations Act (DEC 2010)
☒ 52.222-50 Combating Trafficking in Persons (MAR 2015)
☐ Alternate I (MAR 2015)
☒ 52.222-54 Employment Eligibility Verification (OCT 2015)
☐ 52.222-59 Compliance with Labor Laws (Executive Order 13673) (OCT 2016)
☒ 52.222-60 Paycheck Transparency (Executive Order 13673) (OCT 2016)
☐ 52.223-9 Estimate of Percentage of Recovered Material Content for EPA-Designated Products (MAY 2008)
☐ Alternate I (MAY 2008)
☐ 52.223-11 Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016)
☐ 52.223-12 Maintenance, Service, Repair or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016)
☐ 52.223-13 Acquisition of EPEAT®-Registered Imaging Equipment (JUNE 2014)
☐ Alternate I (OCT 2015)
☐ 52.223-14 Acquisition of EPEAT®-Registered Televisions (JUNE 2014)
☐ Alternate I (JUNE 2014)
☐ 52.223-15 Energy Efficiency in Energy-Consuming Products (DEC 2007)
☐ 52.223-16 Acquisition of EPEAT®-Registered Personal Computer Products (OCT 2015)
☐ Alternate I (JUNE 2014)
☒ 52.223-18 Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)
☐ 52.223-20 Aerosols (JUN 2016)
☐ 52.223-21 Foams (JUN 2016)
☒ 52.224-3 Privacy Training (JAN 2017)
☐ Alternate 1 (JAN 2017)
☐ 52.225-1 Buy American – Supplies (MAY 2014)
☐ 52.225-3 Buy American – Free Trade Agreements – Israeli Trade Act (MAY 2014)
☐ Alternate I (MAY 2014)
☐ Alternate II (MAY 2014)
☐ Alternate III (MAY 2014)
☐ 52.225-5 Trade Agreements (OCT 2016)
☒ 52.225-13 Restrictions on Certain Foreign Purchases (JUN 2008)
☐ 52.225-26 Contractors Performing Private Security Functions Outside the United States (OCT 2016)
☐ 52.226-4 Notice of Disaster or Emergency Area Set-Aside (NOV 2007)
☐ 52.226-5 Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007)
☐ 52.232-29 Terms for Financing of Purchases of Commercial Items (FEB 2002)
☐ 52.232-30 Installment Payments for Commercial Items (JAN 2017)

☒ 52.232-33 Payment by Electronic Funds Transfer—System for Award Management (JUL 2013)
☐ 52.232-34 Payment by Electronic Funds Transfer—Other than System for Award Management (JUL 2013)
☐ 52.232-36 Payment by Third Party (MAY 2014)
☒ 52.239-1 Privacy or Security Safeguards (AUG 1996)
☐ 52.242-5 Payments to Small Business Subcontractors (JAN 2017)
☐ 52.247-64 Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006)
☐ Alternate I (APR 2003)

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

☐ 52.222-17 Non-displacement of Qualified Workers (MAY 2014)
☐ 52.222-41 Service Contract Labor Standards (MAY 2014)
☐ 52.222-42 Statement of Equivalent Rates for Federal Hires (MAY 2014)
☐ 52.222-43 Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (MAY 2014)
☐ 52.222-44 Fair Labor Standards Act and Service Contract Act—Price Adjustment (MAY 2014)
☐ 52.222-51 Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014)
☐ 52.222-53 Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014)
☒ 52.222-55 Minimum Wages Under Executive Order 13658 (DEC 2015)
☐ 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2017)
☐ 52.226-6 Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014)
☐ 52.237-11 Accepting and Dispensing of $1 Coin (SEPT 2008)

(d) *Comptroller General Examination of Record.* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records-Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause

or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113- 235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iv) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(v) 52.222-21, Prohibition of Segregated Facilities (Apr 2015)

(vi) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).

(vii) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(viii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(ix) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212)

(x) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xi) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

(xii)

(A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O 13627).

(xii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(xiii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xiv) 52.222-54, Employment Eligibility Verification (Oct 2015).
(xv) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
(xvi) 52.222-59, Compliance with Labor Laws (Executive Order 13673) (OCT 2016)

Note to paragraph (e)(1)(xvi): By a court order issued on October 24, 2016, 52.222-59 is enjoined indefinitely as of the date of the order. The enjoined paragraph will become effective immediately if the court terminates the injunction. At that time, GSA, DoD and NASA will publish a document in the *Federal Register* advising the public of the termination of the injunction.

(xvii) 52.222-60, Paycheck Transparency (Executive Order 13673) (OCT 2016)).
(xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
(xix) (A) 52.224-3, Privacy Training (JAN 2017) (5U.S.C. 552a).
(B) Alternate I (JAN 2017) of 52.224-3.
(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
(xxii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

ICE Directive 4007.1: **Records and Information Management**

Issue Date: January 25, 2021
Superseded: None.
Federal Enterprise Architecture Number: 306-112-002b

1. Purpose/Background. U.S. Immigration and Customs Enforcement (ICE) has the responsibility to effectively and efficiently manage all its records to meet the agency's strategic goals and mission requirements. This Directive establishes ICE policy and procedures for governing the management of records regardless of form or characteristics, created or received by ICE, consistent with Department of Homeland Security (DHS) policy and guidance. The preservation of all ICE records must be done in accordance with applicable laws, regulations, and policies.[1]

2. Policy. All ICE employees and contractors are required to adequately maintain, identify, capture, retain, file, dispose, and transfer all ICE records within their respective Directorate or Program Office. All ICE records are required to be preserved appropriately, easily accessible, and dispositioned at the end of their lifecycle. This includes all ICE records created or received in the course of conducting ICE business, including email, according to applicable federal and DHS regulations. All ICE records, either electronic or hardcopy, must be maintained and stored in a centralized electronic records repository in accordance with records schedules approved by ICE's Office of Information Governance and Privacy (IGP) Records and Data Management Unit (RDM) and the National Archives and Records Administration (NARA).[2]

3. Definitions. The following definitions apply for purposes of this Directive only.

3.1. Capstone. Identification and capture of email records that should be preserved as permanent from the accounts of designated senior officials at or near the top of an agency who are generally responsible for agency and program policy and mission-related actions.

3.2. Disposition. Actions taken when records are no longer needed to conduct current agency business, which include disposal or permanent preservation.

3.3. Essential Record. Information that is essential to the continued functioning or reconstitution of an organization during and after an emergency and also essential to

[1] *See* 44 U.S.C. §§ 3102 – 07 and U.S. Dep't of Homeland Sec., DHS Directive No. 141-01, Records and Information Management (Aug. 11, 2014).

[2] There are three types of records: temporary, permanent, and unscheduled. Temporary records are those determined by NARA to be destroyed at the end of their lifecycle. Permanent records are determined by NARA to have sufficient value to continue preservation as part of the National Archives. Records that do not fall under a NARA-approved records schedule cannot be legally destroyed or transferred for storage. Unscheduled records are considered permanent until a records schedule is approved by NARA. More information regarding ICE adherence to records schedules can be found in the accompanying Handbook.

protecting the rights and interests of that organization and of the individuals directly affected by its activities.

3.4. Essential Records Manager. Serves as the individual responsible for coordinating the agency's Essential Records Program and Plan.

3.5. Essential Records Plan. Guidance that identifies records critical to continued agency operations in the event of an emergency and ensures that records are adequately protected and accessible.

3.6. Headquarters Responsible Officials (HROs). Executive Associate Directors (EADs) of Enforcement and Removal Operations, Homeland Security Investigations, and Management and Administration (M&A); the Principal Legal Advisor; the Associate Director of the Office of Professional Responsibility; and the Assistant Directors, Officers, or equivalent positions who report directly to the Director, Deputy Director, or Chief of Staff.

3.7. Permanent Records. Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time it is needed for administrative, legal, or fiscal purposes.

3.8. Records. All recorded information made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or deemed appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data they contain. Records do not include: library and museum material made or acquired and preserved solely for reference or exhibition purposes, or duplicate copies of records preserved only for convenience.[3]

3.9. Records Assistants (RAs). Representatives within a Directorate or a Program Office responsible for assisting the Records Liaison Officers (RLOs) with day-to-day records management activities.

3.10. Records Liaison Officers (RLOs). Designated representative responsible for overseeing records management activities within a Directorate or Program Office and coordinating those activities with RDM.

3.11. Records Schedule. A set of instructions that provides the legal authority for retention and disposition of records grouped together in a series. It is used to indicate the length of time records must be maintained, identifies records as either permanent or temporary, and provides mandatory instructions for the disposition of records. It may also be referred to as a retention schedule.

[3] *See* 44 U.S.C § 3301.

3.12. Temporary Records. Records approved by NARA to be disposed of after a specified period.

4. Responsibilities.

4.1. HROs are responsible for ensuring compliance with this Directive within their Directorates and Program Offices, including the designation of RLOs and RAs.

4.2. The **ICE Records Officer** is responsible for:

1) Overseeing, developing, issuing, and implementing ICE-wide records management policy and procedures;

2) Conducting site assessments and compliance visits of Directorates and Program Offices to include all ICE facilities—regardless of whether they are controlled by the Government or by non-government entities (e.g., detention facilities owned and/or operated by contractors)—to evaluate record-keeping practices and provide guidance and feedback concerning any risks or vulnerabilities that may exist;

3) Developing and implementing records management training;

4) Coordinating with the Office of the Chief Information Officer (OCIO) to ensure that electronic records management considerations for systems access and security controls are implemented;

5) Developing and implementing the Essential Records Plan; and

6) Establishing procedures and guidance for email records, to include Capstone.

4.3. OCIO is responsible for coordinating with the RDM basic framework for electronic records management storage that enables ICE employees and contractors to follow records management policies.

4.4. The **Essential Records Manager** is responsible for coordinating the agency's Essential Records Program, developing and maintaining ICE's Essential Records Plan, coordinating agency inventory of essential records, outlining measures to protect them, and annually conducting an Essential Records Risk Assessment. The Essential Records Manager periodically tests emergency plans and procedures to determine whether essential records are properly identified, protected, and managed, and also modifies plans and procedures when needed.

4.5. RLOs are responsible for:

1) Assisting RDM with coordination and implementation of records policies and procedures within specific Directorates and Program Offices;

2) Conducting an annual records inventory;

3) Ensuring that office records are managed pursuant to DHS, ICE, NARA, and Office of Management and Budget policies, as well as applicable laws and regulations; and

4) Ensuring that all Directorate and Program Office recordkeeping procedures are established, implemented, and periodically updated for all electronic and hardcopy records.

4.6. **RAs** are responsible for assisting the RLO in coordinating RIM activities for the Directorate or Program Office, including managing the transfer and retrieval of program records to or from storage facilities, the creation of box lists documenting the records maintained in storage, and assisting with the management of paper and electronic filing systems that may exist within the Directorate, the Program Office or its sub-divisions. RA functions are a secondary duty. Directorate or Program Office leadership will assign these duties as needed.

4.7. **ICE Employees and Contractors** are responsible for:

1) Complying with the terms of this Directive;

2) Transferring ICE records upon departure or separation and complying with the mandate to not exit with any records without prior approval from the Records Officer;

3) Working with their Directorate or Program Office's RLO and/or RA to maintain, store, transfer, and/or dispose of records in accordance with law and policy; and

4) Completing annual records management training.

5. **Procedures/Requirements.** See the most current version of the *Records and Information Management Handbook* for implementing guidance and procedures.

6. **Recordkeeping.** All records created by the RDM will be maintained in accordance with a NARA approved retention schedule.

7. **Authorities/References.**

7.1. 5 U.S.C. § 552(a), (g).

7.2. 44 U.S.C. §§ 3101 – 07.

7.3. 44 U.S.C. § 21.

7.4. 44 U.S.C. § 29.

7.5. 36 C.F.R. §§ 1220.1 – 1239.26.

7.6. U.S. Dep't of Homeland Sec., DHS Directive No. 141-01, Records and Information Management (Aug. 11, 2014).

7.7. U.S. Dep't of Homeland Sec., Fed. Emergency Mgmt. Agency, Federal Continuity Directive 1 (Jan. 2017).

8. **Attachment.** None

9. **No Private Right.** This Directorate provides only internal ICE policy guidance, which may be modified, rescinded, or superseded at any time without notice. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigative prerogatives of ICE.

(b)(6); (b)(7)(C)

Tae D. Johnson
Acting Director
U.S. Immigration and Customs Enforcement

From: ERO Assistant Directors
Sent: Wed, 3 Mar 2021 17:38:19 +0000
To: Undisclosed recipients:
Subject: Updated: Law Enforcement Investigative Database Subscription (LEIDS) Accurint Virtual Crime Center (AVCC) available on March 1, 2021
Attachments: LN AVCC ID for Sign-In.docx

Assistant Director for Enforcement

Enforcement and Removal Operations

U.S. Immigration and Customs Enforcement

To: All ERO Employees

Update: As part of this transition of vendors, there is no longer access to Justice Exchange. ERO and Homeland Security Investigations are working on adding Justice Exchange or an equivalent service to the LEIDS contract as soon as possible. ERO is prioritizing obtaining access to this critical information tool.

Headquarters requires everyone with a LEARN account login to LEARN (b)(7)(E) prior to COB March 5, 2021, to maintain access to the license plate reader database. Headquarters Accurint Virtual Crime Center (AVCC) users can contac (b)(7)(E) @ice.dhs.gov to resolve issues connecting to AVCC.

ICE's Law Enforcement Investigative Database Subscription (LEIDS) contract was awarded to LexisNexis Risk Solutions. Effective March 1, 2021, all authorized users will transition from the Thomson Reuters Special Services (TRSS) Consolidated Lead evaluation and Reporting (CLEAR) database to the LexisNexis Accurint Virtual Crime Center (AVCC) database. The AVCC database provides access to public records and state and local record management systems (RMS) and computer-aided dispatch (CAD) data from over 1,500 agencies nationwide, all in one search. Users will also have mapping and link analysis capabilities to help locate non-obvious relationships between people, assets, and incidents.

In an effort to migrate all ICE authorized users seamlessly, it is anticipated that ICE users will be able to access AVCC via sign-in at (b)(7)(E) Information with their assigned username and password will be sent by LexisNexis to the user's ICE email address. Password will be sent in a separate email. Prior to logging in to the system, the user must concur with the agency's permissible uses of the system and affirmatively consent to these rules before proceeding further.

In the event that an automatic registration email is not received, and users need to register for access, please contact your local LEIDS database administrator for registration instructions.

With the migration from the incumbent platform (TRSS CLEAR), users will no longer be able to access the Vigilant Solutions - Law Enforcement Archival Reporting Network (LEARN) License Plate Reader (LPR) through CLEAR. Users may log into their current LPR accounts directly through the LEARN website at (b)(7)(E)

Potential Questions:

Q: What is Accurint Virtual Crime Center (AVCC)?
A: Access to Lexis Nexis AVCC will provide users with the information required to assist in investigations. Users will be able to access public records and state & local RMS and CAD data from over 1,500 agencies nationwide, all in one search.

Q: How do I login?
A: Users must log into Accurint via (b)(7)(E)

Q: What's my user id and password?
A: Users should have a seamless transition. Sign-in at Accurint.com with your username and password. The username and password will be provided to users via registration emails from LexisNexis to your assigned ICE email address. The password will be sent in a separate email.

Q: How do I use the platform?
A: Attached you will find the "Welcome to Accurint Virtual Crime Center (Part 1: ID for Sign-In)" quick instruction guide. Please review the training resources provided in 4 easy steps: (1) Video: a quick-start video to walk you through your first sign in. (2) Live Training via webinars, (3) Getting Started Guide: download getting started guide for basic information on searching and reports and (4) On-demand training: for more in-depth training, a series of courses available via LexisNexis University Public Safety Academy.

If you have any questions about Accurint Virtual Crime Center, please contact customer support at (b)(7)(E) (b)(7)(E)

(b)(6); (b)(7)(C)
Assistant Director
Enforcement
Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement

This message was sent in concurrence with AD Field Operations.

This message expires one year from the date it was sent, pursuant to ERO policy.

Serving with Integrity.
Integrity • **C**ourage • **E**xcellence

U.S. Immigration and Customs Enforcement

From: ERO Assistant Directors
Sent: Wed, 30 Jun 2021 16:07:31 +0000
To: Undisclosed recipients:
Subject: Updated: **Time Sensitive** Addition of Accurint Virtual Crime Center Jail Booking Data [ENF]
Attachments: LN Jail Booking Tipsheet 2.pdf

Assistant Director for Enforcement

Enforcement and Removal Operations

U.S. Immigration and Customs Enforcement

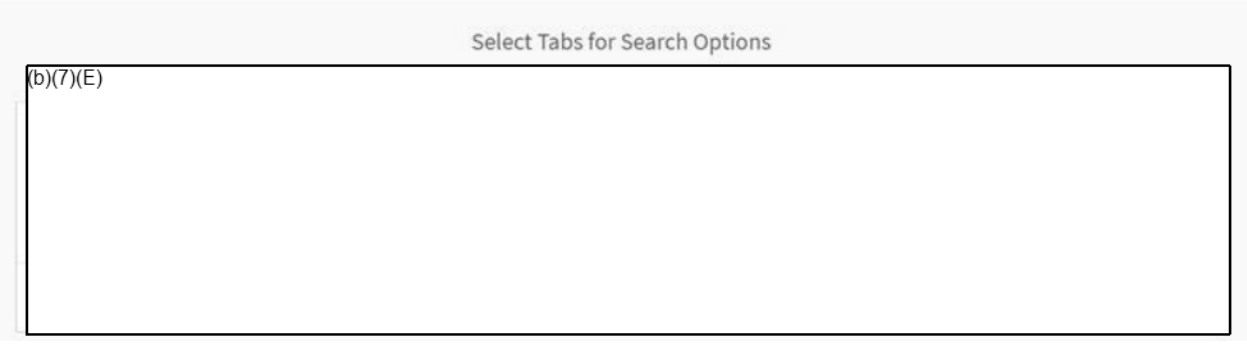
To: Field Office Directors, Assistant Directors, Deputy Field Office Directors, and Deputy Assistant Directors

Subject: **Time Sensitive** Addition of Accurint Virtual Crime Center Jail Booking Data

Updated to include previous broadcast that includes information regarding registration

Please pass this message along to ERO Accurint Virtual Crime Center (AVCC) users and all Criminal Alien Program, National Fugitive Operations Program staff.

The jail booking search was added for all users on ERO accounts effective June 30, 2021. You can find this search option from the home page, as shown below:



LexisNexis Jail Booking Data includes over 140M+ booking records and 38M+ offender images from 2,000+ law enforcement databases. Local booking data is available from facilities in 41 states plus DC,

and state Department of Corrections data is available from 27 states. This equates to over 80% of all incarcerations in the U.S.

Please take a moment to review the attached tip sheet and **this video** for general information.

Please note this additional valuable resource should be widely utilized by ERO personnel as an integral part of our mission to protect the homeland through the identification, location, arrest, and removal of noncitizens who undermine the safety of our communities and the integrity of our immigration laws. ERO currently has available resources to bring on over 4,200 users onto Accurint. Please disseminate the attached broadcast regarding registration, and the below training information.

Training:

The Enforcement Division is providing training support for up to 7,500 ERO AVCC users. The LexisNexis Education team is offering 30 minute training sessions for this new feature to begin June 30, 2021. During this session, you will learn how to conduct these new jail booking searches as well as information to best understand the results returned. A brief overview of some common questions will also be covered during these sessions. Please feel free to ask any questions you may have regarding AVCC during these sessions. The education team is happy to address any questions for us to best use this valuable resource.

To register for the jail booking sessions, please use the link below:

(b)(7)(E)

If you have not attended the 90 minute AVCC new user training, please use the link below to register for an upcoming session that best fits your schedule:

(b)(7)(E)

(b)(6); (b)(7)(C)

Assistant Director
Enforcement
Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement

This message was sent in concurrence with AD Field Operations.

This message expires one year from the date it was sent, pursuant to ERO policy.

Serving with Integrity.
Integrity • **C**ourage • **E**xcellence

U.S. Immigration and Customs Enforcement

PUBLIC SAFETY

Jail Booking Search Now Available with Accurint® Virtual Crime Center

Accurint® Virtual Crime Center Jail Booking Search includes real-time, nationwide incarceration data—direct from the nation's leading source of custody status information. Effectively locate and monitor specialized populations with the most comprehensive and frequently updated database of historical booking information.

EASILY SEARCH DATA COVERING:

85%
of all incarcerations across the U.S., with over 160M+ booking records.

2,800
law enforcement databases across 48 states.

40M+
offender images assist in identification.

15 minutes
Updates as frequently as every 15 minutes allowing for immediate response.

NOW AVAILABLE WITH ACCURINT VIRTUAL CRIME CENTER, ACCESS JAIL BOOKING SEARCH WITH ONE CLICK FROM YOUR HOME SCREEN.

LexisNexis® RISK SOLUTIONS

For more information, call (b)(6); (b)(7)(C) or visit (b)(6); (b)(7)(C)

About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

4003.2: Safeguarding Law Enforcement Sensitive Information

Issue Date: 5/20/2014
Effective Date: 5/20/2014
Superseded: U.S. Immigration and Customs Enforcement (ICE) Directive 4003.1 (formerly ICE Directive 5–2.0), Safeguarding Law Enforcement Sensitive Information, dated March 23, 2007; United States Customs Service Directive 4320–025, Disclosure of Law Enforcement Related/Sensitive Information to Foreign Governments, dated February 26, 2001.
Federal Enterprise Architecture Number: 306–112–002b

1. **Purpose/Background.** This Directive establishes U.S. Immigration and Customs Enforcement (ICE) policy and procedures for the designation, dissemination, and safeguarding of law enforcement sensitive (LES) information. LES information is a subset of For Official Use Only (FOUO) information.

   FOUO–LES information must be marked to ensure its protection. The loss or misuse of, or unauthorized access to, such information could adversely affect the national interest, the conduct of investigative work, or the privacy to which individuals are entitled under the Privacy Act (Title 5, United States Code (U.S.C.), § 552a). The loss or misuse of, or unauthorized access to, such information could also cause the obstruction or impairment of official law enforcement or regulatory functions; damage leading to loss of life or personal injury; loss of property through fraud, theft, or other unlawful means; loss of privacy of an individual; gain by an individual, corporation, or any other type of commercial business structure of an unfair advantage in the competitive marketplace; or damage to a person or any type of commercial business structure that has entrusted its proprietary information to the U.S. Government.

   This Directive applies to information designated as FOUO–LES originated by ICE or received by ICE from other Department of Homeland Security (DHS) components or from state, local, tribal, international, or other federal entities. This Directive also applies to information considered LES that is received from non-governmental entities, foreign governments, or international organizations but is not marked LES. Examples of other such markings may include Confidential,[1] Limited Official Use, Official Use Only, or other terms used by non-U.S. Government entities, and/or information protected by

[1] In this context, "Confidential" refers to documents or information received from a non-governmental entity or foreign agency containing information that is to be treated as "confidential" as that term is interpreted by the respective entity.

specific statutory authority and noted as such. This Directive does not apply to classified U.S. Government information (Confidential,[2] Secret, and Top Secret).

2. Policy. DHS personnel must have timely access to all relevant information they need to successfully perform their duties. Therefore, absent any compromise of the mission of DHS or ICE, or prohibition by law, policy, or established agreement, information shall be shared within DHS and with external partners based on the need-to-know of the requesting employee and according to the dissemination and safeguarding requirements contained in this Directive. All DHS components are considered part of one agency for the purposes of the Privacy Act, and no DHS component should consider another DHS component to be a separate agency for information-sharing purposes.

3. Definitions. The following definitions apply for the purposes of this Directive only:

3.1. Access. The ability or opportunity to gain knowledge of information.

3.2. Authorized. Used in the context of authorized access to information, a determination made by an ICE official that access to FOUO–LES information for an individual is sanctioned by DHS and ICE policies or directives.

3.3. For Official Use Only (FOUO). Term identifying Sensitive But Unclassified information that may or may not be categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest. Information affecting the national security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 13526, "Classified National Security Information," as amended, or its predecessor or successor orders, is not considered FOUO. Sensitive But Unclassified information is a term used within the federal government for documents and information that are sufficiently sensitive to warrant some level of protection from disclosure but that do not warrant classification.

3.4. Foreign Government. Includes any government, faction, or body of insurgents within a country with which the United States is at peace, irrespective of recognition by the United States.

3.5. Headquarters Responsible Officials. Executive Associate Directors (EADs) of ICE Homeland Security Investigations (HSI), ICE Enforcement and Removal Operations (ERO), and Management and Administration (M&A); and the Assistant Directors, Officers, or equivalent positions who report directly to the Director, Deputy Director, the Chief of Staff, the EAD for M&A, or the ICE Principal Legal Advisor.

3.6. Holder. Includes users and/or individuals authorized to mark, store, disseminate, safeguard, and destroy FOUO–LES information within the provisions of this Directive.

[2] In this context, "Confidential" refers to a U.S. Government classification.

3.7. Information Sharing and Access Agreement (ISAA). An agreement that defines the terms and conditions of information/data exchanges between two or more parties. The ISAA is a critical element of the DHS data governance model and typically includes clearly articulated controls for managing the risks of unauthorized use, uncontrolled sharing, and non-compliant information processes, among other agreement terms.

3.8. Interconnection Security Agreement (ISA). An agreement that documents the security features in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. This includes such areas as incident reporting and personnel clearances.

3.9. International Organization. A public international organization in which the United States participates pursuant to any treaty or under the authority of any Act of Congress authorizing such participation or making an appropriation for such participation, and which shall have been designated by the President through an appropriate Executive Order.

3.10. Law Enforcement Records or Information. Any information collected in the course of or related to preliminary, open, pending, or closed administrative, criminal, or civil investigations or enforcement activities within an agency's assigned law enforcement mission.

3.11. Law Enforcement Sensitive (LES). A type of FOUO information that is compiled for law enforcement purposes and which the loss or misuse of, or unauthorized access to could adversely affect the national interest or the conduct of investigative work, disclose the identity of a confidential informant or source of information, endanger life or physical safety, or impact the privacy to which individuals are entitled under the Privacy Act or the DHS privacy policy (DHS Privacy Policy Guidance Memorandum 2007–01 entitled "Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons," dated January 19, 2007, as amended January 7, 2009).

Information impacting the national security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 13526, "Classified National Security Information," as amended, or its predecessor or successor orders, is not considered FOUO–LES information.

3.12. Need-to-Know. Absent any compromise of the mission of DHS or ICE, or prohibition by law, policy, or established agreement, a determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized government function.

3.13. Originator. An ICE employee, detailee, or contractor who prepares material that contains information designated as FOUO–LES as described in this Directive. A supervisor or management official may act on behalf of the originator.

3.14. Originating Office. The directorate or program office where the document containing FOUO–LES information as described in this Directive was created or prepared.

3.15. Personally Identifiable Information (PII). Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, or DHS employee, detailee, or contractor.

3.16. Protected Critical Infrastructure Information (PCII). Critical infrastructure information (CII) is defined in 6 U.S.C. § 131(3) (Section 212(3) of the Homeland Security Act of 2002) as information not customarily in the public domain and related to the security of critical infrastructure or protected systems. PCII is a subset of CII that is voluntarily submitted directly or indirectly to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purpose, and any information, statements, compilations, or other materials reasonably necessary to explain the CII, put the CII in context, or describe the importance or use of the CII, and for which protection is requested under the PCII program. PCII includes the identity of the submitting person or entity, and any person or entity on whose behalf the CII is submitted.

3.17. Sensitive Personally Identifiable Information (Sensitive PII). Sensitive PII is PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements. Examples include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. Sensitive PII is subject to special handling requirements described in the "Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security," dated October 31, 2008, or as updated. Finally, while all SPII is FOUO, depending on the information only some SPII is FOUO-LES.

3.18. Sensitive Security Information (SSI). SSI is defined in 49 U.S.C. § 40119 and in implementing regulations at Title 49, Code of Federal Regulations (C.F.R.) Parts 15 and 1520 as information obtained or developed in the conduct of security activities, including research and development, in carrying out certain security or research and development activities, the disclosure of which would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety or security of passengers in transportation. SSI is a specific category of information that requires protections against disclosure.

3.19. Terrorism Information. The term "terrorism information," consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485(a)(5), means all information, (whether collected, produced, or distributed by

intelligence, law enforcement, military, or homeland security), or other activities, relating to:

1) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
2) threats posed by such groups or individuals to the United States, U.S. persons, or U.S. interests or to those of other nations;
3) communications of or by such groups or individuals; or
4) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

The term "terrorism information" also includes weapons of mass destruction information, which means all information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

4. Responsibilities.

4.1. **The Director** is responsible for ensuring that standards for safeguarding FOUO–LES information within ICE are established and implemented.

4.2. **The Chief Information Security Officer** and the **ICE Chief Security Officer** are jointly responsible for the implementation and oversight of the FOUO–LES information protection program related to computer/information security and will serve as the liaisons between ICE and the DHS Office of Security and all other DHS organizational security officials.

4.3. **The Service Desk** is responsible for receipt and dissemination of reports regarding the actual or suspected loss, compromise, suspected compromise, or unauthorized disclosure of FOUO–LES information and information containing Sensitive PII.

4.4 **The Privacy and Records Office (PRO)** is responsible for helping ICE employees, detailees, and contractors to identify Sensitive PII and for managing the response to privacy incidents, which DHS defines as the loss, compromise, or unauthorized disclosure/exposure of Sensitive PII, whether suspected or confirmed. PRO provides privacy advice, training, and educational materials to all ICE personnel.

4.5. **Headquarters Responsible Officials** are responsible for following the policies and procedures of this Directive to ensure proper designation, safeguarding, dissemination, removal of designations, and/or resolution of all requests for designation removal determinations for FOUO–LES information within their area of responsibility.

4.6. **Supervisors and Managers** are responsible for ensuring employees are aware of what constitutes FOUO–LES information and the steps necessary to properly designate, disseminate, and safeguard such information from unauthorized disclosure. Awareness of the requirements for safeguarding LES information should begin upon the initial assignment of an employee and should be reinforced periodically thereafter through ICE-delivered formal classroom or computer-based training sessions as well as through routine office interaction, e-mail reminders, staff meetings, or any other method or media that contributes to an informed workforce.

4.7. **HSI** is designated as the lead directorate for the disclosure of all ICE-generated, FOUO–LES information originating within HSI, except as listed in 4.8 below, to federal, state, local, tribal, foreign governments, and international organizations. In addition, all requests to ICE from foreign governments or international organizations for FOUO–LES information (and other international information sharing agreements), except as listed in 4.8 below, must be coordinated through the HSI Office of International Affairs (OIA) before release.

4.8. **ERO** is designated as the lead directorate for the disclosure of all ICE-generated, FOUO–LES information originating within ERO. ERO generates information for the conduct of operations to identify and apprehend removable aliens, to detain these individuals when necessary, and to remove aliens from the United States. ERO is the lead for disclosure of FOUO–LES information generated for logistical aspects of the removal process, including domestic transportation, detention, alternatives to detention programs, bond management, and supervised release to federal, state, local, and tribal governments and for the disclosure of this FOUO–LES information to foreign governments and international organizations. Disclosure of FOUO–LES information for the purposes stated in this paragraph does not require coordination through HSI OIA before release. However, ERO officers working under the umbrella of an OIA Attaché Office as an Assistant Attaché for Removals will coordinate the release of any ICE information to a foreign government with the attaché in their chain of command.

4.9. **Other Directorates and Program Offices** that generate FOUO–LES information are authorized to disclose FOUO–LES information originating from their respective directorate(s) or program office(s) to federal, state, local, and tribal organizations. In addition, all requests to ICE from foreign governments or international organizations for FOUO–LES information, except as listed in 4.8 above, must be coordinated through HSI OIA before release.

All ICE Employees, Detailees, and Contractors are responsible for complying with the provisions of this Directive and completing mandatory training on designation, safeguarding, dissemination, removal of designations, and/or resolution of all requests for designation removal determinations for FOUO–LES information.

4.10. **Contractors** must sign a DHS Form 11000–6, Sensitive But Unclassified Information non-disclosure agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS but to whom access to

information will be granted may be required to sign an NDA as determined by the applicable program manager.

4.11. All ICE Offices and Employees who develop requirements for contractor support are responsible for requiring application of all provisions of this Directive. The originator of documents containing FOUO–LES information is responsible for ensuring that all such documents are appropriately marked. When it is determined that it is necessary to include these requirements in a specific ICE contract, it is ICE's responsibility to ensure that this Directive is made a material part of the contract, thereby making contractors responsible for complying with the contract terms on proper designation, safeguarding, dissemination, and destruction of FOUO–LES information. The requiring office will submit specific requirements as part of its acquisition package (along with the estimated cost for implementation).

4.12. Directorates and Program Offices receiving FOUO–LES Information must designate, safeguard, and disseminate that information in accordance with the procedures provided in this Directive or with corresponding internal procedures that comply with this Directive. This information must also be used only as authorized by law or policy or as agreed to if received pursuant to a formally executed agreement or arrangement between the receiving organization/government and ICE. Upon receipt of a document containing FOUO–LES information that is not properly designated, the receiving office will place appropriate markings on the document. The receiving office will notify the originating office that the appropriate markings have been placed on the document.

5. Procedures. These procedures address the designation, marking, safeguarding, dissemination, transmission, and storage of FOUO–LES information as well as incident reporting.

5.1. Designation of Information as FOUO–LES. FOUO information is FOUO–LES when any authorized release could fall within the categories defined by the Freedom of Information Act (FOIA) exemption (b)(7), which applies to information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information:

1) could reasonably be expected to interfere with (law) enforcement proceedings (or investigations);[3]

2) would deprive a person of a right to a fair trial or an impartial adjudication;

3) could reasonably be expected to constitute an unwarranted invasion of personal privacy;

4) could reasonably be expected to disclose the identity of a confidential informant or source of information, including a federal, state, local, tribal, or foreign agency or

[3] Information contained within the parentheses provides additional guidance regarding FOUO–LES information above what is set forth in the FOIA.

authority or any private institution which furnished information on a confidential basis, or, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source;

5) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or

6) could reasonably be expected to endanger the life or physical safety of any individual.

5.2. Designation Authority. Any ICE employee, detailee, or contractor, in the course of performing assigned duties, may designate information falling within one or more of the categories, including, but not limited to, those cited in sections 5.1 and 5.7(3) of this Directive as FOUO–LES.

5.3. Duration of Designation. Information designated as LES will retain its designation until determined otherwise by the respective originating office. As needed, the originating directorate or program office will review FOUO–LES information to determine if the designation is still required.

5.4. Designation Removal. The originating office may remove the FOUO–LES designation of information. If the designation is recommended for removal by an ICE directorate or program office other than the originating office, including through the established ICE FOIA public release process, the originating office must be contacted and concur with the removal. When an FOUO–LES designation is removed, all known holders will be notified to the greatest extent possible. Although downgrading instructions are not required for FOUO–LES designated documents, the originating office must record/document when the FOUO–LES designation is removed. The rationale for designation removal must be noted.

5.5. Marking LES Information.

1) Materials containing FOUO–LES information generated by ICE shall be marked "FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE" as required by DHS Management Directive 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," dated January 1, 2005, or as updated, and shall identify the originator and the originating office responsible for the material. Insertion of this information in the header and/or footer of each page containing FOUO–LES information would satisfy this requirement.

2) Where the appropriate marking is not present on materials known by the authorized holder to be FOUO–LES information (internal or external to ICE), the holder must protect it as FOUO–LES and notify the ICE originating office that the information is

not properly marked. If the information is inadvertently released outside of ICE, the notification requirements set forth in Section 5.13, Incident Reporting, must be followed.

3) Digital storage media (e.g., compact disks, disks, tapes, etc.) containing FOUO–LES information will be marked "SENSITIVE" in accordance with the provisions of DHS Handbook 4300A, entitled "DHS Sensitive Systems Handbook," dated September 30, 2007.

4) Portions of a classified document (e.g., subjects, titles, paragraphs, and subparagraphs) that are unclassified but contain FOUO–LES information must be marked with the FOUO–LES abbreviation next to the (U) designation, as follows: "(U) (FOUO–LES)".

5) Limited FOUO–LES information may be contained in an Alien File (A-File). FOUO information pertinent to the subject of the A-File that is required for adjudication, asylum purposes, exclusion, deportation, or removal of the subject from the United States is required to be placed in the A-File (including travel document-related information generated or received by ERO). Any FOUO–LES information contained in the A-File must be appropriately marked before insertion into the A-File.

   FOUO–LES information contained in investigative case management records that falls outside the above-mentioned requirements must not be stored in the A-File. Treasury Enforcement Case System (TECS) records or other FOUO–LES investigative case management system information shall not be printed and placed in the A-File.

   Contents of A-Files held by directorates and program offices that were generated before the signature of this Directive must be reviewed before being forwarded to the National Records Center (NRC). Additionally, any A-File pulled from the NRC for future law enforcement action must be reviewed to ensure that the A-File does not contain investigative case management records, printed TECS records, or other FOUO–LES investigative case management system information.

6) Individual portion markings are encouraged but not required on a document that contains only FOUO–LES information.

7) Documents, whether in hardcopy or electronic media, released to foreign governments or international organizations must be clearly marked to indicate the purpose for which the documents are being provided. However, where documents are required for judicial proceedings and the marking would not be appropriate, a cover letter should accompany the documents and explain that the documents are being provided for that judicial proceeding and, if the foreign government or international organization would like to use the same documents in another judicial

proceeding, it must first obtain written ICE authorization. Written authorization must be obtained from the originating office and coordinated through HSI OIA.

5.6. Access and Dissemination of FOUO–LES Information to Entities Other Than Foreign Governments or International Organizations.

1) Subject to the provisions of Section 5.7(5), FOUO–LES information may be shared with other federal, state, local, or tribal government law enforcement officials, provided that a specific need-to-know has been established, the information is shared in furtherance of a coordinated and official government activity, and is authorized by applicable law or policy.

2) Subject to the provisions of Section 5.7(5), when ICE personnel (employees, detailees, or contractors) disclose (either orally or in writing) FOUO–LES information to another individual(s), ICE personnel must ensure that the individual to whom the information is to be disclosed has a valid need-to-know and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

3) An ISAA in the form of a memorandum of understanding (MOU), memorandum of agreement (MOA), or letter of intent may formalize FOUO–LES information exchanges between DHS and an external entity.

4) Subject to the provisions of Section 5.7(5) below, where FOUO–LES information is requested by an official of another agency and there is no coordinated or other official agreement, a written request will be made from the requesting agency to the applicable ICE directorate or program office that originated the FOUO–LES information providing the name(s) and title of personnel for whom access is requested, the specific information to which access is requested, and the basis for the need-to-know. The originating ICE directorate or program office shall then determine whether it is appropriate to release the information to the other agency official.

5) Other sensitive information protected by law or policy (e.g., Sensitive PII, Privacy Act, CII, SSI, grand jury, etc.) must be controlled and disseminated in accordance with the applicable guidance for that type of information.

6) Terrorism information shall be shared with other federal agencies that have counterterrorism functions in compliance with Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," dated October 25, 2005, unless otherwise directed by the President, and in conjunction with any guidance issued by the Attorney General of the United States and any other applicable law.

7) When anticipating release of FOUO–LES information where there is no formally executed agreement or arrangement between the receiving entity and ICE, the originating directorate or program office will be contacted for approval before release. If the release is to a foreign government or entity, the releasing directorate or program office must coordinate with HSI OIA, except as set forth in Section 4.8. (See Section 5.9, Dissemination to Foreign Governments and International Organizations.)

8) ICE shall advise the requesting agency of the following:

   a) records are furnished under the conditions that the information will be handled as FOUO–LES information and used only for the purpose stated in the request;
   b) information may not be further disseminated to third parties without the express written permission from the originating ICE directorate or program office;
   c) in the event that an unauthorized release has occurred, the providing office will be notified at the point of discovery of the unauthorized release, and procedures will be followed in accordance with section 5.13 of this Directive; and
   d) where information is being provided under 19 U.S.C. § 1628, a foreign customs or law enforcement agency that has violated the terms of subsection (b)(1) of that statute may not receive further information under 19 U.S.C. § 1628.[4]

9) When discussing FOUO–LES information over a telephone, the use of a Secure Telephone Unit III or Secure Telephone Equipment is encouraged but not required.

10) A security clearance is not required for access to FOUO–LES information; however, all persons having access to FOUO–LES information systems must have undergone, at a minimum, a suitability determination. For ICE personnel, suitability determination requirements are defined in ICE Policy Index Number 17002.1 (formerly numbered ICE Directive 6–7.0), "ICE Personnel Security and Suitability Program," dated February 4, 2008, or as updated, or ICE Policy Index ICE Index Number 17003.1 (formerly numbered Directive 6–8.0), "ICE Suitability and Screening Requirements for Contractor Personnel," dated May 29, 2008, or as updated.

11) Information from another government agency, commonly referred to as third-party information, is subject to that agency's policy and regulations concerning discussion and dissemination of the information, unless alternative arrangements have been made.

12) As a best practice, all known disseminations of FOUO–LES case information should be noted in the case file, in the case management file, or documented on the Case

[4] 19 U.S.C. § 1628(b)(1): "Information may be provided to foreign customs and law enforcement agencies under subsection (a) only if the Secretary obtains assurances from such agencies that such information will be held in confidence and used only for the law enforcement purposes for which such information is provided to such agencies by the Secretary."

Chronology and Review Sheet (ICE Form 73–004) to provide a record of such disseminations.

13) When disclosing Privacy Act information (see Section 5.7(4)) outside of DHS, employees must create a record of the disclosure that reflects the date, nature, and purpose of the disclosure, the name and address of the person or agency to whom the disclosure is made. Employees may use the Privacy Act Disclosure Record (DHS Form 191) to account for the disclosure or may document it using other appropriate means. Whenever possible, the accounting should be placed in the file from which the disclosure was made or in another appropriate file about the individual where it is likely to be easily located. This accounting of the disclosure must be maintained for at least five years or the life of the record, whichever is longer.

5.7. Dissemination Limitations.

1) ICE directorates and program offices may disseminate FOUO–LES information to internal and/or external parties, unless the directorate or program office determines that such sharing would compromise the mission of DHS or ICE or it is prohibited by law, policy, or established agreement. Disputes will be handled in accordance with the DHS information sharing dispute resolution process. The Executive Director, Law Enforcement Information Sharing Initiative, will provide guidance to ICE directorates and program offices regarding dispute resolution.

2) Absent any compromise of the mission of DHS or ICE, or prohibition by law, policy, or established agreement, access to the following FOUO–LES information may be granted in accordance with the provisions of this Directive at the discretion of the originating office only when justified by a need-to-know and an established agreement. For the following FOUO–LES information, the authorized holder may be subject to further policy constraints at the discretion of the originating office:

   a) information pertaining to open investigations;
   b) information that reveals the identity of informants;
   c) information pertaining to planned or ongoing surveillance and/or undercover operations; and
   d) information that reveals other sensitive operations.

3) FOUO–LES information that is protected by statute or regulation must be controlled and disseminated in accordance with the applicable guidance for the information. This includes, but is not limited to, the following information:

   a) grand jury (6e) information. In accordance with Federal Rule of Criminal Procedure 6(e)(3);
   b) child victim/witness. In accordance with 18 U.S.C. § 3509;
   c) juvenile. In accordance with 18 U.S.C. § 5031;
   d) Witness Security Program. In accordance with 18 U.S.C. § 3521;
   e) restricted by court order. Dependent upon the text of the Court Order;

f) proprietary. In accordance with 18 U.S.C. § 1905 or in accordance with written agreement between ICE and the provider of the information;
g) federal taxpayer information.[5] When information has been shared with ICE by the Internal Revenue Service in accordance with 26 U.S.C. § 6103;
h) CII. As defined in 6 U.S.C. § 131(3) (section 212(3) of the Homeland Security Act);
i) SSI. As defined in 49 C.F.R. Parts 15, 1250, and 1520.5 and 49 U.S.C. § 40119;
j) violence against women claimants. In accordance with 8 U.S.C. § 1367(a)(2) (section 384(a)(2) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996);
k) battered spouse or child information. In accordance with 8 U.S.C. § 1186a(c)(4)(C) (section 216(c)(4)(C) of the Immigration and Nationality Act (INA));
l) legalization/seasonal agricultural worker claims. In accordance with 8 U.S.C. §§ 1255a(c)(4), (5), and 1160(b)(5) and (6) (sections 245A and 210 of the INA);
m) U.S. Department of State records pertaining to the issuance or refusal of visas or permits to enter the United States. In accordance with 8 U.S.C. § 1202(f) (section 222(f) of the INA);
n) T visa (nonimmigrant status) and U visa (nonimmigrant status). In accordance with the Victims of Trafficking Protection Act of 2000, section 107(c)(l)(C) and pursuant to 8 C.F.R. § 214.11(e);
o) temporary protected status. In accordance with 8 U.S.C. § 1254a(c)(6) (section 244(c)(6) of the INA);
p) alien fingerprint and registration forms. In accordance with 8 U.S.C. § 1304(b) (section 264(b) of the INA);
q) asylum information. In accordance with 8 C.F.R. §§ 208.6 and 1208.6;
r) Bank Secrecy Act (BSA). In accordance with 31 U.S.C. § 5311, *et seq.*; and
s) Trade Secrets Act. In accordance with 18 U.S.C. § 1905.

4) Additional FOUO–LES information that must be controlled and disseminated in accordance with applicable guidance is listed below:

a) information contains Deliberative Process, Attorney Work Product, or Attorney Client Privileged Communication. The processes of evaluating relevant evidence, arguments, and options for the purpose of making a decision related to the performance of an agency's functions;
b) Not to be Disclosed Outside of Internal DHS Intelligence Channels. Used when information is requested by DHS under the DHS Office of Intelligence and Analysis (I&A);
c) Request for Information, or when DHS I&A requests FOUO–LES information for briefing, analysis, or other purposes; and
d) ICE FOUO–LES Reports of Investigation (ROIs). ROIs containing the following types of information:

[5] This does not include taxpayer information disclosed to ICE by a party other than the Internal Revenue Service. Although such information is still FOUO information, it is not further protected by statute.

i) reports resulting from Title III wire intercepts;
ii) reports of certified undercover operations;
iii) reports citing information obtained under the BSA;
iv) reports citing confidential sources of information;
v) grand jury material (6e);
vi) reports including information covered by the third-agency rule;
vii) reports including information protected by the Trade Secrets Act; and
viii) reports relating to asylum claims.

5) Privacy Act:

a) electronic or paper records and information that contain information about individuals and are actually retrieved by an individual's name or other personal identifier (e.g., Social Security number, A-Number, Subject ID) are subject to the requirements of the Privacy Act. The Privacy Act applies to U.S. Citizens and lawful permanent residents, however, DHS has extended the act's application by policy to all individuals. The use and dissemination of this information is governed by the Privacy Act, the DHS Privacy Policy, and the relevant Privacy Act System of Records Notices (SORN(s)) that describe the collection, use, and disclosure of information in its paper and electronic recordkeeping systems. ICE employees shall not disclose Privacy Act information unless authorized by subsection (b) of the Privacy Act (5 U.S.C. § 552a(b)). This Directive describes some, but not all, situations in which Privacy Act information from ICE recordkeeping systems may be disclosed. Because disclosure questions are often complex, ICE employees and their supervisors are encouraged to consult with the Office of the Principal Legal Advisor or PRO;
b) ICE employees are authorized to disclose Privacy Act information within DHS for official purposes where the receiving employee has a need for the information for the conduct of his or her official duties. ICE employees may disclose information outside of DHS if authority exists from subsection (b) of the Privacy Act pursuant to written permission from the individual to whom the record pertains, as authorized by the Privacy Act itself in subsection (b), or pursuant to one of the Privacy Act "Routine Uses" in applicable Privacy Act SORN(s). When disclosures are authorized by the Privacy Act, these disclosures are discretionary. ICE employees have the authority to disclose the information but are not required to make such disclosures. (Note: A complete list of ICE SORNs is available on the Privacy intranet website.) Routine Uses permit disclosures of Privacy Act information for reasons that vary depending on the nature of the records and the purpose for which they were created. Routine Uses permitted for ICE's law enforcement recordkeeping systems will typically allow for sharing for purposes related to law enforcement, counterterrorism, immigration and removal proceedings, and litigation. Before making a disclosure, ICE employees and their supervisors shall ensure that it is clearly within the scope of the Routine Use or seek appropriate guidance from the Office of the Principal Legal Advisor or PRO; and

c) Privacy Act-protected information may be disclosed to a domestic agency conducting a civil or criminal law enforcement investigation or activity authorized by law pursuant to section (b)(7) of the Privacy Act (5 U.S.C. § 552a(b)(7)). To make a disclosure pursuant to section (b)(7), the ICE Privacy Guidance: "Requests for Information Under Section (b)(7) of the Privacy Act," dated August 13, 2010, should be consulted.

6) Third parties may not compel disclosure of the information held in agency systems of records to non-law enforcement organizations or persons through the use of state laws ("sunshine" laws or freedom of information laws).

7) Information designated as FOUO–LES may not be used in legal proceedings without first consulting and requesting approval of the originating office and adhering to appropriate DHS and ICE procedures.

5.8. Dissemination of FOUO–LES Information to Foreign Governments or International Organizations. ICE employees, detailees, and contractors will contact the ICE originating office for approval and coordinate with HSI OIA before disseminating LES information to foreign governments or international organizations, with the exception of certain ERO information as set forth in section 4.8 of this Directive.

1) The dissemination of FOUO–LES information to foreign governments or international organizations may be authorized if the disclosure is necessary to:

   a) ensure compliance with any law or regulation enforced or administered by ICE;
   b) administer or enforce provisions of multilateral or bilateral agreements to which the United States is a party; or
   c) assist in investigative, judicial, and quasi-judicial proceedings in the United States and any action comparable to any of those described above undertaken by a foreign customs, immigration, or law enforcement agency.

2) Title 19 U.S.C. § 1628, Exchange of Information, authorizes Customs officers to share information with foreign customs and law enforcement agencies. This statute sets forth the purposes for which such information may be shared, and that the information must be provided only if assurances are obtained that the information will be held in confidence and used only for the law enforcement purposes for which it is sought. If a foreign customs or law enforcement agency violates these assurances, no further information may be provided to that agency under this statute. U.S. Customs officers sharing information under this statute should refer to the current delegation order. (See also Section 5.6(8)(d) above.)

3) HSI OIA shall review and coordinate all international requests for FOUO–LES information, unless the request is to ERO for the purpose of procuring travel documents or for coordinating and conducting removals from the United States. (See also Section 4.8 above.)

4) Except in exigent circumstances, requests for records or information (FOUO–LES or otherwise) must be made formally in writing or contained in an approved ISAA, setting forth the specific records or information requested and the reason(s) for the request. In exigent circumstances where a formal request cannot be received before an oral request to disseminate FOUO–LES information, the requestor must provide the formal request to ICE in writing within 24 hours after the submission of the oral request.

    a) Examples of exigent circumstances include:
        i. there is an actual or potential threat of terrorism accompanied by an immediate danger of death or serious physical injury to any person or imminent harm to national security; and

        ii. it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to such a threat, danger, or harm.

    If immediate dissemination of FOUO–LES information is required before ICE's receipt of the written request, FOUO–LES information may be released based on the approval of an ICE-authorized dissemination official in coordination with HSI OIA. The dissemination will be documented by the ICE official who authorized the dissemination. Documentation must include the specific records or information requested, the reason needed, and the urgency of the request. Authorized ICE dissemination officials are listed in Section 4, Responsibilities, of this Directive. (See Section 4.7, 4.8, and 4.9.)

5) The ICE directorate or program office will notify the respective HSI attachés of any requests from and/or dissemination to their foreign area of responsibility regarding the disclosure of FOUO–LES information.

6) All foreign government requests for disclosure of FOUO–LES information received by ICE must be forwarded to the appropriate directorate or program office official(s) designated in Section 4 of this Directive. All requests except information originating within ERO for the purpose of procuring travel documents must be coordinated through HSI OIA before release.

7) A cover letter should accompany the exchange of information to foreign governments and international organizations, stating that the records are furnished under the conditions that the information will be used only for the purpose stated in the request; the foreign government must obtain ICE's express written permission for any future or subsequent use(s) of the records beyond the purposes stated in the request; the information will not be released to third parties without ICE's express written permission; and, in the event of any unauthorized release, the government or organization will notify ICE, intercede on ICE's behalf, and assume responsibility for any and all expenses, costs, or liabilities arising therefrom where possible.

8) Documents released to foreign governments or international organizations must be clearly marked to indicate the purpose for which they are being disclosed. Additional guidance on marking of documents released to foreign governments or international organizations is contained in Section 5.5., Marking LES Information, of this document.

5.9. Transmission (Domestic and Foreign).

1) Transmission of FOUO–LES information within the United States and its commonwealths, territories, and possessions:

   a) Transmittal via Hardcopy. When forwarding FOUO–LES information, an FOUO cover sheet should be placed on top of the transmittal letter, memorandum, or document. FOUO–LES information may be mailed within the United States and its territories via regular U.S. Postal Service, using a method where the mail can be tracked and delivery confirmed (i.e., certified mail, delivery confirmation, signature confirmation, express mail, express mail international, priority mail with delivery confirmation, priority mail international with delivery confirmation, registered mail, and global express guaranteed). Any other accountable commercial delivery service that provides tracking and delivery confirmation, such as Federal Express and United Parcel Service, may also be used. Material shall be packaged in accordance with DHS MD 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only Information)," dated January 6, 2005, or as updated, before being introduced into the mailing system;
   b) Transmittal via Fax. Unless otherwise restricted by the originating office, FOUO–LES information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originating office;
   c) Transmittal via eMail. FOUO–LES information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO–LES information may be transmitted over regular U.S. Government email channels. Per DHS 4300A, "Sensitive Systems Handbook," dated January 20, 2011, or as updated, due to inherent vulnerabilities, FOUO–LES information shall not be sent to personal email accounts. For FOUO–LES information that is also Sensitive PII, DHS guidance requires that the information be encrypted if sent to an email address outside the dhs.gov domain. For added security, when transmitting FOUO–LES information over a regular email channel, the information may be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO–LES information must comply with any email restrictions imposed by the originating office;

d) Internet and DHS or ICE Intranet. FOUO–LES information may not be posted on a DHS or any other Internet (public) Web site. FOUO–LES information may be posted on the ICE secure (unclassified) intranet or other government-controlled or -sponsored protected encrypted data networks, such as the Homeland Security Information Network. However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine whether the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked FOUO–LES; and the information posted does not violate any provisions of the Privacy Act; and

e) Public Domain. Personnel may not use any unauthorized system to access, download, or attempt to download from a public Web site any information that is believed to be FOUO–LES, nor may they comment on or confirm the degree of sensitivity of such information, or discuss the content with persons who would not otherwise be authorized access. (See DHS Employee Communications, Message from Chief Security Officer, Jerry Williams: "Security Reminder," dated August 13, 2010).

2) Transmission of hardcopy FOUO–LES information outside the United States and its commonwealths, territories, and possessions:

a) the originating ICE directorate or program office must coordinate with HSI OIA to ensure that the appropriate written request or appropriate agreements are in place before any international transmission of FOUO–LES information; and

b) transmission to offices in foreign locations: Transmission to an office in a foreign country shall be in accordance with DHS MD 11402.1, "Safeguarding Sensitive But Unclassified (For Official Use Only Information)," dated January 6, 2005, or as updated.

3) Network connectivity. DHS Directive 4300B, "National Security Systems Policy Directive," establishes DHS policy for network connectivity. The section of the aforementioned document on network connectivity states that:

a) components shall ensure that appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every network component;

b) interconnections between classified information technology (IT) systems and IT systems not controlled by DHS shall be established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of the information on the network;

c) components shall document interconnections with other external networks with an ISA. Interconnections between DHS components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both Designated

Approval Authorities (DAAs) or by the official designated by the DAA to have signatory authority;

d) ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems;
e) ISAs shall be reviewed as part of the annual Federal Information Security Management Act self-assessment; and
f) if the requirements stated above cannot be met or the connection was in place before the stated requirements, waivers and/or exceptions can be requested through the ICE Chief Information Security Officer. The Waivers and Exceptions Request Form, which is located in the DHS 4300B National Security Systems Handbook, shall be used.

Interconnections between DHS and non-DHS IT systems must use an ISA, primarily because the two agencies may be using different security policies. Generally, it is preferable that an approved ISAA is in place before the ISA.

Connections between DHS components may require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems.

4) Network connectivity outside the United States and its commonwealths, territories, and possessions. In addition to the requirements outlined in Subsection 5.10(3), where required or appropriate, all communications outside of the United States and its commonwealths, territories, and possessions shall be in accordance with the U.S. Department of State Foreign Affairs Manual (FAM), 12 FAM 600, "Information Security Technology."

The appropriate ICE directorate or program office must coordinate with HSI OIA to ensure that the appropriate agreements are in place before any international network connectivity or transmission of FOUO–LES information.

5.10. General Handling Procedures.

Although FOUO–LES is the DHS standard caveat for identifying Sensitive But Unclassified information, some types of FOUO–LES information may be more sensitive than others and thus warrant additional safeguarding measures beyond the requirements established in this Directive. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could include loss of life or the compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. ICE employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly. When documents contain Sensitive PII, employees should consult the DHS Handbook,

"Handbook for Safeguarding Sensitive Personally Identifiable Information," dated January 19, 2011, or as updated, for proper handling, retention, disclosure, and disposal requirements.

1) When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal FOUO–LES information to unauthorized persons, a "FOR OFFICIAL USE ONLY" cover sheet (see DHS MD 11042.1) must be used to prevent unauthorized or inadvertent disclosure.

2) Received FOUO-equivalent information from another government agency should be handled in accordance with the guidance provided by the other government agency. Where no guidance is provided, such information should be handled in accordance with the requirements of this Directive.

5.11. Storage.

1) When unattended, FOUO–LES information must be, at a minimum, stored in a locked file cabinet, a locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials may also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know. This storage area can be a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

2) FOUO–LES information will not be stored in the same container used for storage of classified information unless there is a correlation between the information. If there is a correlation of information, and the FOUO–LES information are stored in the same container used for the storage of classified materials, such FOUO–LES documents/information will be segregated from the classified materials to the greatest extent possible, i.e., separate folders, separate drawers, etc.

3) IT systems that store FOUO–LES information must be certified and accredited for operation in accordance with federal and ICE standards. DHS Handbook 4300A, "DHS Sensitive Systems Handbook," dated January 20, 2011, or as updated, should be consulted for more detailed information.

4) Laptop computers and other media containing FOUO–LES information must be stored and protected to prevent loss, theft, unauthorized access, and unauthorized disclosure. Storage and control will be in accordance with DHS Handbook 4300A, "DHS Sensitive Systems Handbook," dated January 20, 2011, or as updated.

5.12. Destruction.

FOUO–LES information must be destroyed when no longer needed or required by record retention schedules or litigation holds. Destruction may be accomplished as follows:

1) Hardcopy materials will be destroyed by shredding, burning, pulping, or pulverizing so as to ensure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

2) Electronic storage media shall be wiped/erased and rendered inaccessible by destruction of the media in accordance with established DHS procedures. Local IT personnel should be contacted for additional guidance.

3) Paper products containing FOUO–LES information ~~will~~ may not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

5.13. Incident Reporting.

1) The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO–LES information must be reported no more than 24 hours after the incident as follows:

   a) computer/information security—contact the ICE Service Desk and/or ICE Security Operations Center (SOC)/ ICE Computer Security Incident Response Center (CSIRC);
   b) privacy and Sensitive PII—contact the ICE Service Desk and/or ICE SOC/ICE CSIRC; and
   c) security and information assurance—contact the ICE Information Assurance Division and the Office of Professional Responsibility Security Management Unit.

2) Suspicious or inappropriate requests for information by any means—e.g., email, or oral—shall be reported to icecounterintelligence@ice.dhs.gov.

3) Should the possibility of disclosure or compromise result in physical harm to an individual(s) or compromise of a planned or ongoing operation, immediate notification must be made without delay to the ICE Joint Intelligence Operations Center.

6. Recordkeeping. Records documenting the disclosure of FOUO–LES information will be kept as described in Sections 5.6, 5.10, and 5.12.

7. Authorities/References. (Authorities/references are as dated or as updated.)

7.1. Homeland Security Act of 2002, Public Law 107–296 (including, in particular, § 891).

7.2. 5 U.S.C. § 552, The Freedom of Information Act.

7.3. 5 U.S.C. § 552a, Privacy Act of 1974.

7.4. 6 U.S.C. § 485(a)(5) (section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004), information sharing; "terrorism information" defined.

7.5. 18 U.S.C. § 11, "foreign government" defined.

7.6. 19 U.S.C. § 1628, exchange of information.

7.7. 22 U.S.C. § 288, "international organization" defined.

7.8. 6 C.F.R. § 29.2(g), "protected critical infrastructure information" defined.

7.9. 19 C.F.R. § 103.33, availability of information, release of information to foreign agencies.

7.10. Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," dated October 25, 2005.

7.11. Executive Order 13526, "Classified National Security Information," dated December 29, 2009.

7.12. Executive Order 13556, "Controlled Unclassified Information," dated November 4, 2010.

7.13. DHS MD 11042.1, "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated January 6, 2005.

7.14. DHS handbook 4300A, entitled "DHS Sensitive Systems Handbook," dated January 20, 2011.

7.15. DHS Policy Directive 4300B, entitled "National Security Systems Policy," dated July 26, 2010.

7.16. DHS memorandum to Secretary Chertoff, Secretary of Homeland Security, from Under Secretary for Policy and International Relations, Assistant Secretary for Intelligence and Analysis, Director of Operations, and Chief Information Officer, entitled "Information Sharing at the Department of Homeland Security," dated December 16, 2005.

7.17. DHS memorandum to all DHS components from Secretary Michael Chertoff, entitled "DHS Policy for Internal Information Exchange and Sharing," dated February 1, 2007.

7.18. DHS memorandum signed by Charles E. Allen, DHS, Under Secretary for Intelligence and Analysis, Chair Information Sharing Governance Board, "Policy Guidance: Implementation of the One DHS Information Sharing Memorandum," dated February 6, 2008.

7.19. DHS MD 0450.1, entitled "Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)," dated January 24, 2003.

7.20. DHS Delegation 7030.2, entitled "Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement," dated November 13, 2004.

7.21. DHS employee communications, message from Chief Security Officer, Jerry Williams, entitled "Security Reminder," dated August 13, 2010.

7.22. DHS Privacy Policy Guidance Memorandum 2007–01, entitled "Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons," dated January 19, 2007, as amended January 7, 2009.

7.23. DHS handbook, entitled "Handbook for Safeguarding Sensitive Personally Identifiable Information (PII)," dated January 19, 2011.

7.24. ICE Delegation Order 4001.1, entitled "Authority to Exchange Information or Documents with Foreign Customs and Law Enforcement Agencies," dated March 12, 2009.

7.25. ICE Directive 17002.1 (formerly U.S. ICE Directive 6–7.0), "ICE Personnel Security and Suitability Program," dated February 4, 2008.

7.26. ICE Directive 17003.1 (formerly U.S. ICE Directive 6–8.0), "ICE Suitability and Screening Requirements for Contractor Personnel," dated May 29, 2008.

7.27. ICE Privacy Guidance, "Requests for Information Under Section (b)(7) of the Privacy Act," dated August 13, 2010.

8. **Attachments.** None.

9. **No Private Right.** These guidelines and priorities are not intended to, do not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter against the United States; its Departments, Agencies, or other entities; its officers or employees; and/or contractors or any other person.

(b)(6); (b)(7)(C)

Thomas S. Winkowski
Principal Deputy Assistant Secretary
U.S. Immigration and Customs Enforcement