MEMORANDUM OF AGREEMENT

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY

AND

THE NATIONAL COUNTERTERRORISM CENTER

REGARDING

ADVANCE PASSENGER INFORMATION SYSTEM DATA

1. INTRODUCTION AND PURPOSE.

The United States Department of Homeland Security (DHS), acting through the Office of Intelligence and Analysis (I&A) and U.S. Customs and Border Protection (CBP), and the National Counterterrorism Center (NCTC), hereinafter collectively referenced as the "Parties," have entered into this Memorandum of Agreement ("MOA" or "Agreement") to govern the sharing, use and safeguarding of data contained within the Advance Passenger Information System (APIS) for the purpose of identifying information within APIS as Terrorism Information. The Parties agree that this MOA constitutes the for Terms and Conditions required by the United States Attorney General Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information (March 22, 2012) for the sharing of APIS Data.

2. BACKGROUND.

A. NCTC.

Pursuant to the National Security Act of 1947, as amended, NCTC "serve[s] as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." 50 U.S.C. § 404o. In order to enhance information sharing, the President issued Executive Order No. 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (Oct. 27, 2005), which provides that the head of each agency that possesses or acquires Terrorism Information will promptly give access to that information to the head of each other agency that has counterterrorism functions.

The Directorate of Operations Support (DOS) at NCTC is responsible for providing the counterterrorism community with 24/7 counterterrorism intelligence monitoring, assessment and notification support. The DOS provides situational awareness, terrorism threat reporting and management, and incident information tracking. The DOS conducts immediate analysis of active threat streams 24/7.

The DOS will also have access to APIS Records in the Counterterrorism Data Layer (CTDL) to support requirements to vet names based on new threat information provided to NCTC [redacted], which enhances the counterterrorism community's awareness of emergent terrorist threats. APIS data that constitutes terrorism information will be used in internal NCTC products and will not be coordinated prior to internal dissemination; NCTC will coordinate finished intelligence with DHS NOC prior to dissemination, to the extent such product includes APIS data.

The Directorate of Intelligence (DI) at NCTC is the designated lead within the IC for all-source counterterrorism analysis and data integration. The DI will have access to APIS Records in the CTDL to support review of emerging terrorist threat information. If a connection is found between APIS Data and information regarding an emerging terrorist threat, the APIS Data, compiled with other analysis, could be used by the DI in finished intelligence disseminated to IC partners as part of an ongoing effort to determine the extent and severity of the threat. The DI will use the APIS Data in coordination with various types of [redacted] data derived from multiple government sources to discover leads to terrorism and [redacted]. The DI is focused on supporting operators in the IC with tactical intelligence, to include operational leads of possible terrorists or violent extremists [redacted], and will use APIS Data to identify [redacted] of terrorists, assemble additional details on known or suspected terrorists, and include the information in leads passed to DHS and other partners [redacted].

The Directorate of Terrorist Identities (DTI) maintains the Terrorist Identities Datamart Environment (TIDE). TIDE serves as the central knowledge bank for all-source information on international terrorist identities for use by the IC, the law enforcement community, and others. DTI analysts will work with partners to enhance TIDE records with [redacted] to support [redacted] analysis and [redacted] activities. This includes supporting watchlisting and providing data to the Terrorist Screening Center to [redacted]. The DTI receives information from across the IC. Any indication that a TIDE-listed person has [redacted], and DTI needs access to the full APIS Record to ensure that sourcing is correct, all appropriate information is utilized, and to identify and handle correctly United States Person information. The DTI's efforts to utilize data for TIDE enhancement still require DHS to fulfill its responsibilities under the interagency Watchlisting Guidance.

The DTI also engages in select searches through external databases, if applicable. However, these searches are done only after DTI determines that a record of interest constitutes Terrorism Information either to [redacted] or [redacted].

B. THE APIS DATABASE.

The Aviation and Transportation Security Act of 2001, as amended, and the Enhanced Border Security and Visa Entry Reform Act of 2002 provide specific authority for the

mandatory collection of certain information on all passengers and crewmembers that arrive in, depart from (and, in the case of aviation crew, fly over) the United States via private and commercial aircraft and commercial vessels. CBP uses the information to identify those travelers who may pose a risk to border, transportation, or public security; may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists; may be inadmissible; may be a person of interest; or may otherwise be engaged in activity in violation of U.S. law; or are the subject of wants or warrants.

The APIS system is described in a published Privacy Act System of Record Notice (SORN) entitled "Customs and Border Protection Advanced Passenger Information System" and dated November 18, 2008. The SORN lists routine uses of the records maintained in APIS, including, under Routine Use J, the following:

> To Federal and foreign government intelligence or counterterrorism agencies or components where DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

73 Fed. Reg. 68,435, 68,438 (Nov. 18, 2008).

Specifically, APIS Data is being provided to NCTC to assist in both Parties' counterterrorism efforts.

3. DEFINITIONS.

As used in this Agreement, the following terms will have the following meanings:

A. Alien: Any person not a citizen or national of the United States.

B. Asylum and Refugee Information: Any information pertaining to any asylum or refugee application or status the confidentiality of which is protected by 8 C.F.R. § 208.6 (asylum) and policy (refugee), [redacted]

C. APIS Data: Biographic data and other travel itinerary information on passengers and crewmembers for all commercial air, commercial vessels, and all private aircraft, arriving in and departing from (and, in the case of aviation crew, flying over) the United States.

D. APIS Record: APIS Data associated with an individual, as specifically mandated by applicable regulations.

E. Counterterrorism Data Layer (CTDL): NCTC's data holdings from external providers and internal analytic operations, which houses [redacted]. Within the CTDL, data goes through

extract, transform, and load (ETL) processes and is standardized for analytical consumption [redacted] and [redacted]. The CTDL then exposes the data to a variety of analytic and search tools, using role-based access control.

F. Lawful Permanent Resident (LPR): An Alien who has obtained the "status of having been lawfully accorded the privilege of residing permanently in the United States, as an immigrant in accordance with the immigration laws, such status not having changed." 8 U.S.C. § 1101(a)(20).

G. Personally Identifiable Information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual. This applies regardless of whether the individual is a United States citizen, Lawful Permanent Resident, or visitor to the United States.

H. Special Protected Classes: Classes of Aliens for which there are additional statutory, regulatory, or policy protections. Data pertaining to these classes of Aliens may have handling or use requirements different from United States Person information or other Alien data. The classes of Aliens covered under this definition include Asylum-Seekers; Asylees; Refugees; S, T, and U visa holders; individuals covered by the protections of the Violence Against Women Act (VAWA); Aliens with Temporary Protected Status; Legalization and Seasonal Agricultural Worker program applicants; and other individuals.

I. Terrorism Information: All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (1) the existence, organization, capabilities, plan, 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, United States persons, or United States 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 includes Weapons of Mass Destruction Information.

J. United States Person: A United States citizen, an Alien known by the intelligence element concerned to be a Lawful Permanent Resident, an unincorporated association substantially composed of United States citizens or Lawful Permanent Residents, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

4. REFERENCES.

The information sharing and enhanced cooperation among the Parties to this Agreement is authorized under, and complies with the provisions of:

A. Title 5, United States Code, Section 552a;

B. Title 6, United States Code, Sections 112, 121, and 485;

C. Title 8, United States Code, Sections 1103, 1221, 1365a, 1365a note, 1365b, 1379;

D. Title 19, United States Code, Section 1433;

E. Title 49, United States Code, Section 44909;

F. Title 50, United States Code, Sections 404o, 404o note, 501 note;

G. Executive Order No. 12333, United States Intelligence Activities, as amended;

H. Executive Order No. 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans (Oct. 25, 2005);

I. Homeland Security Presidential Directive-2, Combating Terrorism Through Immigration Policies (Oct. 29, 2001);

J. Homeland Security Presidential Directive-6, Integration and Use of Screening Information (Sept. 16, 2003);

K. Homeland Security Presidential Directive-11, Comprehensive Terrorist-Related Screening Procedures (Aug. 27, 2004);

L. Title 19, Code of Federal Regulations, Sections 4.7b, 122.22, 122.49a-122.49c, 122.75a-122.75b;

M. Intelligence Community Directive 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation (Sept. 15, 2008);

N. National Institute for Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations (Aug. 2009), as revised;

O. NCTC Knowledge Repository System of Records Notice (ODNI/NCTC-004), 76 Fed. Reg. 42747 (July 19, 2011);

P. United States Attorney General, Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information (March 22, 2012); (the "2012 NCTC Guidelines".

Q. Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), as amended;

R. Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (as amended Jan. 18, 2007);

S. Office of the Director of National Intelligence Instruction 80.02, Managing Breaches of Personally Identifiable Information (Feb. 20, 2008);

T. Office of the Director of National Intelligence Instruction No. 80.05, Implementation of Privacy Guidelines for Sharing Protected Information (Sept. 2, 2009);

U. Office of the Director of National Intelligence Instruction 80.13 (2006-3). Protection of Privacy and Civil Liberties (Feb. 27, 2006);

V. Memorandum from Secretary Chertoff, Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies (Apr. 18, 2007);

W. Memorandum from Secretary Napolitano, Disclosure of Asylum and Refugee-Related Information to U.S. Intelligence and Counterterrorism Agencies Pursuant to 8 C.F.R. § 208.6 Addendum to 2007 Secretary Chertoff Memo (Aug. 25, 2011);

X. Memorandum from Secretary Napolitano, Policy Statement Regarding the Disclosure of Asylum and Refugee-Related Information to United States Intelligence and Counterterrorism Agencies ([Date TBD]);

Y. DHS Privacy Policy Guidance Memorandum No. 2007-1, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons (as amended Jan. 19, 2007);

Z. DHS Memorandum No. 2009-01, The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy (June 5, 2009);

AA. Notice of Privacy Act System of Records, Customs and Border Protection Advance Passenger Information System, Fed. Reg. 68435 (Nov. 18, 2008); and

BB. Watchlisting Guidance (March 2013).

5. RESPONSIBILITIES.

The following roles and responsibilities have been defined for each of the Parties to this MOA.

A. DATA SENSITIVITY.

DHS considers the APIS Data provided to NCTC as "Unclassified" and "For Official Use Only." Specific technical and security details are set forth in Section 5 of this Agreement.

DHS will provide available APIS Data to NCTC as described within this MOA in accordance with DHS policies and procedures concerning the handling of sensitive information, including, as appropriate, applicable rules governing the safeguarding of sensitive unclassified information and classified national security information. NCTC will provide data and other responsive information back to DHS under this MOA in accordance with its policies and procedures concerning the handling of sensitive information, including, as appropriate, applicable rules governing the safeguarding of sensitive unclassified information and classified national security information. The fact of classification, alone, will not be a prohibition upon sharing with appropriately cleared DHS personnel.

B. DELIVERY OF DATA.

Data Set: DHS will deliver appropriate APIS Data, as identified in Appendix A, along with [redacted]

Modification of Data Set: Under the terms of this MOA, at any time, NCTC may, through the APIS Points of Contact (POCs) listed in this MOA, request that additional APIS Data elements be added to the list in Appendix A. Upon such request DHS will consider sharing additional APIS Data elements with NCTC, through appropriate internal DHS processes, to include CBP, the Office of the General Counsel, Privacy Office and Office for Civil Rights and Civil Liberties. If DHS consents to add additional data elements to the scope of this MOA, Appendix A will be amended accordingly.

Delivery Method: DHS will deliver APIS Data to NCTC pursuant to and in accordance with the terms of this MOA via [redacted] strong privacy protections and information security standards as agreed to by the Parties. NCTC will securely maintain APIS Data received from DHS. [redacted]

Regular/Periodic Updates: [redacted], as agreed under this MOA.

Ad Hoc Requests for Additional Information: In instances where NCTC analysts identify information within the dataset as Terrorism Information, NCTC may request additional data elements maintained in the relevant APIS Record. For enhancing TIDE records, upon request, [redacted]

[redacted]

Support: DHS, through CBP, will regularly provide NCTC with successor data to APIS Data should the format of data collection be changed or modified, provided such transmission continues to be authorized by law and regulation and is otherwise consistent with the data elements identified in Appendix A.

Technical Updates: DHS will provide NCTC with new deliveries of data [redacted]. The Parties have initiated discussions to [redacted]

Special Class Restrictions: APIS information and other APIS-related data pertaining to individuals in Special Protected Classes, including individuals covered by the protections of 8 U.S.C. § 1367 (VAWA, "T" and "U" visa applicants and beneficiaries), may be provided to NCTC under this Agreement only when authorized and not otherwise prohibited by statute.

United States Person Information: Any APIS Record or information for which there is a reasonable belief that the record refers to a United States Person will be treated by NCTC in accordance with applicable provisions of the Privacy Act and Executive Order No. 12333, consistent with NCTC's responsibilities reflected in section 5.E. of this MOA, provided that notice of such status is provided to NCTC by DHS where the identification of the record as being associated with a United States Person is made by DHS. NCTC may not use or otherwise take action regarding those records in a manner that would violate relevant provisions of the Privacy Act, Executive Order No. 12333, or any of its responsibilities under Section 5 of this MOA.

C. TREATMENT AND RETENTION OF RECORDS.

Having reviewed all applicable statutes, executive orders, regulations, agreements, all applicable Privacy Act System of Records Notices, and other binding instruments relevant to this dataset, the data provider has determined that there is no requirement that would prohibit NCTC from temporarily retaining this data for up to one year, provided the retention is limited to the uses and subject to the safeguards described in this MOA.

When NCTC replicates APIS Data, it will be marked with a "time-to-live" date, which will specify when the APIS Data will be deleted if it is not identified as Terrorism Information. NCTC will purge all APIS Data not determined to constitute Terrorism

Information no later than one year from receipt of the record from DHS.[1] This process will be audited as required in Section 5.N of this Agreement. NCTC may retain beyond one year APIS Data it has determined to constitute Terrorism Information in accordance with procedures approved for NCTC by the Attorney General pursuant to Section 2.3 of Executive Order No. 12333 and the terms and conditions specified in this Agreement; specifically, through human review by an NCTC analyst utilizing APIS Data loaded into the CTDL consistent with the strategic analytic uses of APIS Data outlined in Section 5.D of this Agreement.

All APIS information retained as Terrorism Information as identified via the processes above will be appropriately marked as Terrorism Information and shared with the parties identified within sections E and F of this Agreement and other departments and agencies with counterterrorism responsibilities, as appropriate.

D. USE.

A material condition for the sharing by NCTC and DHS of APIS Data is real and ongoing value to both NCTC's and DHS's operational missions.

NCTC may use any APIS Record its analysts identify as containing Terrorism Information in any manner consistent with its authorities and in accordance with applicable policies and procedures, including those reflected elsewhere in this MOA. With respect to APIS Data received by NCTC under this MOA that does not constitute Terrorism Information, NCTC may only use such information for the purposes authorized by this MOA. This MOA does not alter or impair the right of DHS to use any information subject to this MOA in support of its lawful mission in accordance with its statutory and executive authorities.

NCTC's DOS, DI, and DTI will analyze APIS Records in conjunction with other data it holds to determine if those APIS Records constitute Terrorism Information, in which case NCTC will retain the data pursuant to its authorities, as described in Section 5.C of this Agreement.

Directorate of Operations Support:

The DOS is responsible for providing the counterterrorism community with 24/7 counterterrorism intelligence monitoring, assessment and notification support. All DOS watch officers require access to the data because they rotate shifts. The watch officers will search all NCTC data holdings (to include APIS Data provided under this MOA) for information that can further enhance knowledge of terrorism threat and [redacted] in order to conduct immediate analysis of active threat streams 24/7. The DOS will have access to APIS Records in the Counterterrorism Data Layer (CTDL) to support

[1] Section III.C.3(c) of the 2012 NCTC Guidelines (Reference P), specifies the temporary retention period commences when the data is made generally available for access and use following both the determination period discussed in section III.C.3(b) and any necessary testing and formatting. For the purposes of this Agreement, the Parties agree the temporary retention period will begin on the day after receipt of each data delivery.

requirements to vet names daily based on new threat information provided to NCTC, thereby enhancing the counterterrorism community's awareness of emergent terrorist threats. APIS data that constitutes terrorism information will be used in internal NCTC products and will not be coordinated prior to internal dissemination; DOS will coordinate with DHS, as appropriate, in the event and external product contains APIS data.

Directorate of Intelligence (DI):

The DI at NCTC is the designated lead within the IC for all-source counterterrorism analysis and data integration. DI analysts in strategic counterterrorism and analysis and targeting terrorists will have access to APIS Records in the CTDL and will search NCTC data holdings, to include APIS Records, for connections to terrorism. In addition, the DI analysts will also use [redacted] of terrorism information based on new threat-based information in order to detect and prevent emergent terrorist threats. The DI will use the APIS Records [redacted] to discover leads to terrorism and [redacted].

The DI is focused on supporting operators in the IC with tactical intelligence, to include operational leads of possible terrorists [redacted], and will use APIS Data to identify [redacted], glean additional details on known or suspected terrorists, and include the information in leads passed to DHS and other partners [redacted]. APIS Data that constitutes Terrorism Information, compiled with other analysis, could be used by the DI in finished intelligence disseminated to IC partners as part of an ongoing effort to determine the extent and severity of the threat.

NCTC will use the APIS Data to determine any corollary between [redacted], which could lead to the identification of Terrorism Information. Any dissemination of APIS Data will be as part of an analytic product provided to IC partners and CBP.

Directorate of Terrorist Identities (DTI):

The DTI maintains TIDE. DTI Analysts will search on NCTC data holdings (to include APIS Data provided under this MOA) for information that can further enhance knowledge of known or suspected terrorists. DTI Analysts will primarily search the NCTC data holdings to identify correlations with Terrorism Information. Terrorist Identity Analysts will access NCTC data holdings should they have a question concerning the Analytic Methodologist's findings. Both will work to enhance TIDE records with biographic data and verification of fragmentary nominations [redacted] correlated with Terrorism Information. This includes supporting watchlisting and providing data to the Terrorist Screening Center for [redacted] DTI analysts involved in supporting screening missions will search NCTC data holdings, to include APIS Data, for connections to specific terrorism threat information NCTC has identified and prioritized.

Responsibility to Nominate:

NCTC/DTI's efforts to utilize data for TIDE enhancement still require DHS to fulfill its responsibilities, under the interagency Watchlisting Guidance, to nominate new data in the standard nomination format.

E. NOTIFICATION, MARKING, AND COORDINATION REQUIREMENTS.

Records of Transfer: Each Party agrees to maintain a log of all information received from and sent to the other Party, including names of recipients and senders, as well as the date and method of transfer.

Marking of APIS Data: NCTC will appropriately mark the origin of APIS Data received under this MOA as derived from "CBP APIS" when entered into intelligence reports, TIDE, or other authorized reports or databases unless [redacted] If it is necessary to identify Asylum and Refugee Information and/or the Refugee Travel Document with more specificity, reference to asylum and/or refugee status may be made. Regardless of how reference to Asylum and Refugee Information is made, in no instance may it be disseminated to any foreign government agency, official, representative, employee, agent, or contractor without the specific authorization of the Secretary, Deputy Secretary, or other DHS official to whom disclosure authority under 8 C.F.R. § 208.6(a) has been delegated.

Feedback to DHS: Upon identification of APIS Data that constitutes Terrorism Information, NCTC will coordinate with DHS by including the [redacted] on the distribution of the lead or finished intelligence product. If the identification does not result in the distribution of a lead or finished intelligence product, NCTC will otherwise notify, in a timely manner, [redacted] The DTI will provide the [redacted] feedback on any DHS information correlated to a TIDE record.

F. DISSEMINATION[2].

Terrorism Information: NCTC may disseminate APIS Data identified as Terrorism Information consistent with its authorities, without the need for DHS approval, provided

[2] Section IV.B.2 of the 2012 NCTC Guidelines (Reference P), provides for "Dissemination for Limited Purposes," Section IV.B for "Dissemination of United States Person Information Acquired Under Tracks 1, 2, or 3," Section IV.C for "Dissemination of United States Person Information Acquired Under Track 3" and Section IV.E for "Foreign Disseminations." For the purposes of this Agreement, the Parties agree that dissemination will be further limited according to the terms of Section 5.F.

such dissemination is to other appropriate United States Government authorities and for counterterrorism purposes. Such dissemination will include notification, that the recipient U.S. government authority may not disseminate APIS Data derived from records [redacted] to any foreign government agency, official, representative, employee, agent, or contractor without the specific authorization of the Secretary, Deputy Secretary, or other DHS official to whom disclosure authority under 8 C.F.R. § 208.6(a) has been delegated. (Contact DHS Intelligence and Analysis Single Point of Service to request authorization for such dissemination).
NCTC will maintain a copy of the information that was disseminated, to whom, and the purpose for the dissemination in accordance with applicable audit requirements pursuant to Section 5.N of this Agreement.

Other Information: NCTC will not share APIS Data that has not been identified as Terrorism Information in accordance with the provisions of Section 5.C of this Agreement. If there is a question on APIS Data and its relationship to terrorism, NCTC may request in writing that DHS allow the provision of that information to third parties for further judgment. Upon such a request, DHS will respond to NCTC within [redacted]

G. CONTROL OF RECORDS.

Until such time as APIS Data has been determined to constitute Terrorism Information in accordance with Section 5.C of this Agreement, DHS/CBP will be deemed to have retained control of APIS Data provided to NCTC under this MOA for the purposes of addressing any requests for information made under the Freedom of Information Act (FOIA), the Privacy Act, or as part of or in support of any other legal proceeding. The Parties agree that any documents or records based upon or incorporating information provided pursuant to this Agreement (including under FOIA, Privacy Act or any legal or administrative proceeding) will be coordinated with the other Party prior to release.

H. SAFEGUARDS.

The Parties agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the information shared under this Agreement against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification or deletion. Neither Party will use data provided to it under this MOA in affidavits, subpoenas, or submissions in legal, judicial, or administrative proceedings unless authorized by the providing Party or required by law (in which case the Party required to provide such data will coordinate its provision of the data with the providing Party).

In addition to the reporting and coordination requirements specified in other sections of this MOA, NCTC will report to the data provider any significant failure to comply with: (i) the 2012 NCTC Guidelines (Reference P); (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) these Terms and Conditions (2012 NCTC Guidelines, section VI.D(1)). A "significant failure" is defined in Section IV.D.1.ii of the 2012 NCTC Guidelines (Reference P).

In the event of such significant failure or failure to meet the terms and conditions of this Agreement, including the oversight requirements in Appendix B, NCTC will notify, in writing, the designated DHS point of contact and the DHS oversight official assigned to NCTC pursuant to Section 5.P of this Agreement.

I. TRAINING.

Completion of training on privacy and APIS information, as outlined below, is a requirement for NCTC staff to receive and maintain access to APIS. The Parties will be appropriately trained regarding the proper treatment of PII and proper care of the information systems used to ensure the overall safeguarding of the information in addition to applicable rules and conditions concerning United States Person information. Each Party will ensure that its employees, including contractors with access to any of the other Party's data, have completed privacy training on the handling of PII.

DHS/CBP will provide annual and periodic training requirements to appropriate NCTC personnel on the proper interpretation of APIS Data and on proper treatment of information regarding Special Protected Classes. NCTC staff must complete the training within one year of its implementation or they will lose access to APIS Data until such time as they have completed the training. NCTC staff with access to APIS Data will complete refresher training on APIS, Special Protected Classes, and United States Person information on an annual basis to retain access to APIS Data.

J. PRIVACY AND CIVIL LIBERTIES.

General Protections and Public Notice: The Parties are members of the Information Sharing Environment. Each Party will conduct its activities under this MOA in accordance with its own Information Sharing Exchange Privacy and Civil Liberties Protection Policy. Each Party will provide appropriate notice to the public regarding the existence and contents of this Agreement, including through the creation and release to the public of Privacy Impact Assessments (PIAs). The Parties will jointly develop a PIA discussing the overarching bulk information sharing relationship between DHS and NCTC no later than one year from the date of enactment of this Agreement. DHS will provide appropriate expertise and human resources to facilitate the drafting of the joint PIA, and NCTC will provide resources to support coordination of the joint PIA within NCTC. The Parties will cooperate with each other in this regard, which may include (but is not limited to) providing joint presentations regarding this Agreement to Congress and the DHS Data Privacy and Integrity Advisory Committee.

Treatment of APIS Data Under the Privacy Act: Until such time as APIS Data has been determined to constitute Terrorism Information in accordance with Section 5.C of this Agreement, the collection, use, disclosure, and retention of PII will be limited by the terms and conditions set forth in this MOA, notwithstanding any routine uses for disclosures of information under NCTC's Knowledge Repository Privacy Act SORN (ODNI/NCTC-004). Any APIS Data determined to constitute Terrorism Information in

accordance with Section 5.C of this Agreement will be maintained, shared, used, and disclosed in accordance with NCTC's SORN (ODNI/NCTC-004), except as limited by Sections 5.D and 5.F of this Agreement.

PII will be protected by administrative, technical and physical safeguards appropriate to the sensitivity of the information. PII will only be disclosed to authorized individuals with a need to know and only for uses that are consistent with the stated purposes under this MOA and for which the information was originally collected. NCTC is the responsible agency for purposes of the Privacy Act concerning any violation of applicable Privacy Act provisions resulting from NCTC's treatment, handling, dissemination, and/or use of APIS Data provided under this MOA.

K. CORRECTION AND REDRESS.

PII shared and maintained under this Agreement will, to the extent feasible, be as accurate, complete, and up-to-date as necessary for the purposes identified in this Agreement. The Parties will cooperate with each other in this regard. NCTC will, in a timely manner, take appropriate action with regard to any request made by DHS for additions, changes, deletions, or corrections of PII. In addition, NCTC will, in a timely manner, notify DHS of any data errors that it discovers.

NCTC will maintain an ability to locate and update specific DHS records identified by DHS as requiring correction. Additionally, NCTC will correct any disseminated information based on DHS data that is later deemed to be erroneous. Location and correction of records will be accomplished in not more than fourteen calendar days and NCTC will provide written confirmation to DHS of the corrections made.

No later than ninety days from the execution of this Agreement, NCTC will document and establish a redress mechanism for individuals whose PII has been obtained by NCTC pursuant to this Agreement and retained as Terrorism Information in accordance with Section 5.C of this Agreement. This redress process will direct any requests for correction of or redress regarding those records to DHS for resolution, as appropriate. For any records corrected by DHS through this process, NCTC will correct such records in its possession upon receipt of notification of correction from DHS.

L. COOPERATION/DECONFLICTION.

The Parties will work together to the greatest extent possible to achieve the maximum preventative, preemptive, and disruptive effect on potential threats, including coordinating simultaneous and complementary activities when appropriate. The Parties further agree to coordinate operational activities to the greatest possible extent when based upon the information exchanged pursuant to this MOA. Specifically, each Party will take all reasonable steps to ensure coordination and de-confliction of homeland security-related law enforcement or intelligence activities, or other activities under its authority, with such activities of the other Party.

Where the Parties have a mutual interest based on information shared pursuant to this Agreement, the Parties will coordinate with each other to determine the appropriate course of action. In such matters, unless there are exigent circumstances requiring immediate action, NCTC will verify information and coordinate with DHS before taking action on leads or disseminating intelligence products developed as a result of information shared pursuant to this Agreement. In the event of exigent circumstances, NCTC will notify the designated DHS representative as soon as possible and no longer than 24 hours after taking the action.

M. REPORTING AND COMPLIANCE.

Each organization will report privacy or security incidents in accordance with their own privacy or security procedures. However, the Parties must notify each other by telephone and e-mail of any breach in security, especially those that result in unauthorized use or disclosure of any PII or other information shared under this MOA. NCTC will make such notification in accordance with ODNI Instruction 80.02. NCTC will notify POCs identified in Appendix C.
To further safeguard the privacy, security, confidentiality, integrity and availability of the connected systems and the information they store, process and transmit, the Parties agree to maintain records of information provided to each other under the terms of this Agreement consistent with applicable law, as well as established records retention policies and guidance of the respective Parties.

The Parties will meet at the request of any Party, to discuss and review the implementation of this MOA. Any disagreement over the implementation of this MOA will be resolved in accordance with Section 10 of this Agreement.

NCTC will develop methods to track and report to DHS on a quarterly basis the information identified in Appendix B of this Agreement. DHS will review NCTC's reporting metrics on a quarterly basis.

N. AUDITING.

NCTC will perform system audits and ensure that any PII is shared consistent with applicable laws, regulations, and guidelines. In order to ensure that data is only used for the purposes described in this MOA, DHS will have the right to review NCTC's audit records as they pertain to DHS data in accordance with NCTC information security policy and procedures, and to view NCTC's audit records and inspect NCTC's use of APIS Data. Audited events will include who has accessed the data, what reports have been generated based on the APIS Data and to whom the reports have been disseminated. NCTC systems storing and accessing APIS Data will be Certified and Accredited in accordance with Intelligence Community Directive 503 and will contain security controls, including auditable events appropriate to the data stored in the systems.

P. ON-SITE DHS OVERSIGHT REPRESENTATIVE.

DHS will, subject to the availability of resources, assign a DHS on-site oversight representative to ODNI/NCTC, under the terms of a separate personnel agreement between the Parties for the purpose of providing oversight (to include intelligence, data stewardship, privacy, civil rights, and civil liberties oversight) of the handling of APIS Data by NCTC. This representative will coordinate with the Office of the Director of National Intelligence's Civil Liberties Protection Office and Office of the General Counsel, as appropriate.

Q. JOINT REPORT.

Within a year of signature of this agreement, the Parties will complete a joint report regarding prioritization of screening, TIDE enhancement, and analytic initiatives that leverage NCTC's data holdings and provide value to the Department and the IC. The Parties will provide interim reports quarterly to the Deputy Secretary of Homeland Security, Director of NCTC, Under Secretary for Intelligence and Analysis, DHS Chief Privacy Officer, DHS Officer for Civil Rights and Civil Liberties, the DHS General Counsel, and the ODNI Civil Liberties Protection Officer.

6. POINTS OF CONTACT.

The persons responsible for implementation of this MOA and the identification and resolution of issues hereunder are identified in Appendix C. The Parties agree the points of contact listed in Appendix C may be updated at any time without the need for coordination.

7. SEVERABILITY.

Nothing in this Agreement is intended to conflict with applicable law, executive order, presidential or other directive, regulation, international obligation, national policy, or departmental policies of DHS or NCTC. If a term of this Agreement is inconsistent with such authority, then that term will be invalid, but the remaining terms and conditions of this Agreement will remain in full force and effect.

8. NO PRIVATE RIGHT.

This MOA is an internal agreement between DHS and NCTC. It does not create or confer any right or benefit, substantive or procedural, enforceable by any third party against the Parties, the United States, or the officers, employees, agents, or associated personnel thereof. Nothing in this MOA is intended to restrict the authority of either party to act as provided by law, executive order, presidential or other directive, regulation, international obligation, or national or departmental policy, or to restrict any party from administering or enforcing any laws within its authority or jurisdiction.

9. FUNDING.

This MOA is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed in writing, each Party will bear its own costs in relation to this

MOA. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

10. ISSUE RESOLUTION.

Throughout the course of this Agreement, issues concerning aspects of this Agreement, such as its scope, the interpretation of its provisions, unanticipated technical matters (including improvements), and other proposed modifications may arise. Both Parties agree to appoint their respective points of contact to work in good faith towards resolution. Failing resolution, either party may refer a dispute concerning constitutional or other legal matters to the Attorney General and may seek the resolution of any other disputes through the National Security Council process, subject to Presidential Policy Directive (PPD) 1 as required.

11. EFFECTIVE DATE.

The terms of this Agreement will become effective upon the last signature to this MOA.

12. MODIFICATION.

This Agreement and any appendices thereto, may be modified upon the mutual written consent of the Parties, which will be recorded and incorporated into this MOA as a separate addendum.

13. TERMINATION.

The terms of this Agreement, as modified with the consent of both Parties, will remain in effect until three years from the date of execution. The Agreement may be extended by mutual written agreement of the Parties. Either Party may, upon thirty days written notice to the other Party, terminate this Agreement without need for cause. Should one Party to this Agreement violate any of the terms set forth within this Agreement, the other Party may terminate the Agreement for cause immediately provided that (1) prior written notice is provided by the terminating Party setting forth the circumstances giving rise to and the basis for the immediate termination of the Agreement and (2) such notice is provided within sixty days of the terminating Party's discovery of the violation giving rise to immediate termination of the Agreement.

14. ENTIRE AGREEMENT.

This MOA, and any concurrently or subsequently approved appendices, constitutes the entire agreement between the parties.

APPROVED BY:

This MOA represents the understanding reached between DHS and NCTC. By signing below, the Parties have caused their duly authorized representatives to execute this MOA.

FOR THE UNTIED STATES DEPARTMENT OF HOMELAND SECURITY

5 June 2013

William E. Tarry, Jr. [Date]
Acting Under Secretary for Intelligence and Analysis
Intelligence and Analysis
United States Department of Homeland Security

[redacted]

6/4/2013

Michael Keegan [Date]
Acting Assistant Commissioner
Office of Intelligence and Investigative Liaison
U.S. Customs and Border Protection

FOR THE NATIONAL COUNTERTERRORISM CENTER

June 3, 2013

Nicholas J. Rasmussen [Date]
Principal Deputy Director
National Counterterrorism Center

APPENDIX A: List of APIS Record Data Elements

DHS/CBP has agreed to provide the following elements of APIS Record data to NCTC under the MOA:

[redacted]

Additional APIS Record data elements [redacted] are also provided by DHS/CBP to NCTC under this MOA:

[redacted]

APPENDIX B: NCTC Reporting Requirements for APIS

No.	NCTC Report Category	Metric	APIS
1	DHS Provided	DHS reported records delivered (as counted by DHS.)	Event
2	Records Retention	Number of Records received by NCTC (counted using the same method as DHS.)	Event
3	Records Retention	The number of Records loaded into the CTDL (counted using NCTC's method for CTDL)	Event
4	Records Retention	Number of Records NCTC deleted after NCTC determined no terrorism Information exists for that record	Event
5	Records Retention	Number of Records NCTC deleted after the temporary retention period expired	Event

6	Records Retention	Number of corrective actions taken (based on correction requests received from DHS)	Event
8	Records Retention	Cumulative number of [redacted] records for the data set in total	Event
9	Data Usage	Number of [redacted] records determined to be Terrorism Information through human vetting in support of the [redacted] process	Event
10	Data Usage/Retention	Number of records determined by an NCTC analyst to be Terrorism Information outside the [redacted] process	Record
11	Data Usage	Number of NCTC intelligence products created and disseminated (to include [redacted] reports, studies or other analysis), that cite APIS data	Event
12	DHS Provided	Number of DHS [redacted] based on NCTC's identification of DHS information as Terrorism Information	Event
13	Data Usage	The number of times APIS data is queried via internal NCTC search tools	Record

14	Data Usage	The number of TIDE records enhanced with DHS data ([redacted])	Person
15	Data Usage	Number of products recalled that cite the data if such recall was related to the data	Product

APPENDIX C: Points of Contact

POCs for the Parties are as follows:

OIIL Targeting Executive Director
Office of Intelligence and Investigative Liaison
Customs and Border Protection
[redacted]

Chief, Information Sharing Program and Policy Office
National Counterterrorism Center
[redacted]

Division Director
Information Sharing and Intelligence Enterprise Management Division
Office of Intelligence and Analysis
[redacted]

In the event of a reporting requirement under Section M of the MOA, the parties will make notifications to the following POCs:

CBP Information System Security Manager (ISSM): [redacted]

CBP Privacy Officer: [redacted]

NCTC Information Sharing Program and Policy Office: [redacted]

NCTC Legal Office: [redacted]

NCTC Civil Liberties and Privacy Office: [redacted]

APPENDIX D: AG Guidelines – Baseline Safeguards

During the temporary retention period, the following baseline safeguards, procedures, and oversight mechanisms for any datasets acquired pursuant to Track 3 that have been determined to contain United States Person information will apply:

1. The data will be maintained in a secure, restricted-access repository.

2. Access to the data will be limited to those NCTC personnel, who are acting under, and agree to abide by NCTC's information sharing and use rules, including the 2012 NCTC Guidelines; who have the requisite security clearance and a need-to-know in the course of their official duties; and who have received the training required by section III.B.3 of the 2012 NCTC Guidelines.

3. Access to the data will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the IC. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with the rules applicable to the data for which audit records apply.

4. NCTC's queries or other activities to assess information contained in datasets acquired pursuant to Track 3 shall be designed solely to identify information that is reasonably believed to constitute Terrorism Information. NCTC shall query the data in a way designed to minimize the review of information concerning United States Persons that does not constitute terrorism information. To identify information reasonably believed to constitute Terrorism Information contained in Track 3 data, NCTC may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, DHS will coordinate with NCTC to ensure proper reporting and to identify which element should report these activities as required by that Act.

5. DHS will conduct compliance reviews as described in section VI of the 2012 NCTC Guidelines.