

**MEMORANDUM OF AGREEMENT
BETWEEN
THE DEPARTMENT OF DEFENSE
AND
THE DEPARTMENT OF HOMELAND SECURITY
ON INFORMATION SHARING AND TECHNOLOGY PARTNERING
RELATING TO IDENTITY VERIFICATION AND SCREENING ACTIVITIES**

I. PARTIES

The Parties to this Memorandum of Agreement (MOA) are the Department of Defense, including its components, agencies, and offices (hereinafter “DoD”), and the Department of Homeland Security, including its components, agencies, and offices (hereinafter “DHS”), collectively, the “Parties.”

II. BACKGROUND

Information sharing between DoD and DHS is intended to support the missions of the Parties, including for DoD: warfighter, detainee affairs, and force protection efforts; anti-terrorism, special operations, stability operations, homeland defense, counterintelligence, and intelligence; for DHS: critical infrastructure protection, transportation and border security, law enforcement, administration of immigration benefits, emergency management, and intelligence; and other interests of the United States.

This MOA currently includes six types of information exchanges. Any further information exchanges beyond those enumerated below will be included as appendices as agreed to by the Parties:

A. Biometric Information Exchange. The provision of a biometric identifier (such as fingerprint) by one party (the providing party) to the other (the receiving party) for the purpose of determining or confirming the identity and associated information concerning the individual. Additional terms relating to these types of exchanges under this MOA are in Appendix A.

B. System Account Access. One Party creates a specified number of user accounts for individuals employed by the other Party to access its systems for the purposes specified in this MOA and its Appendices. Additional terms relating to this type of exchange under this MOA are in Appendix B.

C. Watchlist Export. DoD transfer of its unclassified Biometrically Enabled Watchlist, and associated data, to DHS. Additional terms relating to this type of exchange under this MOA are in Appendix C.

D. Science and Technology (S&T) Management. DHS and DoD collaboration on S&T efforts and information exchange about the direction of their respective programs. Additional terms relating to this type of exchange under this MOA are in Appendix D.

E. Identity and Biometric Credentialing Coordination. DoD and DHS collaboration on Federal Identity & Credentialing and Access Management (FICAM) Committee, subsequent exchange of relevant work product. Additional terms relating to this type of exchange under this MOA are in Appendix F.

F. Federated Privilege Management/Attribute Management. Development of DoD/DHS technical interfaces for biographic information. Additional terms relating to this type of exchange under this MOA are in Appendix G.

III. PURPOSE

This MOA is the governing information sharing and technology partnering agreement between DoD and DHS with respect to biometric, biographic, contextual and other identity management data. This MOA is intended to formalize the ongoing relationship between DoD and DHS, and to clarify the Parties' commitment to sharing appropriate biometric, biographic, contextual, and other information related to identity verification and people screening between the Parties. This MOA shall be implemented in a manner consistent with applicable laws, regulations, Executive Orders, and departmental policies concerning the sharing and protection of information – including those related to the protection of privacy and civil liberties of individuals; intelligence sources, methods and activities; law enforcement information; and classified national security information.

This MOA is intended to replace existing biometric, biographic, contextual and any other identity management, and/or people screening or vetting data sharing agreements between the Parties only to the extent that such agreements contain terms inconsistent with this MOA in which case the terms in this MOA shall supersede/prevail.

The MOA is intended to be interpreted at the strategic level. Detailed coordination, planning, and program development specifics are not included in this MOA. These will be collaboratively developed and coordinated to ensure the execution and lifecycle of the MOA consistent with its intent and the actual principles, terms, obligations, and responsibilities contained herein.

IV. DEFINITIONS As used in this MOA, the following terms will have the following meanings:

A. **BIOMETRIC:** A measure of an identifying physical aspect of an individual—e.g., a fingerprint, iris scan, or DNA—that can be turned into a digital template capable of being electronically stored and compared for verification or matching purposes.

B. **DATA:** biometric, biographic, contextual and other information related to identity verification and people screening as described in the Appendices to this MOA,

and as further delineated in associated Interface Control Documents (ICDs), Service Level Agreements (SLAs), Operational Protocols and any other related project documentation separately agreed to and approved by the parties as described in Section VI. B. of this MOA. Collectively, all information described under this subpart is “data” or “information” under the terms of this MOA.

C. **KNOWN OR SUSPECTED TERRORIST (KST):** As described in Homeland Security Presidential Directive (HSPD) 6, individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to, terrorism.

D. **NATIONAL SECURITY THREAT (NST):** As described in HSPD-24, individuals for whom there is an articulable and reasonable basis for suspicion that the individual poses a threat to national security.

E. **INFORMATION SHARING ENVIRONMENT (ISE):** As established by section 1016(b)(1)(A) and defined in section 1016(a)(3) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007.

F. **INFORMATION INCIDENT:** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, or for any other than authorized purpose, have access or potential access to the information in usable form, whether physical or electronic.

G. **PERSONALLY IDENTIFIABLE INFORMATION (PII):** Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an identifiable individual.

H. **U.S. PERSON:** A citizen of the United States or an alien lawfully admitted for permanent residence, as defined in 8 U.S.C. § 1101(a)(20).

V. AUTHORITY

This MOA is both enabled by, and facilitates implementation of, the following legal authorities:

1. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Pub. L. 107-56);
2. The Homeland Security Act, as amended (Pub. L. 107-296);
3. The Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458);
4. The National Security Act of 1947, as amended;
5. The Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53);

6. The Immigration and Nationality Act, as amended (8 U.S.C. § 1101 et seq.);
7. The Privacy Act of 1974, as amended (Pub. L. 93-579);
8. 8 U.S.C. §§ 1365a and note; 1365b; and 1731;
9. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans;
10. Executive Order 12333, United States Intelligence Activities, as amended;
11. Executive Order 13526, Classified National Security Information;
12. Homeland Security Presidential Directive (HSPD) 6, Integration and Use of Screening Information to Protect Against Terrorism; HSPD 11, Comprehensive Terrorist Related Screening Procedures, and HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors;
13. HSPD- 24/National Security Presidential Directive (NSPD) 59, Biometrics for Identification and Screening to Enhance National Security;
14. Intelligence Community Directive 710, Classification and Control Marking System;
15. Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 2003), as extended;
16. Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (TSC MOU) (September 2003), including Addendum B to the TSC MOU; and
17. Memorandum from the Secretary of DHS, Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies (April 2007).

VI. RESPONSIBILITIES

The Parties agree to the following shared responsibilities:

A. **AUTHORIZED USERS.** Authorized users are those within each Party who have an official need for access to the data covered by this MOA in performance of official duties, consistent with applicable laws, regulations, and system of records notices (SORNs), Privacy Impact Assessments (PIAs), Departmental Policies, and the purposes identified in the Appendices to this MOA.

B. **DATA SHARING TECHNICAL INTERFACE.** The Parties will adhere to the principles, technical standards, business processes, information assurance and privacy protection mechanisms required under the Privacy Act and other relevant laws, regulations, SORNs, PIAs, and departmental policies for the sharing of data under this MOA. These shall be included in ICDs, SLAs, Operational Protocols and any other related project documentation as agreed to separately by the Parties. The Parties will explore the sharing of biographic data, often referred to as "attributes," through federated means to further support the information sharing goals of the Parties under this MOA. More specific information on the technical interaction between the Parties for the sharing of data is also contained in the appendices to this MOA.

The technical means by which the information will be shared, what specific data elements will be shared, and the related ICDs, SLAs, Operational Protocols and other related project documentation will be approved by the Parties' Privacy Office, Office for Civil Rights and Civil Liberties, Office of General Counsel, and the relevant data steward (or the equivalent or designee of these offices) prior to implementation. Additional mitigation strategies may be identified and implemented at that time.

C. TECHNOLOGY. Each Party is committed to updating its relevant systems, procedures, and protocols when practicable and as appropriate to implement this MOA, as required, to ensure the data shared under this MOA remains current, and that respective systems remain efficient as data volumes increase and more advanced technologies become available.

D. RECORDS STORAGE. The Parties shall search and retain data as described below and as specified in the Appendices to this MOA, and the associated SLAs, ICDs, Operational Protocols, and other project documentation as appropriate. Neither party will retain data except as specified in the applicable Appendices to this MOA. The Parties will retain the data only as long as is needed to fulfill the purposes stated in the Appendices to this MOA. In no instance will the retention period of any data item exceed the maximum period permissible by applicable legal and regulatory requirements or official retention policies. When the Parties store data received from the other Party, such data shall be stored in systems that ensure protection of the information and shall be retained in accordance with the Parties' respective National Archives and Records Administration (NARA)-approved records retention schedules. Each party will ensure that its systems are accredited and certified to the highest classification level of data potentially shared on that system(s).

E. SUPPORT. Through designated points of contact (POCs), the Parties will assist each other with inquiries on their data as provided through mutually agreeable operational protocols. The Parties will designate and, to the extent possible, maintain an office and staff to field technical questions for the systems listed in Appendix A as expeditiously as possible. The Parties will notify each other of their POCs for this purpose.

F. TRAINING.

1. The Parties shall ensure that personnel with access to data shared under this MOA are appropriately educated and trained in the protection and proper treatment of all data, including but not limited to personally identifiable information (PII) exchanged under this MOA, to ensure overall safeguarding of the information, in accordance with the Privacy Act and other applicable laws and policies, including but not limited to provisions enumerated in Section VII.B (confidentiality regulations associated with particular immigration benefits).

2. The Parties shall abide by their respective department's privacy policies, and will ensure that its employees, including contractors and detailees from third

agencies with access to any of the other Party's data, have completed any required privacy and information assurance training on the handling of all data.

3. The Parties will also train designated users on techniques to effectively query any shared systems, if requested. The training will include an explanation of data fields and be closely coordinated by the Parties.

G. **REPORTING of MATCHES.** The Parties shall report to each other, through appropriate channels, all potential matches against data provided by the other Party as expeditiously as possible and as specified in the Appendices to this MOA, and associated ICDs, SLAs, Operating Protocols, and/or other project documentation as agreed to by the Parties. The Parties shall endeavor to identify an individual as a US person when reporting matches pertaining to a US person.

H. **COMPLIANCE AUDITS.** The Parties agree to maintain records of information provided to each other under the terms of this MOA. The Parties may audit the access, use, handling and maintenance of each other's data to ensure compliance with this MOA and its appendices. Each party shall have the right to independently audit and inspect the other Parties' use of data provided under this MOA, and to review the audit records of the other Party. The Parties may also accept the results of internal agency audits (such as Inspector General audits) conducted in lieu of an audit under this section where and to the extent that such audits address compliance with this MOA.

VII. LIMITATIONS ON THE DISCLOSURE AND USE OF INFORMATION

A. **APPLICABLE AUTHORITIES.** Both Parties acknowledge that the information shared under this MOA may be subject to the Privacy Act, other laws, regulations, SORNs, PIAs, departmental policies, and the ISE Privacy Guidelines, and to additional terms and conditions set forth in relevant SORNs and Departmental policies as appropriate. The sharing of information under this MOA will be done in accordance with those authorities, when applicable.

B. **SPECIAL PROTECTED CLASSES.** The Parties further acknowledge that the data and other information provided under this MOA may be subject to specific nondisclosure provisions and other limitations on use under existing law and policy, including but not limited to sections 222(f) (Department of State visa records); 244(c)(6) (temporary protected status), and 245a(c)(5) (adjustment of status of certain entrants) of the Immigration and Nationality Act; 8 U.S.C. § 1367 (Violence Against Women Act claims); 8 C.F.R. § 214.11(e) (T and U non-immigrant claims); and 8 C.F.R. § 208.6 (asylum information; protections afforded to refugee data as a matter of DHS policy), and Convention Against Torture (CAT) data (afforded protection as a matter of DHS Policy).

1. Consistent with DHS policy, DHS will provide information contained in asylum and refugee applications, CAT, credible fear determinations, and reasonable fear determinations to DoD intelligence entities pursuant to and in accordance with the DHS Secretarial waiver to 8 C.F.R. § 208.6 for intelligence purposes referenced in section V.17., above.

2. DHS may provide DoD with special handling instructions, or other conditions as appropriate, for the protection of the data and other information described in this paragraph.

3. Any data provided under the terms of this subsection may be further disclosed only upon prior approval from DHS, in coordination with the Department of State (DOS) as appropriate.

C. MEANING OF THIRD PARTIES. For purposes of records disclosure under this MOA, other bureaus within DoD are not considered third parties or separate agencies of DoD. Similarly, offices and component elements of DHS are not considered third parties or separate agencies for information disclosure purposes under this MOA. At all times, the receiving party must use the information only for those official purposes identified in the appendices, including: DoD disclosing information received under this MOA throughout each Party's respective offices, bureaus, or components only where there is an official need in carrying out those purposes as contemplated under this MOA and its Appendices, as authorized by applicable law and policy, and in compliance with applicable privacy and confidentiality requirements. For visa adjudication purposes, DOS shall not be considered a third party for access to DOD information shared under this MOA.

D. THIRD PARTY SHARING. Subject to subsection E below, both parties acknowledge that data stored on behalf of third parties, or subsequent matches to that data, will not be shared without the consent of the data owner.

E. SHARING OF KST AND NST DATA. This section is intended to reflect the Parties' responsibilities with respect to information sharing pertaining to KSTs and NSTs for the purposes reflected in this MOA. These responsibilities are consistent with those of the Parties already reflected under separate interagency agreements concerning the use and exchange of KST and NST data, and no new requirements between the parties are intended.

1. KST and NST data may be transferred and/or shared with other U.S. Government departments or agencies without prior approval, subject to each Party's legal authorities and any applicable policies, regulations, and handling caveats. The sharing party shall notify the data owner within 3 working days. In cases where the DoD policy regarding detainees at Guantanamo Bay prevents DoD from providing notice within 3 working days, notice shall be provided as soon as possible, consistent with that policy.

2. KST and NST data may be transferred and/or shared with foreign governments as approved by the data owner/data steward, and including consultation with other relevant agencies, as appropriate.

3. The Parties agree not to disclose individuals' personally identifiable information, including watchlist status, to any person who does not have the appropriate security clearance, where required, and need-to-know such information for the performance of official duties.

F. **SHARING DUE TO IMMINENT THREAT.** The Parties may share information that is associated with an imminent threat to national security, or that is extremely time sensitive for supporting the warfighter effort, with other U.S. Government departments or agencies. Such sharing will be followed by notification to the data owner/data steward as expeditiously as possible.

G. **SPECIAL DoD CONSIDERATIONS.**

1. Shared information about a U.S. Person that identifies, links, relates, is unique to, or describes him or her (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc.) collected and stored by DoD pursuant to this MOA may only be used for purposes outlined in this MOA and its appendices.

2. DoD will maintain flags and alert texts denoting all KST, NST and/or watchlist data in the databases described in Appendix A to this MOA.

H. **RESPONDING TO THIRD PARTY REQUESTS FOR INFORMATION SHARED UNDER THIS MOA.** Where a Party receives a third party request for information shared under this MOA, such as a request under the Freedom of Information Act or the Privacy Act, or through Congressional or media request, or any other method, that Party will ensure that it does not adjudicate such requests for the other Party. The Party receiving a third party request for information which is owned or originated by the other Party shall immediately consult with the other Party as to how to respond to the request.

VIII. DISPOSITION OF DATA

A. CORRECTION AND REDRESS.

Personally identifiable information shared and/or maintained under this MOA shall, to the extent feasible, be as accurate, complete, and current as feasible for the purposes identified in this MOA. The Parties shall cooperate with each other in this regard. The Parties will, in a timely manner, take appropriate action with regard to any request made by the other Party for access, additions, changes, deletions, or corrections of PII. In addition, each Party will, in a timely manner, notify the other Party of any data errors that it discovers.

Each Party shall maintain an ability to locate and correct PII provided under this MOA that is maintained by the other Party. Additionally, the Parties shall correct any disseminated information based on the information shared under this MOA that is later deemed to be erroneous. Location and correction of records shall be accomplished in not more than three working days and each Party will provide written confirmation to the other of the corrections made.

B. In the event of an adverse screening experience as a result of data exchanged under this MOA, the Parties shall refer the individual to seek redress through the established DHS TRIP redress process. DoD will provide assistance to the DHS redress process by verifying that all relevant information relied upon in the screening process is thorough, accurate, and current; and making any warranted corrections to pertinent records in DoD systems, as appropriate, when notified to take such action as a result of the redress adjudication.

C. Before either Party uses any data exchanged under this MOA to make decisions or take actions that could affect the legal rights or other interests of any individual, that Party shall make every effort to verify whether such data has been updated with more timely, complete, or accurate information using whatever technical means for data exchange have been established.

D. The Parties shall, as expeditiously as possible, inform each other of any change in status (e.g., foreign national to U.S. Person) of an individual whose information has been shared and retained by either Party.

IX. SECURITY AND BREACH REPORTING

A. The Parties agree to maintain appropriate physical, electronic, and procedural safeguards to adequately protect the information shared under this MOA, against loss, theft or misuse, as well as unauthorized access, disclosure, copying, modification, or deletion.

B. Unauthorized activity and activity disruptions.

1. When there has been or may have been an information incident, including actual or potential unauthorized access, use, dissemination, storage, or disposal of data shared under this MOA or its Appendices, the Party discovering the incident shall immediately report to, and consult with, the other Party. The Parties shall also take any other action as required by applicable laws and regulations, including as appropriate, reporting the incident in accordance with Office of Management and Budget (OMB) Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost of Security in Agency Information Technology Investments" (12 July 2006).

2. The Parties shall immediately notify each other in the event of a service disruption that disrupts the normal operation of connected systems. Project-level documentation will establish the points of contact for this notification as appropriate.

X. FUTURE DATA SHARING

A. More detailed arrangements to implement the activities envisioned under this MOA will be implemented through creation of SLAs and ICDs as appropriate and as agreed to by the Parties under this MOA, consistent with the principles reflected in this MOA and the users and uses detailed in the Appendices.

B. An addendum to this MOA is required for any data sharing that represents an expansion in scope of the terms of covered data contemplated by this MOA or its approved appendices. An addendum may be added to this MOA after review and consent by the Parties.

XI. INTERPRETATION AND SEVERABILITY

This MOA is not intended to conflict with current law or regulation. If a term within this MOA or any of its appendices is inconsistent with such authority, then that term shall be invalid to the extent of the inconsistency, and any remaining terms and conditions shall remain in full force and effect.

XII. NO PRIVATE RIGHT OR CAUSE OF ACTION

This MOA is an internal agreement between DoD and DHS. It does not create or confer any right or benefit of any kind, either substantive or procedural, that may be enforceable by any third party against the Parties, the United States, or the officers, employees, agents, or associated personnel thereof. Nothing in this MOA or its Appendices is intended to restrict the authority of either Party to act as provided by law, statutes, or regulation, or to restrict any Party from administering or enforcing any laws within its authority or jurisdiction.

XIII. FUNDING

This MOA is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each Party shall 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.

XIV. DISPUTE RESOLUTION

Disagreement between the Parties arising under or related to this MOA shall be resolved exclusively by consultation between the Parties. Disagreements may not be referred to any court or administrative body for settlement.

XV. EFFECTIVE DATE

The terms of this MOA will become effective upon date of the last signature of the Parties.

XVI. ENTIRE AGREEMENT

This MOA and its Appendices constitute the entire agreement between the Parties.

XVII. MODIFICATION

This MOA and its Appendices may only be modified or amended by the mutual written consent of the Parties. Future data sharing arrangements or agreements between DoD and DHS, as articulated in Section X and consistent with the terms and scope of this MOA, will be attached to this MOA as Appendices. The specific terms of the Appendices and other operative documents between the Parties pursuant to this MOA can be individually negotiated and modified without requiring a modification to the terms of this MOA, as provided in Section X, unless the terms or scope of information and activities contemplated in an appendix or other operative document is inconsistent with the purposes, terms, and scope of the MOA, in which case the MOA itself would require an addendum, or else be modified or amended.

XVIII. PERIODIC REVIEW

The Parties are to designate responsible officials to meet annually, or at the request of either Party, to discuss and review the implementation, execution and lifecycle of this MOA.

XIX. TERMINATION

Either Party may terminate this MOA or its appendices by providing thirty (30) days written notice to the other Party. However, all provisions regarding the protection of records, including data privacy and confidentiality, remain in effect as long as either Party remains in possession of any such records or any information obtained from the other Party.

The foregoing represents the agreement reached by the U.S. Department of Defense and U.S. Department of Homeland Security.

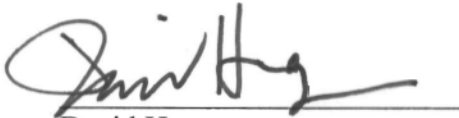
SIGNED:



Paul N. Stockton
Assistant Secretary of Defense
Homeland Defense and Americas' Security Affairs
U.S. Department of Defense

MAR 3 2011

Date



David Heyman
Assistant Secretary, Policy
U.S. Department of Homeland Security

18-Feb-2011

Date

APPENDIX A

BIOMETRIC INFORMATION EXCHANGE

Biometric Information Exchange refers to the provision of a biometric (including associated biographic and contextual data)¹ by one party (the Providing Party) to the other party (the Receiving Party), for use by the Receiving Party to determine or confirm the identity of the subject and provide the Providing Party with associated information concerning the subject. As detailed below, the Receiving Party will: (1) compare the received biometric to biometrics in its applicable system(s);² (2) determine if there is a match; and (3) provide the biographic, contextual, and other identity verification-related data associated with a match from the applicable systems to the Providing Party, except as set forth in Section B.2 in this Appendix.

This Appendix identifies authorized data transfer (manual or automated), access, uses, and users for particular data under this Memorandum of Agreement (MOA) for the purpose of biometric information exchange. All authorized users and uses of data described in this Appendix are explicitly stated; any changes require mutual agreement by the Parties via mutually acceptable documentation.

There will be no new categories of information shared under this Appendix until the terms of this Appendix and the separate Operational Protocols document are agreed to between DHS and DoD.

The Parties will ensure, prior to the exchange of biometric information, that their systems of records notices (SORNs) adequately cover the exchange of biometric information described in this appendix. The data shared under this Appendix will be identified in the Operational Protocols document, and attached as an addendum to this appendix.

A. Users and Uses

1. The Parties will have access to data in the databases as described below in Sections C and D. Additional processes for the DoD Watchlist Export and appropriate DHS Automated Biometrics Information System (IDENT) information (as determined by DHS) are set forth in Appendices C and H, respectively.
2. Data may be provided through bulk data export or through automated interoperable mechanisms once established (the latter is the preferred method). The exact data and means of access will be further delineated in associated Service Level Agreements (SLAs), Interface Control Documents (ICDs), Operational Protocols, and any other related project documentation separately agreed to and approved by the Parties, as described in section VI.B. of the MOA.
3. The Providing Party will provide a biometric with each search request covered by this Appendix.

¹ Defined in section IV.A. of the MOA as “a measure of an identifying physical aspect of an individual – e.g., a fingerprint, iris scan, or DNA – that can be turned into a digital template capable of being electronically stored and compared for verification or matching purposes.”

² See sections C and D in this Appendix for specific applicable systems.

4. As applicable, DHS fingerprint search requests will be conducted through IDENT,³ which serves as the common communication tool with DoD Automated Biometric Information System (ABIS) on behalf of DHS Components.⁴ For biometric modalities not currently supported for inclusion in IDENT, DHS will work with DoD to determine the appropriate alternative mechanism for sharing such information.
5. DoD search requests will be conducted through DoD ABIS,⁵ which acts as the common communication tool to IDENT, on behalf of all DoD offices.
6. DHS will notify DoD if submitted data is regarding a known U.S. Person in accordance with ICDs, SLAs, and other Operational Protocols as appropriate.
7. The Parties will limit access to information provided under this Appendix to authorized users.⁶

B. Matches

1. The Receiving Party shall report all matches to the Providing Party, through appropriate channels, as expeditiously as possible. The Receiving Party will provide additional information associated with the match, as specified below:
 - a. **Known or Suspected Terrorist or National Security Threat Match:** When a confirmed match to a known or suspected terrorist (KST) or a national security threat (NST) is identified, the Receiving Party will share with the Providing Party appropriate information (e.g., underlying and/or derogatory information) as defined in the Operational Protocols related to the match, as well as all biometric, biographic, contextual, and identity-verification related information from the applicable systems, consistent with the terms of Section VI.G. of the MOA.
 - i. KST and NST data may be further transferred and/or shared with other U.S. Government departments or agencies, subject to each Party's legal authorities and any applicable policies, regulations, and handling caveats, and consistent

³ IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions and functions, including but not limited to: the enforcement of civil and criminal laws (including immigration laws); investigations, inquiries, and proceedings in connection with those missions and functions; and national security and intelligence activities.

⁴ U.S. Citizenship and Immigration Services (USCIS) will exchange communications with DoD through its existing direct interface until IDENT acquires all DoD data requested by USCIS, or when IDENT can provide the technical exchange for communications with DoD ABIS.

⁵ DoD ABIS is the DoD central, authoritative multi-modal (i.e., fingerprint, palm, iris, face) biometric repository. DoD ABIS is an enterprise solution that is the strategic level authoritative data source for unclassified DoD biometrics. It integrates the DoD worldwide biometric efforts targeting known and suspected terrorists. The system operates and enhances associated search and retrieval services and interfaces with existing DoD and interagency biometric systems. The repository interfaces with collection systems, intelligence systems and other deployed biometric repositories across the Federal Government.

⁶ Defined in section VI.A. of the MOA as "those within each Party who have an official need for access to the data covered by this MOA in performance of official duties, consistent with applicable laws, regulations, and system of records notices (SORNs), Privacy Impact Assessments (PIAs), Departmental Policies, and the purposes identified in the Appendices to this MOA."

with Section VII.E of the MOA. The sharing party shall notify the other party within three working days of the date that such transfer or sharing occurs.

- b. **Non-KST/NST Match:**⁷ When a subject is matched to information in the Receiving Party's applicable system(s), the Parties will share appropriate information (e.g., underlying and/or derogatory information) related to the match, as well as all biometric, biographic, contextual, and identity-verification related information from applicable systems specified under this MOA, consistent with the terms of Section VI.G of the MOA.
2. DHS will not provide to DoD any information related to special protected classes of persons as described in Section VII.B of the MOA unless authorized by, and then only in accordance with, governing statute, regulation, or DHS policy.⁸ Provisions concerning the use, handling, retention, marking, and further dissemination of such information will be outlined in the Operational Protocols.
 3. Pursuant to section VII.D of this MOA, data stored by the Providing Party on behalf of Third Parties (not DHS or DoD), or subsequent matches to such data, will only be shared with the consent of the data owner.
 4. Except pursuant to existing agreement or Section B.1 of this Appendix, data may only be retained in accordance with criteria to be outlined in the Operational Protocols, including temporary retention periods and permanent retention criteria.⁹ Such data may not otherwise be retained until the Operational Protocols are approved by both Parties.
 5. In the event of a KST or NST Match, as described in B.1.a in this Appendix, or a Non-KST/NST Match, as described in section B.1.b. in this Appendix, all relevant biometric, biographic, contextual, and other information will be shared between the Parties as permitted by law, regulation, policy, and applicable agreements, so that the Providing Party may take appropriate action, including, as appropriate, analysis of the data and development of intelligence products.

⁷ A non-KST/NST match may include information on immigration violations and criminal activity, and may also include information that may be used to identify inconsistencies or contradictions in a subject's statements. Records should include the most current disposition.

⁸ Consistent with the MOA and DHS policy, DHS will provide to DoD intelligence entities information contained in or pertaining to asylum or refugee applications, credible fear or reasonable fear determinations and applications for applications for protection under the Convention Against Torture pursuant to and in accordance with the Secretary of Homeland Security's authorization under 8 C.F.R. § 208.6(a) to disclose such information for intelligence purposes.

⁹ In no instance will the retention period of any data item exceed the maximum period permissible by applicable legal and regulatory requirements or official retention policies. When the Parties store data received from the other Party, such data shall be stored in systems that ensure protection of the information and shall be retained in accordance with the Parties' respective National Archives and Records Administration-approved (NARA-approved) records retention schedules and the retention periods specified in the Operational Protocols.

C. DoD Biometric Information Exchange Requests to DHS. For the requests listed below, DoD is the Providing Party, and DHS is the Receiving Party.

	Providing Party	Data Provided/ Impacted DHS Systems	Purpose or use of search
1	Joint Force Commander	DoD biometrics matched against IDENT.	Search DoD biometrics against IDENT to provide biometric identity verification to support the identification of potential or realized threats to DoD combat operations.
2	National Ground Intelligence Center (NGIC)	DoD biometrics matched against IDENT.	Search DoD biometrics against IDENT to identify information on subjects of interest for inclusion on the DoD Biometrically Enabled Watchlist (BEWL), in Biometric Identification Analysis Reports (BIAR), or other intelligence products.
3	US Army Recruiting Command	DoD biometrics matched against IDENT.	Search DoD biometrics collected by army recruiters against IDENT to biometrically confirm immigration and/or travel history.
4	All DoD offices of credentialing and access	DoD biometrics matched against IDENT.	Search DoD biometrics against IDENT to determine if subject is a threat and/or ineligible for access to DoD installations, facilities, systems, information, and/or assets.
5	DoD (components, agencies, offices)	DoD-collected prints matched against DHS Unidentified Latent Files.	Search DoD prints against DHS Unidentified Latent Files to identify subjects with whom DoD has had contact who may be a threat, but are only identifiable via latent print matching.
6	Military Departments	Biometrics of DoD service members who have approved court-martial sentences matched against IDENT.	Search DoD biometrics against IDENT to identify non-U.S. citizen service members who may be subject to immigration proceedings.

D. DHS Biometric Information Exchange Requests to DoD. For the requests listed below, DHS is the Providing Party, and DoD is the Receiving Party.

	Providing Party	Data Provided/ Impacted DoD Systems	Purpose or use of search
1	U.S. Citizenship and Immigration Service (USCIS)	Biometrics in USCIS holdings matched against DoD ABIS.	Search biometrics against DoD ABIS to identify information from DOD records that may assess or refute information in an application or other request for an immigration related benefit or status as appropriate for the purpose of determining benefit eligibility or verifying protection claims (e.g., DoD data contradicts information in the subject's application, or identifies the subject as a threat).
2	U.S. Secret Service (USSS)	Biometrics collected by USSS matched against DoD ABIS.	Search biometrics against DoD ABIS to identify subjects that may pose a threat, such as threat to government officials; prevent access to security events, embassy and/or other secured locations.
3	U.S. Coast Guard (USCG)	Biometrics of qualifying individuals interdicted at sea or encountered in the course of boarding operations matched against DoD ABIS	Search biometrics against DoD ABIS to identify and evaluate subjects of unknown risk and intent for administrative, force protection, law enforcement, and/or intelligence actions
4	U.S. Customs and Border Protection (CBP)	Biometrics in CBP holdings matched against DoD ABIS, including biometrics of individuals encountered by CBP between ports of entry	Search biometrics against DoD ABIS to identify and evaluate subjects of unknown risk and intent for administrative, force protection, and/or law enforcement actions. Search biometrics against DoD ABIS to determine if subject encountered between ports of entry presents threat and determination for action (e.g., expedited removal or transport to station for prosecution).

5	U.S. Immigration and Customs Enforcement (ICE)	Biometrics in ICE holdings matched against DoD ABIS. ¹⁰	Search biometrics against DoD ABIS to identify and evaluate individuals identified as part of ICE law enforcement efforts to include persons encountered, arrested or detained domestically or internationally during law enforcement operations targeting immigration and customs law violations. This includes biometrics provided to ICE by foreign partners supporting ICE missions.
6	DHS Office of Intelligence and Analysis (I&A)	Biometrics submitted to I&A or biometrics that I&A has access to on behalf of DHS matched against DoD ABIS.	Search biometrics against DoD ABIS to identify and evaluate information on subjects of interest for inclusion in intelligence products or used to conduct analysis
7	DHS Office of Operations Coordination (OPS)	Biometrics submitted to OPS or biometrics that OPS has access to on behalf of DHS matched against DoD ABIS.	Search biometrics against DoD ABIS to identify and evaluate information on subjects of interest for inclusion in operational products, assessments, for law enforcement, border security, or immigration enforcement.
8	Transportation Security Administration (TSA)	Biometrics in TSA holdings against DoD ABIS for populations for which security threat assessments are conducted prior to approval of credentials, access, or other privileges.	Search biometrics against DoD ABIS to assess or refute provided information as available (e.g., DoD data contradicts information in the subject's application or demonstrates that the subject poses a threat); or demonstrates that the subject is ineligible for credential or benefit.
9	DHS	Prints collected by DHS matched against DoD latent print repository.	Search prints against DoD ABIS to identify subjects seeking admission to the United States, seeking a DHS benefit, or connected to an investigation who may be a threat, but are only identifiable via latent print matching.
10	Department of State (DOS)	(b)(7)(E)	

¹⁰ ICE prints from domestic queries are not retained by DoD.

APPENDIX B SYSTEM ACCOUNT ACCESS

System Account Access refers to one Party creating a specified number of user accounts for individuals employed by the other Party to access its systems for the purposes specified in this MOA and its Appendices.

This Appendix identifies authorized access, uses and users for particular data under this MOA for the purpose of biometric information exchange. All authorized users and uses of data described in this Appendix are explicitly stated; any changes require agreement by the Parties.

A. Users and Uses

1. The Parties will have access to information in the databases described in the chart below. The exact data and means of access will be determined and documented by the Parties through Service Level Agreements, Interface Control Documents, and Operational Protocols, as appropriate.

2. The Parties will limit access to information provided under this Appendix based on the users' clearance level and need to know the information in performance of official duties to carry out the purposes permitted under this MOA and its Appendices.

3. Neither Party will store or retain data accessed in accordance with this Appendix unless the information relates to persons who are KST or NST, or otherwise subjects of intelligence/counterintelligence investigations.

US Army Counter Intelligence	DoD access to ADIS ³	▪ Access to user accounts to conduct a targeted search of individuals who are the subjects of counterintelligence investigations.
I&A	Access to BIR ⁴ / AIMS ⁵ intelligence information	▪ Identify information on subjects of interest for inclusion in intelligence product

³ ADIS is a system for the storage and use of biographic, biometric indicator, and encounter data on aliens who have applied for entry, entered, or departed the United States. ADIS consolidates information from various systems in order to provide a repository of data held by DHS for pre-entry, entry, status management, and exit tracking of immigrants and non-immigrants. ADIS data is used in determining visa or immigration benefits eligibility and providing information in support of law enforcement, intelligence, and national security investigations.

⁴ Biometrics Intelligence Resource. BIR provides users with the unique capability to search across raw information associated with biometric collections and encounters from many different sources. The data model allows the user to query and view common data elements in an identity-based summary called the Biometrically Linked Identity Intelligence Profile (BLIIP), while providing the functionality to view entire data records when requested.

⁵ Automated Identification Management System. AIMS provide an intelligence production environment. A standard workflow ensures that an organization's research and review processes are thoroughly followed. A prioritized work queue ensures that matches are worked in the order that corresponds to the organization's threat matrix. A customized authoring tool provides all the Microsoft Word functionality and allows analysts to easily create Biometric Intelligence Analysis Reports (BIARs) in standard Intelligence Community Markup Language (ICML) format. This capability provides the foundation for a federated Biometrically Enabled Intelligence (BEI) production tool and enables information sharing.

Appendix C

DoD WATCHLIST EXPORT

I. DATA:

A. DoD will provide to DHS the UNCLASSIFIED biometrically-enabled watchlist (BEWL); these records will include available biometrics across the three primary modalities (as defined by HSPD-24), along with limited associated biographic data and DoD's threat Tier level. DoD will also provide to DHS other data sets as agreed to by both Parties.

B. DoD will automatically create, and make available to DHS analysts, biometric match reports for persons with IDENT records who match DoD biometric data, based on match requests referenced in Appendix A.

C. Further details of this exchange will be spelled out by the Parties through Service Level Agreements, Interface Control Documents, and Operational Protocols, as appropriate.

II. Processes

A. To the extent allowable, DHS will have access to, and be able to retrieve, the biometrically-linked identity intelligence profiles (BLIIP) of persons of interest (POI) with DHS records who match DoD biometric data.

B. The Parties will engage in a collaborative effort to establish the necessary mechanisms and develop SLAs and operational protocols, as appropriate, to establish database access privileges, information sharing expectations, and response times to support the provisions of this Appendix.

C. If DHS has a positive match to a DoD record, DHS will make available to DoD intelligence analysts all information in its holdings as permitted by applicable law and DHS policy, pertaining to the person of interest in question to facilitate analysis.

D. To the maximum extent appropriate considering DoD's mission and responsibilities, DHS shall provide information regarding travel partners, movement patterns, and other travel activities based on biometric and biographic encounters of DoD provided identities.

E. DHS shall provide a silent hit/protected movement capability for specified DoD records within US-VISIT.

Appendix D

SCIENCE & TECHNOLOGY PROJECTS

I. Coordination.

A. DoD and DHS shall meet regularly, in coordination with the National Science and Technology Council Subcommittee on Biometrics and Identity Management, to share information on current and future biometric S&T efforts and the direction of their respective programs.

B. Additional meetings may be scheduled as needed by mutual agreement. DoD shall host and coordinate meeting arrangements for a period of three years. Prior to the conclusion of the three-year period DoD and DHS shall reevaluate responsibilities for hosting and coordinating annual meetings.

II. Resources.

A. Both DoD and DHS shall invite the other to either observe or participate in test and exercise venues where appropriate.

B. Both Parties will share biometric test data in accordance with applicable U.S. laws and regulations.

III. Sharing of Work Product.

A. DoD and DHS shall make available to each other S&T project work products and deliverables where appropriate and in accordance with applicable U.S. laws and regulations.

B. For purposes of this Appendix, S&T work products and deliverables include, but are not limited to, whitepapers, technical reports, test reports, prototypes, and technology demonstrations.

APPENDIX E

TECHNICAL ARRANGEMENT

I. DATA

The Parties will adhere to the technical standards as identified in the Registry of USG Recommended Biometric Standards, and will update their standards consistent with the Registry as appropriate.

II. TECHNOLOGY

All technical exchanges will be covered with technical specifications detailing the formats and exchange protocols as identified in the ANSI/NIST ITL 1-200X Family and associated with the National Information Exchange Model (NIEM) technical framework. The Parties are committed to updating the information technologies employed to implement this MOA and to ensure that the system remains efficient as data volumes increase and more advanced technologies become available.

III. TECHNICAL DOCUMENTS

The Parties will jointly draft Service Level Agreements, Interface Control Documents, and Operational Protocols to achieve the technical milestones required for the sharing envisioned under this MOA.

FOR OFFICIAL USE ONLY

APPENDIX F

IDENTITY & BIOMETRIC COORDINATION

I. Coordination

- A. As two of the largest federal Departments with vetting and biometric credentialing responsibilities, DoD and DHS mutually require the credentialing and vetting of similar populations – resulting in both overlap and inconsistency of guidance and requirements. DoD and DHS shall meet at least annually, in coordination with Federal Identity & Credentialing and Access Management (FICAM) Committee, to review policy and information on current and future efforts and the direction of respective programs to develop more consistent policy to reduce inconsistent requirements while concurrently safeguarding and protecting public privacy.
- B. Additional meetings may be scheduled as needed by mutual agreement.

II. Processes

- A. To the extent allowable, DoD and DHS will commit to utilize Federal Information Processing Standard (FIPS)-201 and FIPS-201 Interoperability policy, guidance, and standards to reduce confusion and mitigate inconsistent guidance for overlapping populations.
- B. To the extent allowable, DoD and DHS will have access to, and be able to electronically validate the current status of Government-issued credentials, and as further delineated in associated ICDs, SLAs, Operational Protocols and any other related project documentation separately agreed and approved by the parties.
- C. Review the feasibility of the use and migration of existing Personal Identity Verification (PIV) compatible credentialing efforts to PIV / PIV Interoperable framework. This includes acceptance of Transportation Worker Identification Credentials (TWIC) as well as availability of TWIC for Non-Maritime Transportation Security Act populations for common high risk functions (i.e., Arms, Ammunition and Explosives Drivers and Propellant Drivers).

III. Resources

- A. DoD and DHS shall invite the other Party to either observe or participate in test and exercise venues where appropriate.
- B. Both Parties will share electronic-identity media and authentication system test data in accordance with appropriate U.S. Government laws and regulations.

IV. Sharing of Work Product

- A. DoD and DHS shall make available to each other products and deliverables where appropriate and in accordance with applicable U.S. Government laws and regulations.

- B. For purposes of this Appendix, products and deliverables include, but are not limited to, whitepapers, technical reports, specifications, test reports, prototypes, and technology demonstrations.

APPENDIX G

FEDERATED PRIVILEGE MANAGEMENT/ATTRIBUTE MANAGEMENT PROJECTS

I. Federated Privilege Management

A. As part of future planned activities, the Parties will seek to share biographic data, often referred to as “attributes,” through federated means to further support the information sharing goals of the Parties.

B. For purposes of this MOA, a *federation* is defined as a group of two or more trusted partners with business and technical agreements that allow a user from one Party to seamlessly access information resources from the other Party in a secure and trustworthy manner.

C. Technical interface

1. The federation established between the Parties will provide a standardized means for allowing the Parties to directly provide services to the other Party, and after the business rules established by the Parties have been met.

2. The Parties will each retain control over the business rules for granting access to the sensitive information it owns and will determine whether to grant or deny access to the service or information requested by the other Party.

II. Attribute/Privilege Management

A. The Parties will work toward an Attribute / Privilege Management framework for enabling flexible and fine-grained access control for assured information sharing.

B. The Parties, through project-level documentation as appropriate, will identify the systems and resources required to order, create, disseminate, modify, suspend and terminate management controls that implement Information Assurance (IA) services, processes, and devices across the enterprise. On a large scale, an information environment comprises multiple federated enterprises connecting computers, local area networks, and tactical assets. The service-based architecture of the enterprise will mediate access securely to a host of physical and logical systems.

C. Technical interface

1. The Parties will jointly test the utility of credential, vetting and matching mechanisms across enterprise domains with varying degrees of assurance, multi-layered policy to accommodate federated partners, and/or other federation dependencies.

2. Any capability agreed to by the Parties will allow the Parties to maintain control over their user communities and partnerships; leverage available capabilities; provide the ability to control levels of access based on how the user was credentialed

(authentication “level of assurance”); and provide “measures of confidence” for the information required by an authorization policy to make access control decisions.

III. Mutual objectives

The Parties agree to work toward the following high-level objectives. Additional information and level of detail will be available in program-level documentation as appropriate:

- A. Demonstrate viability within at least one architectural areas.
- B. Demonstrate viability of a federated operational environment by enabling assured information sharing of resources on the internet with unclassified users external to the Parties’ enterprise.
- C. Incorporate distinct “levels of assurance” and “measures of confidence” into authorization policy to support multiple types of authentication mechanisms, metadata, and attributes according to the criteria provided.
- D. Integrate heterogeneous commercial off the shelf products (COTS) that incorporate applicable industry standards.
- E. Increase Information Assurance posture across the entire federated operational mission.

APPENDIX H DHS IDENT EXPORT

I. BACKGROUND

This Appendix addresses the export of select categories of subjects of interest of the Department of Homeland Security's (DHS's) Automated Biometric Identification System (IDENT) to the Department of Defense (DoD) and serves as a companion document to Appendix A and Appendix C of the "Memorandum of Agreement between DoD and DHS on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activities" ("DHS-DoD MOA"). Sharing provided under the rules set by this Appendix will be subject to the limitations of the DHS-DoD MOA and all applicable regulations and statutes.

The select categories of data shared under this Appendix, and the terms and conditions of such sharing, including the period for which DoD may retain the IDENT data, will be identified in the Operational Protocols document.

DOD will utilize DHS biometric data derived from DHS IDENT in accordance with uses specified in the MOA and associated Appendices A and C. These uses include: warfighter operations, detainee affairs, anti-terrorism, force protection, special operations, stability operations, homeland defense, counterintelligence, and intelligence.

II. DATA

DHS will provide the UNCLASSIFIED IDENT select categories, where DHS is the authoritative data owner; these records will include available biometrics, along with associated biographic and contextual data.

III. TRANSMISSION OF DATA

The select categories and the mechanism for sharing IDENT information with DoD will be memorialized in associated Service Level Agreements (SLAs), Interface Control Documents (ICDs), Operational Protocols, and any other related project documentation separately agreed to and approved by the Parties, as described in section VI.B. of the MOA. Additional mitigation strategies may be identified and implemented at that time.

There will be no data shared under this Appendix until the terms of this Appendix and the separate Operational Protocols document are agreed to between DHS and DoD. Once the Operational Protocols document is finalized it will be incorporated as a separate Appendix to the MOA.