Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 8, 2021

ACTION

MEMORANDUM FOR THE ACTING UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS

FROM: [redacted]
Acting Director of Field Operations Division [redacted] Digitally signed by [redacted] Date: 2021.03.11 11:14:43 -05'00'

THROUGH: [redacted]
Deputy Under Secretary for Intelligence Enterprise Operations [redacted] Digitally signed by [redacted] Date: 2021.03.11 15:26:44 -05'00'

SUBJECT: **Request the Acting Under Secretary for Intelligence and Analysis Signature on Memoranda of Agreement (MOA)**

Purpose: This is a cover memorandum seeking the Acting Under Secretary for Intelligence and Analysis' signature on the attached Memoranda of Agreement (MOA) with the Wisconsin Department of Justice, Division of Criminal Investigation (WSIC).

Background or Context: Attached is the MOA that describes the partnership and responsibilities of the Department of Homeland Security, Office of Intelligence and Analysis, and the Wisconsin Department of Justice, Division of Criminal Investigation. The Office of General Counsel, Intelligence Law Division, has reviewed this MOA and has no legal objections.

Recommendation: FOD recommends that you sign the attached MOA.

Approve _____ Disapprove _____

Modify _____ Needs more discussion _____

Attachment:
Wisconsin Department of Justice, Division of Criminal Investigation MOA

MEMORANDUM OF AGREEMENT

BETWEEN THE

DEPARTMENT OF HOMELAND SECURITY

[OFFICE OF INTELLIGENCE AND ANALYSIS]

AND

THE WISCONSIN DEPARTMENT OF JUSTICE, DIVISION OF CRIMINAL INVESTIGATION

I. PURPOSE. This Memorandum of Agreement (MOA) describes the partnership and responsibilities of the Department of Homeland Security (DHS), [Office of Intelligence and Analysis (I&A)] and the Wisconsin Department of Justice, Division of Criminal Investigation each individually, "Party," and collectively, "Parties," in an effort to:

(1) Provide direct national-level intelligence support to the Host through the assignment of DHS [I&A] personnel to facilitate intelligence and information sharing consistent with any applicable laws;

(2) Serve as an interface between the Host and the national Intelligence Community (IC) (as defined in 50 U.S.C. 40la)

(3) Manage, analyze, fuse, tailor and disseminate information in accordance with applicable laws, rules, regulations and authorities, and to facilitate the identification and prevention of threats within the scope of DHS's authority, as defined generally by the Homeland Security Act of 2002, as amended, and Executive Order 12333, as amended;

(4) Provide DHS support and coordination to the principal officials of the designated Host fusion center, federal, state, local, tribal, and private sector homeland security officials, and the Homeland Security Advisor of that state, in accordance with section V of this MOU, 6 U.S.C. § 124h, and in addition to those specific functions assigned elsewhere in law to DHS/[I&A]; and

(5) Improve communication and coordination among federal, state, local, tribal and private sector organizations and assist in developing methods to exchange relevant information in support of homeland security responsibilities of each organization.

II. AUTHORITY. This MOA is entered into by DHS pursuant to the Homeland Security Act of 2002, as amended, 6 U.S.C. §§ l21(d), 124h, 481, and 482; the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485; Executive Order 13311, "Homeland Security Information Sharing," July 29, 2003; Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," Oct. 25, 2005; and Executive Order 12333, "United States Intelligence Activities," Dec. 4, 1981, as amended.

This MOA is entered into by the Host pursuant to Wisconsin Statutes Chapter 16, Subchapter IV

III. DEFINITIONS. For purposes of this MOA, the following terms shall have the following meanings when used herein:

A. "Classified Information" has the meaning given that term in 50 U.S.C. § 426, that is, information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

B. "Sensitive But Unclassified Information" shall refer generally to unclassified information in the possession of either Party to this MOU to which access controls or distribution limitations have been applied in accordance with applicable laws, policies, or regulations. It may include any locally-defined handling caveat or marking authorized for use by either party. It also includes unclassified information in the possession of the U.S. Government that may be exempt from public disclosure or subject to other controls.

C. "State and Major Urban Area Fusion Center" means a collaborative effort of two or more federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal, terrorist, or other activity related to homeland security.

D. ""I&A Field Personnel" means employees of I&A assigned, detailed, or deployed to Federal, State, local, tribal, and territorial offices physically located outside of I&A Headquarters. These individuals will not perform duties as an employee or official representative of the Host.

E. "Homeland Security Information" has the meaning given that term in 6 U.S.C. § 482, that is, any information possessed by a federal, state, or local agency that (a) relates to the threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist

activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act. Such information may be "Classified Information" or "Sensitive but Unclassified Information." "Joint-seal intelligence product" means a finished intelligence product in any format which is represented as the combined work product of both the Host and DHS. In some instances, such products may feature the seals or letterhead identifying both the Host and DHS as well as other partner agencies.

F. "Information Sharing Environment" means the information sharing environment established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485.

G. "Homeland Security Data Network" means the classified wide-area network utilized by DHS, DHS Components and other partners, providing effective interconnections to the intelligence community and federal law enforcement resources.

H. "Homeland Security Information Network" means the trusted network for homeland security mission operations to share Sensitive But Unclassified (SBU) information. Federal, State, Local, Territorial, Tribal, International and Private Sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

I. "Intelligence-led policing" means the collection and analysis of information to produce an intelligence product designed to inform law enforcement decision making at the tactical and strategic levels.

J. "Terrorism information" has the meaning given that term in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485, that is, all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to – (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individual to the United States, United States persons, or United States interests, or to those of other nations; (c) communications of or by such groups or individuals; or (d) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and includes weapons of mass destruction information.

K. "Personally Identifiable Information" (PII) means information which can be used to distinguish or trace the identity of a U.S. Citizen or lawful permanent resident, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

I. "Privacy Incident" means the suspected or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII in usable form, whether physical or electronic.

IV. SCOPE.

A. Nothing in this MOA shall be construed as encroaching upon the sovereign rights, privileges, and immunities of either Party, by the other, in the conduct of inherently municipal, state or federal government operations, except as may be authorized pursuant to the U.S. Constitution. Nothing in this MOA is intended to conflict with current law, regulation, or the policies and directives of DHS or the Host. If a term or condition of this MOA is inconsistent with such authorities, the Parties agree to address and resolve the inconsistency in a timely and legally appropriate manner, unless the matter is incapable of timely resolution, in which case the inconsistent term shall be deemed invalid, but the remaining terms and conditions of this MOA shall remain in full-force and effect.

B. This MOA, in and of itself, does not result in the commitment, obligation, or transfer of funds or other financial obligations between the Parties. No provision of this MOA shall be interpreted to require obligation or payment of funds in violation of the Anti-Deficiency Act, Title 31 U.S.C. § 1341.

C. The following activities are specifically excluded from this MOA:

(1) Short-term (usually no more than 30 days) operational DHS support, including through temporary assignments of DHS personnel, to the Host.

(2) Assignments or intergovernmental details, per other formal agreements, which are based on cooperative joint training efforts in which training population drives instructor and support assignments for the training.

(3) Assignment of contractor personnel to the Host to perform contractor services in support of DHS.

V. RESPONSIBILITIES.

A. **DHS Responsibilities.** DHS [I&A] shall select and assign, on a non-reimbursable basis, one or more DHS [Intelligence] I&A Field Personnel to coordinate with and facilitate DHS support to the Host [in the exchange of relevant intelligence and information] consistent with applicable federal statutes, executive orders, Department regulations and policies. DHS

will:

(1) ensure that the assigned DHS [Intelligence] Officer is provided [secure data and telecommunications systems capabilities in appropriately certified and secured space and facilities provided by the Host];

(2) ensure the assigned DHS [Intelligence] Officer is appropriately trained to perform [intelligence analysis or information sharing, including training to support intelligence-led policing, privacy and civil liberties training that is developed, supported, or sponsored by the DHS Chief Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties, and such other training as prescribed by the Under Secretary for I&A;

(3) ensure, to the extent practicable, any anticipated or expected absence of a DHS Officer which exceeds 30 consecutive days is physically or virtually covered by the temporary assignment of a DHS [Intelligence] Officer in a manner consistent with ensuring continuous support to the Host; and

(4) provide necessary personnel management/human capital support for DHS [Intelligence] I&A Field Personnel, in accordance with Office of Personnel Management (herein after "OPM") and DHS regulations and guidelines, including consideration for promotions, awards, and other administrative actions.

B. **Host Responsibilities.** The Host shall, consistent with applicable federal and state statutes, regulations, executive orders and policies:

(1) provide office space, parking, unclassified data and telecommunications systems, and any administrative office supplies necessary to perform the tasks under this MOA;

(2) provide access to all Host facilities, equipment, and technical information that are required to perform the duties outlined in this MOA;

(3) consistent with applicable authorities, policies and procedures of the Parties, provide access to Host databases, reports, investigations, and other information produced, retained, and/or controlled by the Host in order to review this information and assist the Host in identifying the types of information, including enforcement information, that may assist DHS or other entities with homeland security responsibilities;

(4) as appropriate, disseminate DHS and joint-seal intelligence products to local consumers consistent with dissemination guidance provided by DHS or in coordination with and following the concurrence of the DHS [Intelligence] Officer assigned to the Host;

(5) annually participate and provide data for DHS-led capability and performance assessments, consistent with the Federal Resource Allocation Criteria (RAC) Policy, and ensure compliance with all annual homeland security grant program (HSGP) requirements

for fusion centers and similar [intelligence] entities; and

(6) promptly notify DHS following a privacy incident involving information originating with DHS.

C. **DHS [Intelligence] Officer Responsibilities.** Consistent with their functional duties and responsibilities as designated by DHS, DHS [Intelligence] I&A Field Personnel will:

(1) provide information sharing; collection and reporting; and analysis expertise, advice, training, support and assistance;

(2) coordinate with the Host to identify information needs and transform them into information requirements and product requests;

(3) track information requests and the delivery of responsive information and intelligence products and provide feedback from the Host to the producers;

(4) create intelligence and other information products derived from Host and DHS information and other homeland security-relevant information;

(5) consistent with applicable authority, access relevant databases, reports, investigations, and other information produced, retained, and/or controlled by the Host in order to review this information and assist the Host in identifying the types of law enforcement information that may assist DHS or other entities protecting the United States;

(6) consistent with DHS authorities and DHS and Intelligence Community requirements, support efforts of the Host to report information that may assist DHS fulfill its mission, as well as support other entities protecting the United States;

(7) support efforts of the Host to participate in the information sharing environment;

(8) coordinate with other relevant federal entities engaged in homeland security-related activities;

(9) carry out such other duties as the Secretary of Homeland Security determines are appropriate;

(10) refrain from exercising any supervisory or disciplinary authority over personnel of the Host's facility or participating offices; and

(11) ensure that products intended to be issued and/or disseminated by the Host as joint- seal intelligence products have been reviewed and cleared by DHS according to established DHS procedures for disseminating finished intelligence products.

VI. INFORMATION SHARING AND HANDLING

A. **Key Principles.** The following key principles and standards apply to the sharing of information between the Parties in any form including verbal, paper, electronic, audio and visual:

(1) sharing must always be in furtherance of the official duties undertaken by the Parties;

(2) the originator of the information to be shared is considered to be the owner of that information and is accountable for deciding how information will be shared in a manner that will ensure the timely and efficient access by the Parties to all information necessary to discharge their official duties;

(3) the Parties will ensure that information will be appropriately marked to indicate the presence of handling, safeguarding, or dissemination controls and is provided with the expectation that these controls will be preserved;

(4) the sharing of personally identifiable information (PII) must be limited to that which is reasonably necessary for the intended recipient to understand, assess, or act on the information provided;

(5) privacy policies and relevant privacy compliance documents, such as Privacy Act notices (including systems of records notices and "(e)(3)" or similar notices) will be issued, reviewed, and revised as appropriate to ensure that they properly describe the treatment of PII;

(6) information sharing must comply with all applicable laws, regulations, or procedures and will incorporate protection mechanisms for handling of proprietary information;

(7) the use of data by an employee of either Party in an unauthorized or illegal manner will result in a review of the factual circumstances by both Parties and potentially subject the employee to appropriate remedial actions;

(8) to maintain data accuracy, where necessary, the Parties will be informed of any changes to the data they have received and also notify the source of any error they discover;

(9) the Parties will ensure that all staff are educated to manage sensitive information appropriately consistent with these principles and organizational policy on the collection and uses of information during the performance of official duties;

(10) the Parties will ensure that any third parties providing a service to them agree and abide by these principles by inclusion in contracts/agreements;

(11) dissemination of information from one Party to another shall not be considered a release of information to the public, nor shall it constitute a waiver of any exemption to the release of information under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 or the Wisconsin Statutes Chapter 19.

(12) any Party in receipt of a request for information (whether pursuant to a FOIA, "sunshine," or discovery law) whose scope includes information shared by the other Party or documents developed jointly by the Parties, shall (a) consult with that Party prior to any disclosure, with the aim of developing a consensus view regarding an appropriate response, or
(b) refer the request to the originating Party for a direct response to the requester;

(13) information will be classified, marked, and accessed, as appropriate, pursuant to Executive Order 12958, as amended, and Executive Order 12968; and

(14) joint-seal intelligence products will be issued and/or disseminated in accordance with both parties' policies and clearance procedures.

B. Notwithstanding the paragraphs above, the Parties may use, disclose, reproduce, or retain, in accordance with the law of the state and applicable Host policy, any Party provided data or information (except data or information properly classified in accordance with Executive Order l2958) that is or was:

(1) already in the public domain at the time or which thereafter enters the public domain without fault or breach of this MOU by the Party;

(2) already made known to or lawfully acquired from a third party by the Party;

(3) previously disclosed to the Party without restriction from the other Party; or

(4) provided or disclosed to, or independently acquired by, the Party without restrictions from its originating source.

C. Notwithstanding the paragraphs above, pursuant to 6 U.S.C. § 482, Homeland Security Information obtained by a state or local government from a federal agency shall remain under the control of the federal agency, and a state or local law authorizing or requiring such a government to disclose information shall not apply to such information. The state or local agency shall: (a) withhold such information from any response; (b) release such information only with the expressed approval of the federal agency; or (c) refer the request to the originating federal agency for a direct response to the requester.

VII. SECURITY REQUIREMENTS.

A. The DHS I&A Field Personnel, in order to meet his or her mission objectives, shall have appropriate access to all relevant federal databases and information systems, consistent with any applicable policies, guidelines, procedures, instructions, or standards established by the President of the United States or, the program manager of the information sharing environment for the implementation and management of that environment, or as otherwise limited by federal law. This shall require that at a minimum, the DHS I&A Field Personnel must have an active security clearance at the level of Top Secret, and be read-on to Sensitive Compartmented Information (SCI) accesses as required.

B. Host will provide the DHS Officer with any local clearance or access necessary to accomplish duties consistent with DHS's mission responsibilities.

C. Host will protect the identity and personal information of the DHS Officer from public disclosure and will refer all inquiries regarding the presence of the DHS Officer to the DHS Public Affairs Office.

For purposes of access to Host information, the DHS Officer shall be considered a federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be considered by Host as authorized to receive information from law enforcement agencies.

VIII. DISCIPLINE AND REMOVAL.

A. Federal employees are subject to the Ethics in Government Act of 1978, 5 C.F.R. part 735, which regulates employee responsibilities and conduct; the Federal Trade Secrets Act, 18 USC, Section 1905; as well as DHS-specific standards of conduct regulations;

B. The Host may not take disciplinary or other administrative action against a DHS Officer who commits a violation under similar Host procedures and regulations governing the conduct of Host employees. DHS however, will take such administrative or disciplinary action against the DHS Officer as may be appropriate under the specific circumstance; and

C. Host will coordinate with the DHS [Intelligence] Officer's chain of command regarding any issues requiring management oversight or discipline. DHS [I&A] will address those issues and make every efforts to resolve them to the satisfaction of all parties to this MOA.

IX. DISPUTES.

A. Disputes arising under or relating to this MOA shall be resolved only through consultations between the Parties. The dispute shall not be referred to any outside Party or to any other forum for settlement without the consent of both Parties.

B. The Host will not pursue any claims against the U.S. Government or its employees, including, but not limited to claims for money, reimbursement of expenses, benefits or salaries paid to any of the Host's employees for its compliance with the responsibilities described within the terms of this MOA. This provision not to pursue any claims applies to past, present, and future compliance with the responsibilities described within the terms of this MOA and is retroactive to and includes claims for compliance with the responsibilities previously provided by the Host to DHS that are consistent with the responsibilities described within the terms of this MOU. This MOU does not waive remedies otherwise available to the Host under the Federal Tort Claims Act or other federal legislation expressly authorizing a private right of action for damages against the U.S. Government.

X. OTHER PROVISIONS.

A. Nothing in this MOA is intended to conflict with current law or regulation or the directives of either Party. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOU shall remain in full force and effect.

B. Under the Inspector General Act of 1978, as amended, 5 USC App. 3, a review of this MOA may be conducted at any time. The Inspector General of the Department of Homeland Security, or any of his or her duly authorized representatives, shall have access to materials of the Parties, consistent with applicable authorities of the Parties, in order to perform audits, inspections, investigations, or other examinations of the DHS I&A Field Personnel, as authorized by law.

C. Any travel or training will be processed through travel orders with applicable reimbursement paid by the Party that requested and authorized the travel or training. All DHS Officer travel and training will be conducted in accordance with applicable DHS Management Directives and regulations, and the Federal Travel Regulations.

D. Nothing in this MOA shall, or is intended to confer any substantive or procedural right, and this MOA shall not be construed to create a private right of action for enforcement of any of its provisions or a defense to noncompliance with any independently applicable legal obligation.

XI. ENTRY INTO FORCE, AMENDMENT, DURATION AND TERMINATION.

A. All obligations of the Parties under this MOA shall be subject to the availability of properly authorized and appropriated funds for such purposes.

B. This MOA shall become effective upon signature by both Parties and shall remain in effect for an indefinite period.

C. This MOA may be amended by the written agreement of both Parties.

D. This MOA shall supersede any and all prior arrangements regarding DHS I&A Field Personnel entered into by the Parties or their respective organizations, units, or agencies.

E. This MOA may be terminated at will by any party upon ninety (90) days after written notification to the other Party.

F. This MOA may be signed in counterparts, each of which shall be considered to be an original. For the Department of Homeland Security:

Wisconsin Department of Justice
Eric Son, Deputy Attorney General

Date: 2-3-2020

Acting Under Secretary for Intelligence and Analysis
US Department of Homeland Security

Date: 4/8/2021