Domain Stewardship Agreement between

The National Information Exchange Model

Program Management Office (NIEM PMO)

and

# PARTIES

This Domain Stewardship Agreement (DSA) is entered into by and between The National Information Exchange Model (NIEM) Program Management Office (PMO) and , hereafter, jointly referred to as the “Parties” and individually as a “Party.”

# AUTHORITY

This DSA is entered into pursuant to the MOA which established NIEM as a partnership between the U.S. Department of Justice (DOJ) and U.S. Department of Homeland Security (DHS), on April 19, 2005. Among other responsibilities, this directive defines how data shall be maintained and made visible to authorized users. This DSA serves to establish a governing Community-of-Interest (COI) for a new dataset that will be added to NIEM in the form of a new domain, an extension to an existing domain, or modifications to the NIEM Core. Expectations of all parties with regard to the governance, oversight, and long-term maintenance are defined here.

# PURPOSE

NIEM is a partnership between the DOJ and DHS. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information and support the day-to-day operations of agencies throughout the nation. NIEM defines data-exchange standards for information that is commonly shared across the broad justice, public safety, emergency and disaster management, intelligence, and homeland security enterprises. The standards derive from actual exchanges that support the day-to-day operations of officials at all levels of government, as well as the private sector and the general public.

NIEM is organized by domains. There is a central ‘core’ to the NIEM model; from this point forward to be referred to as the *NIEM Core*, which represents elements that are used by multiple domains to develop information exchanges. NIEM Core is updated and maintained by the NIEM PMO. Additional domains are developed around mission areas and maintained by a self-sustaining domain governance body, from this point forward to be referred to as a *Domain Steward*. The Domain Steward is represented by a COI comprised of participants from one or many organizations/components/agencies at the Federal, State, Local or Tribal levels.

The purpose of this DSA is to establish the Domain Steward that will govern and maintain the  *Domain* dataset and define the expectations and responsibilities of involved parties.

# RESPONSIBILITIES

The shall act as the Domain Steward providing:

* A contact list of all members and organizations represented by the newly established COI that will serve as the steward and governing body of the new domain; this shall include indication of a primary point-of-contact who will interface regularly with NIEM PMO;
* A common data dictionary of elements to be included in NIEM which spans across the Federal/State/Local/Tribal/Private/International boundaries represented by the COI;
* A completed executive summary coversheet and Component Mapping Template (CMT) for the Domain, conforming to the NIEM Naming and Design Rules (NDR). Templates for the executive summary and CMT are maintained by the NIEM PMO – the NDR is available through www.NIEM.gov;
* A charter documenting the governance processes related to release management and publication (including a planned schedule) as defined in the NIEM High Level Version Architecture (HLVA);
* Participation in NIEM harmonization and reconciliation activities as required by the NBAC;
* Reporting of NIEM technical issues using the issues tracking tools provided by the NIEM PMO and the NIEM Helpdesk;
* Submission of all formal comments regarding technical or policy issues through the issue tracking tools provided by the NIEM PMO for resolution tracking and auditing;
* Support domain reconciliation and cross-domain harmonization resulting in future NIEM releases (both major and minor) as needed;
* Provide Tier 2 and 3 technical support for domain specific issues related to NIEM and IEPD development to assist implementers and developers;
* Understanding and incorporation of related external data standardization initiatives as appropriate; and
* Ongoing identification of data requirements based on exchange/data modeling and development efforts

NIEM PMO shall provide:

* Assessment of proposed domain documentation, and suggested implementation into NIEM;
* Defined governance processes that support domain self-governance by authorized COIs, and clear guidance as to how processes fit into the larger NIEM structure;
* Versioning and maintenance of NIEM Core including taking the lead on cross-harmonization efforts;
* A repository source for the maintenance of all published IEPDs to local, tribal, state, Federal and private entities;
* Implementation guidance and support for NIEM including general help desk support;
* Training and outreach support;
* Support for the creation of a common data dictionary across domains;
* Development and continued maintenance of NIEM tools; and
* Updates on policies and standards that may impact domain self-governance or NIEM adoption.

The overall intent and goal of this DSA is to create a working guideline to establish a unified strategy for domain development and maintenance.

NIEM will not endorse products or service offerings from any particular company or organization based on this DSA.

# FUNDING

This DSA shall not be used to obligate or commit funds or as the basis for the transfer of funds between the Parties.

# POINTS OF CONTACT

For NIEM PMO:

Donna Roy

Department of Homeland Security

Office of the Chief Information Officer

Washington, DC

(202) 282-9635

donna.roy@dhs.gov

For :

[Insert full name here]

[Insert office name here]

[Insert mailing address here]

[Insert phone number here]

[Insert email address here]

# TERMS OF AGREEMENT, TERMINATION

The term of this DSA shall be from [Insert from-data here] to [Insert to-date here] unless canceled in writing by either Party with a minimum of 30 days prior notice to the other Party. Representatives from the Parties will meet quarterly to review the operation, and the results achieved, under this DSA.

# MODIFICATIONS

This DSA may be modified on the mutual written consent of the signatories hereto or their designees.

# EFFECTIVE DATE

This DSA is effective on the date of last signature of the Parties’ approval authorities in Section XI - Approvals.

# MISCELLANEOUS

1. Nothing in this DSA is intended to supersede current law or regulation. If a term of this DSA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this DSA shall remain in full force and effect.

2. This DSA in no way restricts either Party from participating in similar activities or arrangements with other public or private agencies, organizations, or individuals.

3. This DSA describes in general terms the basis upon which the Parties intend to cooperate. This DSA does not intend to create any rights, privileges, or benefits, substantive or procedural, enforceable by any individual or organization against the United States; its departments, agencies, or other entities; its officers or employees; or any other person.

4. Sensitive But Unclassified Information. The Parties will cooperate with each other to protect Sensitive But Unclassified (SBU) information, and any other information identified by the furnishing Party as in need of special security controls. If such information is either created or provided by one Party to the other, the furnishing Party will mark the data accordingly and the receiving Party will protect it from unauthorized disclosure, including release to the public. At a minimum, the Parties will protect Sensitive But Unclassified Information in accordance with DHS management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.

5. Information Releases and Non-Disclosure. Before any information pertaining to activities performed pursuant to this DSA is made available to the public, the Parties will review and concur that the information may be released. Nonfederal government employees performing activities pursuant to this DSA who may have access to Sensitive But Unclassified Information (e.g., For Official Use Only) shall sign the DHS form Non-Disclosure Agreement (DHS Form 11000-6) and shall safeguard such information in accordance with DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.

# APPROVED BY:

**Representative Signature:**

Date: \_\_\_\_\_\_\_\_\_\_\_\_

Print Name: [Insert full name here]

Title: [Insert title here]

**NIEM PMO Representative Signature:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_

Print Name: Donna Roy

Title: Executive Director, NIEM