



National Information Exchange Model (NIEM)

Military Operations Domain Charter

September 8, 2016

A handwritten signature in black ink, which appears to read "Stuart A. Whitehead". The signature is written in a cursive style and is positioned above a horizontal line.

STUART A. WHITEHEAD, SES
Deputy Director for Cyber and Command,
Control, Communications and Computers Integration, J6

Document Change Control Page

No.	Approver	Date	Description
1	Domain Steward	02 Jun 2014	Initial Release
2	Domain Steward Representative	01 Aug 2016	Stakeholder review / updates
3	Domain Steward Representative	07 Sep 2016	Administrative format updates

Table of Contents

1. References	1
2. Introduction	1
2.1 Document Scope.....	2
2.2 National Information Exchange Model (NIEM) Background.....	2
3. Authority.....	2
4. Military Operations Domain (MilOps) Overview.....	3
3.1 Domain Purpose	3
3.2 Domain Scope.....	3
5. Governance.....	5
5.1 MilOps Domain Governance Structure	6
5.1.1 MilOps Domain Steward.....	6
5.1.2 MilOps Domain Configuration Control Board (CCB)	6
5.1.3 Sub-Working Groups and Tiger Teams	7
5.2 Governance Meetings and Reporting	7
5.3 Relationships and Dependencies.....	8
6. MilOps Domain Operations and Communication	8
7. Domain Metrics.....	8

1. References

This compilation of documents is the basis for DOD's establishment of the MilOps Domain and provides additional key information regarding NIEM.

- a. DOD Information Enterprise Architecture (DOD IEA), Version 2.0, 10 August 2012.
- b. DOD CIO memo, Adoption of the National Information Exchange Model with the Department of Defense, 28 March 2013
- c. DODI 8320.02, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, 5 August 2013.
- d. DODI 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, 3 August 2015
- e. Establishing Domain Governance: Making Self-Service a Reality, NIEM Business Architecture Committee (NBAC), February 2009, v1.0.
- f. NIEM High-Level Version Architecture, NIEM Technical Architecture Committee (NTAC), 31 July 2008, v.1.0, available from <https://reference.niem.gov/niem/specification/high-level-version-architecture/3.0/high-level-version-architecture-3.0.html>.
- g. Office of Management and Budget, Digital Government: Building a 21st Century Platform to Better Serve the American People (May 23, 2012), available at <http://www.whitehouse.gov/sites/defaultfiles/omb/eqov/digital-government/digital-government-strategy.pdf>.
- h. Office of Management and Budget Memo M-13-13, May 9 2013, Open Data Policy Managing Information as an Asset. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>.
- i. NIEM Military Operations Domain Stewardship Agreement signed 13 November 2013.

2. Introduction

In reference (a), The Department of Defense Chief Information Officer (DOD CIO) identified the National Information Exchange Model (NIEM) as the best suited standards-based approach for enhancing the interoperability and standardization of DOD information exchange content. NIEM offers a proven approach for developing standardized, reusable information exchange packages and has been adopted across international, federal, state, local, and tribal agencies. Reference i; as one part of the overall DOD NIEM adoption, the DOD CIO requested the Joint Staff J6 become the Domain Steward for the Military Operations (MilOps) Domain. The JS J6 established a new Military Operations (MilOps) Domain within the NIEM construct. In combination with the existing NIEM Core and domains, the NIEM MilOps Domain supports development of information exchange specifications across the full range of military operations. (Joint Staff J6 Memorandum dtd 12 April 2013). A NIEM domain is an aggregation of stakeholders into a community of interest (COI) that are aligned to the domain's mission space by affiliation, mission, or function. The MilOps Domain is an operational mission focused venue designed to provide multi- functional,

cross-organizational data elements that DOD and non-DOD information exchange developers may use in creating NIEM-based information exchanges.

2.1 Document Scope

This Charter describes the purpose, scope, goals, and governance structure of the MilOps Domain. This Charter is supplemented by the MilOps Domain Operations and Maintenance Plan.

2.2 National Information Exchange Model (NIEM) Background

NIEM is a community-driven, government-wide, standards-based approach to exchanging information. The model was originally designed to develop, disseminate and support enterprise-wide information exchange standards and processes to enable cross-jurisdictional information sharing in emergency situations, as well as support the day-to-day operations of agencies nationwide. NIEM has grown into a working and collaborative partnership among governmental agencies, operational practitioners, systems developers, standards bodies, and other stakeholders at all levels of government. Used in all 50 states and internationally, it includes a data model, governance, training, tools, technical support services, and an active community to assist users in adopting a standards-based approach to exchanging data.

NIEM uses the Extensible Markup Language (XML) standard as a foundation to enable improved information sharing. The NIEM data model consists of two sets of closely related vocabularies: NIEM Core and individual NIEM Domains. NIEM Core represents elements commonly understood across all NIEM domains, and is updated and collaboratively maintained by the NIEM Business Architecture Committee (NBAC). The individual NIEM domains contain mission-specific elements that build upon NIEM Core concepts, and are managed through independent stewards.

DOD participation in NIEM complies with Office of Management and Budget guidance for U.S. government departments and agencies to merge information exchange standards and build common-sense exchanges that sustain multiple, future information enterprise development and applications.¹ Adoption of NIEM offers potential efficiencies and streamlined governance in delivering improved information sharing across the DOD and with DOD's mission partners.

3. Authority

In reference (b), the DOD CIO announced the intent for DOD-wide adoption of NIEM and the establishment of a MilOps Domain. Language in the DOD CIO memo states that except as required otherwise by law or DOD policy, the use of National Information Exchange Model (NIEM)-based exchanges must be considered for all new Extensible Markup Language (XML) information exchanges created and for all XML information exchanges being modernized as part of the normal lifecycle management for these information exchanges.

¹ Office of Management and Budget Memo M-13-13, May 9 2013, Open Data Policy-Managing Information as an Asset.

4. Military Operations Domain Overview

3.1 Domain Purpose

The purpose of the MilOps Domain is to provide and maintain unique military operations and missions data components used to define NIEM Information Exchange Package Documents (IEPDs) that satisfies mission critical information sharing requirements within DOD, and/or with other Federal government agencies, and Mission Partners.

Specific areas of projected improvement include:

- a. Intra-DOD data and information sharing conducted for national security missions;
- b. DOD's interagency information sharing ability and support to the national emergency response system during disaster and catastrophic events;
- c. Further alignment of Extensible Markup Language (XML) data standards within DOD, aimed at improving the visibility, understandability, accessibility, trust and interoperability of shared data; and,
- d. Further development of information exchange development tools as a reusable resource within DOD.

3.2 Domain Scope

The NIEM MilOps domain manages those unique military operations and mission data components used to define NIEM Information Exchange Package Documents (IEPDs) that satisfies operational mission information sharing requirements among DOD and its Mission Partners.

- a. The MilOps domain follows the NIEM governance construct: a domain steward, a domain steward agreement, and a domain charter. The domain data components are managed by the domain steward through the MilOps Configuration Control Board (CCB).
- b. The MilOps domain is sponsored by the DOD, but it is not a "DOD-unique" organization. It is part of NIEM, with participants from the Federal, state, local, tribal and international organizations.
- c. The MilOps domain is not a rebranding of existing standards. It is not a model repository. It is not a universal solution to all military-related information data needs. It is not a security cross-domain solution.
- d. The domain's data components are available for reuse by information exchange

designers. The domain steward does not control or approve that reuse. In general, the domain's data components will be used to support information exchange requirements from the following Joint Capability Areas core competencies.²

- *Force Support:* The ability to establish, develop, maintain and manage a mission ready Total Force.
- *Battle Space Awareness:* The ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making by leveraging all sources of information to include Intelligence, Surveillance, Reconnaissance, Meteorological, and Oceanographic.
- *Force Application:* The ability to integrate the use of maneuver and engagement in all environments to create the effects necessary to achieve mission objectives.
- *Logistics:* The ability to project and sustain a ready joint force through the deliberate sharing of national and multi-national resources to effectively support operations, extend operational reach, and provide the joint force commander the freedom of action necessary to meet mission objectives.
- *Command and Control:* The ability to exercise authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission.
- *Communications and Computers:* The ability to provide a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.
- *Protection:* The ability to prevent/mitigate adverse effects of attacks on personnel (combatant/non-combatant) and physical assets of the United States, allies and friends.
- *Building Partnerships:* The ability to interact with partner, competitor or adversary leaders, security institutions, or relevant populations by developing and presenting information and conducting activities to affect their perceptions, will, behavior, and capabilities in order to build effective, legitimate, interoperable, and self-sustaining strategic partners.
- *Corporate Management and Support:* The ability to provide strategic senior level, enterprise-wide leadership, direction, coordination, and oversight through a chief management officer function.

Changes to the domain's data components are requested by the domain stakeholders and approved through the domain management process. Content will not be added when the business

² Joint Capability Areas. January 9, 2015. https://intellipedia.intelink.gov/wiki/Joint_Capability_Areas.

need and reuse can be satisfied by data components in NIEM Core or in other NIEM domains. New content will be harmonized with NIEM Core and with the other NIEM domains. New content will be added upon approval by the NIEM MilOps Domain stakeholders.

The data components managed by the NIEM MilOps Domain are not intended to provide comprehensive coverage of the functional categories. Instead, the content contained will be primarily based upon the need for reuse among information exchange developers and users.

The MilOps Domain does not approve or contain IEPDs. IEPD designers who reuse MilOps domain data components may participate in the MilOps Domain, but are not required to do so. IEPDs are approved by cooperating program developers, communities of interest or by a standards organization. (e.g. Cursor on Target COI; U.S. Message Text Format USMTF COI etc)

5. Governance

The NIEM governance, in which the DOD CIO participates on behalf of DOD, uses a federated model, headed by an Executive Steering Council (ESC) that sets the overall vision for the NIEM community and serves as the decision-making body regarding NIEM membership, funding requirements, and program technical direction. Day-to-day operations are managed by the NIEM Program Management Office (NIEM PMO), which facilitates collaboration between NIEM community and stakeholders in developing NIEM-based information exchange solutions.

The NIEM Business Architecture Committee (NBAC) guides the development, harmonization, evolution, and implementation of NIEM Core data components, as well as governs the processes for participating in NIEM domains. The NIEM Technical Architecture Committee (NTAC) is responsible for defining the technical architecture that governs NIEM. The DOD CIO appoints the Domain Stewards for DOD-sponsored domains. The stewards, or their designated representative, participate in the NBAC.

The NIEM governance structure is executed through a consensus-based approach and is depicted in Figure 1. Detailed descriptions of the specific functions of each entity in the NIEM governance structure are posted at the NIEM web site <https://www.niem.gov/meet-us/Pages/meet.aspx>

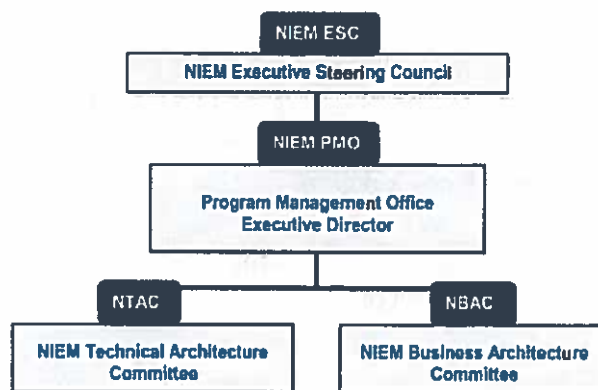


Figure 1: NIEM Governance Structure

5.1 MilOps Domain Governance Structure

The MilOps Domain conforms to the NIEM governance construct, with a Domain Steward, Configuration Control Board, and special working groups to manage Domain activities, facilitation of engagement with Domain participants, oversight of the development of information exchange tools, and prioritization of work. The MilOps Domain governance structure is depicted in Figure 2.

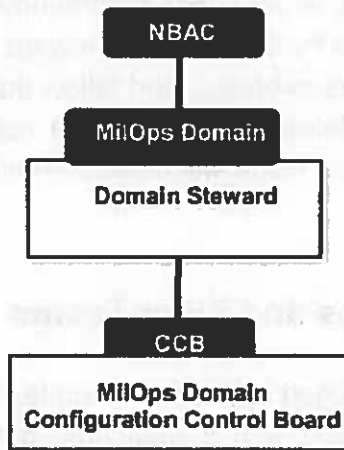


Figure 2: MilOps Domain Governance Structure

5.1.1 MilOps Domain Steward

The Domain Steward is the person and organization approved by the DOD CIO and designated in the Domain Stewardship Agreement with the NIEM PMO to provide oversight of the MilOps Domain consistent with the NIEM PMO and DOD guidance.

5.1.2 MilOps Domain Configuration Control Board (CCB)

The CCB performs working-level coordination of issues to achieve NIEM program and Departmental objectives, and is chaired by a Domain Steward designated in the Domain Stewardship Agreement with the NIEM PMO to provide oversight of the MilOps Domain consistent with the NIEM PMO and DOD guidance. "On a case-by-case basis, the CCB will assist with validation work and will provide business and technical expertise regarding use of the MilOps Domain content and creation of Information Exchange Package Documentations (IEPDs). It also provides the repository and training functions for domain related artifacts, tools and documentation. The CCB is empowered to form sub-working groups to meet long-term coordination needs.

The CCB is chaired by the Domain Steward's designated representative. The CCB is composed of DOD and non-DOD stakeholder organizations with a confirmed and vested interest in establishing, maintaining, and applying MilOps Domain data components to

improve information sharing. Vested interest is defined as development of an IEPD that defines an actual information exchange that will utilize both the NIEM technical framework and MilOps Domain content. The CCB stakeholders will be representatives from those organizations that have adopted and implemented MilOps NIEM data components to share information or plan to in the near future. Representatives should be formally designated by their organization to represent concerns and communicate between the MilOps Domain steward and their organization. The CCB will meet via conference call on a periodic schedule. Meetings will be open to all NIEM community participants. Any CCB Board's secretariat needs will be provided by the Domain Steward.

All CCB decisions will be consensus-based, and follow the business processes prescribed in the MilOps Operations and Maintenance Plan. If a consensus is not achieved for any reason during a CCB meeting, the issue will be presented to the MilOps Domain Steward for resolution.

5.1.3 Sub-Working Groups and Tiger Teams

Sub-Working Groups are established to perform complex, long-term tasks (greater than 4 months) requiring a focused effort with a dedicated group. These groups obtain their authority from their tasking authority (Domain Steward, CCB Chair); self-direct coordination actions to meet tasking requirements; and formally report results to the tasking authority. Tiger Teams are used as needed for short-term tasks (4 months or less), to meet emergent short-term tasking and obtain their authority from their tasking authority (CCB designated lead). Tiger Teams self-direct coordination actions to meet tasking requirements; and they formally report results to the tasking authority.

5.2 Governance Meetings and Reporting

The MilOps Domain mission execution requires regular meetings and reviews. Each entity (Domain Steward, CCB, Sub-Working Groups, and Tiger Teams) will meet as required to achieve timely completion of their tasks and also to align with and support NIEM governance meetings. These meetings will be routinely conducted by conference call/Defense Connect Service. - A summary/minutes of the meeting will be provided to the Domain Steward for review upon request.

The MilOps Domain structure is designed to optimize collaboration and flexibility. The MilOps Domain Steward Representative is the primary conduit for communications to the Domain Steward and NIEM PMO.

The MilOps Domain Steward's designated representative(s) will write the minutes and document MilOps CCB activities and report them to the Domain Steward as appropriate.

5.3 Relationships and Dependencies

The CCB Chair will maintain close communications with the Domain Steward, other NIEM governance bodies and the NIEM PMO. The CCB also serves as a forum for discovery and resolution of semantic matters related to the MilOps domain model, and approves changes to existing or additions to the MilOps domain content. While not all-inclusive, the following interactions exemplify collaboration between organizations:

- The Domain Steward monitors activities of the CCB, and coordinates with all participants and stakeholders the accomplishment of NIEM PMO I DOD objectives in the MilOps Domain.
- The CCB will collaborate with the NIEM PMO, NBAC, NTAC and domain stakeholders for resolution of issues impacting the use of the MilOps Domain.
- The CCB collaborates with representatives to develop, refine, approve and implement content.
- The NBAC provides feedback via the designated MilOps Domain NBAC representative of any updates or changes to the submitted content for the purpose of mutual resolution and harmonization.

6. MilOps Domain Operations and Communication

MilOps Domain day-to-day and configuration management processes are described in the MilOps Domain Operations and Maintenance Plan (O&M Plan). The MilOps Domain structure and processes will be adapted to meet priorities from the DOD CIO, MilOps Domain Steward, and the NIEM PMO.

7. Domain Metrics

The CCB will track relevant metrics to evaluate the performance of the MilOps Domain and its processes. Additional details on Domain Metrics will be documented in the NIEM MilOps O&M Plan. Metrics may include the following among others:

- The number of stakeholders or organizations who are participating in the MilOps Domain CCB.
- The number of content change requests adjudicated within the MilOps Domain.
- The number of IEPDs created that leverage MilOps Domain content.