Homeland Security

NIEM Biometrics Domain
Enterprise Level
Data Standards Execution Plan

February 2021

Approval

The NIEM Biometrics Domain: Enterprise-Level Data Standards Execution Plan was signed by the NIEM Biometrics Domain Executive Committee in February 2021.

A copy of this approved document is on file with DHS Office of Biometric Identity Management (OBIM).

Record of Changes

No.	Date	Reference: Page, Table, Figure, Paragraph	A = Add. M = Mod. D = Del.	Change Description
1	8-10-2018	All	A	Initial version approval
2	1-23-2019	P ii, 3	M	Updated Executive Committee member list.
3	04-30-2020		M	Updates related to NIEM Management Office, NIST revisions, Biometric Standards.
4	10-8-2020	All	M	Update to working groups in alignment with revised charter.

Table of Contents

List of Figures

1 Introduction

1.1 Overview

The Office of Biometric Identity Management (OBIM) serves as the lead entity for biometric identity management services within the U.S. Department of Homeland Security (DHS). OBIM provides enterprise-level biometric identity information to DHS and its mission partners. It operates and maintains the Automated Biometric Identification System (IDENT) and provides identity services expertise as a service provider for customers across DHS, at other federal agencies, in state and local law enforcement, and overseas. OBIM is also focused on improving biometric sharing in support of national security and public safety. By matching, storing, sharing, and analyzing biometric data, OBIM provides partners on the front lines of homeland security with rapid, accurate, and secure identification.

As interest in the National Information Exchange Model (NIEM) continues to grow across the federal, state, local, international and private sectors, an execution plan is needed to help organizations across federal government apply NIEM to their information sharing and exchange activities and develop a NIEM adoption strategy based on their specific capabilities, business needs and technical needs. To address this need, the Futures Identity Team and ITD (Identity Technology Division) at OBIM work with the Assistant Director (AD) to create and maintain an Enterprise-Level Data Standards Execution plan (EDSEP).

EDSEP helps agencies and organizations adopting data standards gain faster access to information, reduce cost of automated information exchanges and leverage existing systems. It also enables participation in regional, state and national information sharing systems based on interoperability standards and contribution towards shaping national standards for information sharing.

1.2 Background

The Office of Management and Budget (OMB) Memorandum M-13-13, Open Data Policy - Managing Information as an Asset, dated May 2013, requires executive departments and agencies to manage information as an asset through its lifecycle to increase operational efficiencies, reduce costs, improve services, support mission needs, and safeguard personal information. The memorandum contains specific requirements for data standardization, stewardship, interoperability, accessibility, and inventory.

Within the Department, Directive 262-05, Information Sharing and Safeguarding, September 2014, requires Department of Homeland Security components to share information as one Department, and requires components, to the greatest extent possible, to standardize the technology used in systems to categorize, access, exchange, and manage information in automated systems to support the Department's missions. Established in 2011, the Information Sharing and Safeguarding Governance Board (ISSGB) serves as the steering committee and decision-making body for DHS collaboration on information sharing and safeguarding issues. The ISSGB will coordinate with, but not preempt the authority of, the Homeland Security Intelligence Council or authorities of any DHS component or office under statute or Executive Order. The ISSGB, to the extent required, will issue management directives that clarify and streamline implementation and execution of the information sharing and safeguarding mission. The ISSGB charter operationalizes DHS Directive 262-05 by authorizing the ISSGB to oversee the Department's data sharing efforts. The Undersecretary for Intelligence and Analysis (I&A) heads the ISSGB while representatives of all major DHS components serve as voting members.

In September 2015, DHS issued a one-page overview of its proposed data strategy, outlining objectives that address many of the elements of the OMB Memorandum. In August 2016, the Undersecretary for I &A formally signed DHS' Enterprise Data Strategy. The ISSGB is responsible for development, coordination, governance, and implementation of the Enterprise Data Strategy. The purpose of the Enterprise Data Strategy is to "present a clearly defined, actionable roadmap and strategic approach to drive departmental resources toward innovative and effective data management, sharing, safeguarding, and integration to fully leverage the Department's data assets towards mission operations, strategic planning, resource management, and analytics." To accomplish this vision, the Enterprise Data Strategy outlines the following five major goals for managing and using data.

1. Improve data quality through collective governance;
2. Organize data for effective mission use;
3. Ensure data is interoperable and that data rules are understood;
4. Ensure secure data platforms that meet mission demands;
5. Attract and develop a skilled data workforce.

As one of the largest biometric identity repositories in the world, IDENT holds biometric identity information for more than 267 million individuals. As OBIM continues to expand its biometric identity management services to include additional biometric modalities and stakeholders, it will be important to maintain alignment with organizations including National Information Exchange Model (NIEM), American National Standards Institute (ANSI) National Institute of Standards and Technology (NIST), International Committee for Information Technology Standards (INCITS), International Organization for Standardization (ISO), and International Civil Aviation Organization (ICAO).

David Pekoske, Senior Official performing the duties of the Deputy Secretary, of the Department of Homeland Security (DHS) signed the "NIEM first" memorandum on May 3rd, 2019 outlining the Department's adoption of the National Information Exchange Model (NIEM). The Information Sharing and Safeguarding Governance Board (ISSGB), has recommended DHS, unanimously, that the Department adopt the National Information Exchange Model (NIEM) for all new data exchanges created by DHS operational components and Headquarters.

OBIM supports the development of standards for the Registry of US Government Recommended Biometric Standards and implements standards consistent with the registry. Accordingly, OBIM conforms to the ANSI/NIST-ITL 1-2011 standard widely used internationally. OBIM is also the steward of the National Information Exchange Model (NIEM) Biometrics Domain to further develop standards for eXtensible Markup Language (XML)-based biometric data exchange consistent with the recommendations of the Registry of USG Recommended Biometric Standards and to encourage its stakeholders to follow suit.

The biometrics industry, local and state governments, the federal government, and international governments rely heavily on published standards to deploy biometrics identity systems. These standards are used to baseline the quality of biometric modalities, design software applications to communicate, exchange data, and use the information being exchanged. As a leader in biometrics for the federal government, OBIM closely follows these standards to implement technology for collecting and storing biometric data, provide data for analysis, update its watchlist, and ensure data integrity.

OBIM's goal of standards adoption and adherence is to establish a framework towards the above five major goals of enterprise data strategy to reach interagency consensus on biometric standards adoption for the federal government.

This document addresses goals 1 through 3 using the NIEM model as a solution. Federal agency adoption of these recommended standards, and associated conformity assessment programs, will enable interoperability in next generation federal biometric systems, and enhance the effectiveness of biometric products and processes. Enabling the development, adoption and use of biometric standards will allow OBIM to integrate its data assets using multiple communication techniques and protocols, such as data converters, data extensions, data adapters, and data exchange necessary for interoperability.

1.3 Scope

The EDSEP strategy covers the need, development, adoption, implementation, and maintenance of data standards required for the efficient interoperability between disparate systems across the federal government. The enterprise strategy of data standards implementation aligns with the goal of successful interoperability to share a common, unambiguous understanding of the meaning of the information being exchanged. This plan provides NIEM execution guidance for Enterprise-Level Data Standards including its relation to other data exchange standards, e.g. ISO and ANSI/NIST-ITL, INCITS and ICAO. This document includes standards, specifications, and best practice recommendations resulting from the INCITS M1, ISO/International Electrotechnical Commission (IEC) Joint Technical Committee (JTC)1/Subcommittee (SC) 37, ANSI/NIST-ITL, and NIEM. It explains how to use the corresponding tools, templates, and outlines a path for successful data standards execution.

1.4 Audience

This document's intended audience comprises federal, state, local, tribal, private and international organizations establishing or improving data standards with a focus on the biometrics industry. These organizations can inform, participate, and collaborate to help shape, develop, and refine data standards programs.

2 Policy and Domain Governence

Policies and rules establish, declare and make known the basic requirements for the general data structure, format, identity, ownership, usage and access for all information systems within the enterprise. They aide in the conformance to standards and the mitigation of risk and are further delivered and enacted through the establishment of operational rules and applications. Rules are required for the effective management and valuation of information, ensuring consistency of information, and that it conforms to given standards and quality metrics. They further allow for the active monitoring and compliance against the corporate or regulatory initiatives and specified business objectives.

OBIM is the NIEM Biometrics Domain Steward and receives domain guidance from members of the NIEM Biometrics Domain Executive Committee (NBDEC). The NIEM Biometrics Domain Executive Committee members include the Biometrics Domain Chair (John Boyd of OBIM), two Co-Chairs (Jennifer Stathakis of DOJ/Federal Bureau of Investigation and William Graves of DoD) and the NIST Ombudsman (Diane Stephens). NIEM NBAC publishes policies and guidance to the NIEM community and technical specifications documents on NIEM.gov to improve the understanding of NIEM data standards and supports adoption within the Community

of Interest (COI). The NIEM User Guide provides detailed guidance about how to develop information exchanges utilizing this model. It provides a detailed description of the rationale for the creation of NIEM, an architectural overview, and technical concepts derived from NIEM Management Office (NMO) documentation.

For organizations interested in active contribution, the NIEM Biometrics Domain has a standing working group, the NIEM Biometrics Domain Working Group (NBDWG) which includes the NBDEC with various stakeholders, i.e. Biometric SME's, members of the Domain, etc., as appropriate. The working group is administered by the Domain Steward in conjunction with the NBDEC, which communicates issues and resolutions among the working group, the NIEM NMO, and the COI. The NBDWG activities are specific to potential NIEM Biometrics Domain model updates. The NBDWG addresses technical and business/operational issues and meets on an as needed basis.

The NBDEC works closely with the Biometrics COI via the NBDWG in accordance with the Domain Governance process to ensure technical recommendations are in alignment from a business perspective and that business decisions are appropriately reviewed for technical feasibility. The NBDWG works with the Harmonization Working Group (initiated by the NBAC) during each NIEM release as a part of the Domain reconciliation process which is detailed in further sections. The NBDWG will participate as a canvassee in the ANSI/NIST-ITL revision process to assist with the adaptation of major stakeholder requirements to a NIEM based representation, led by the DOJ Co-Chair.

The Executive Steering Council (ESC) is designed to provide executive leadership, vision, direction, and fundamental support for the NIEM program. The ESC sets policy and strategy, secures funding, appoints key personnel to the NMO, approves the NIEM ConOps, and makes other decisions as required. The ESC advocates for NIEM at senior levels of government and among key constituencies. The Policy Advisory Panel is designed to identify policy issues of concern to the NIEM community, analyze them, resolve them when appropriate, provide policy recommendations, and address emerging policy issues associated with NIEM planning, operations, and implementation.

The Chair of the NIEM Policy Advisory Panel will be appointed by and serve at the pleasure of the NIEM program Executive Director. The panel will be appointed by and serve at the pleasure of the Policy Panel Chair in consultation with the NIEM program Executive Director. Consideration will be given to expanding the panel to ensure that new domains that are signatories to a Memorandum of Understanding (MOU) are properly represented. Panel members will represent organizations that are signatories to NIEM MOUs. Provision will be made for appropriate representation of local, state, tribal, and federal interests. Panel members will serve as liaison to the NIEM Business Architecture Committee (NBAC), NIEM Technical Architecture Committee (NTAC), National Priority Exchange Panel (NPEP), and NIEM Communications and Outreach Committee (NC&OC).

The panel develops recommendations for NIEM program target outcomes and the related spending plan for approval by the ESC through the NEIM NMO. The panel also makes recommendations for approval through the NMO by the ESC regarding the requirements for funding and potential sources. The NIEM domain governance structure is laid out as depicted in ***Figure 1*** below.

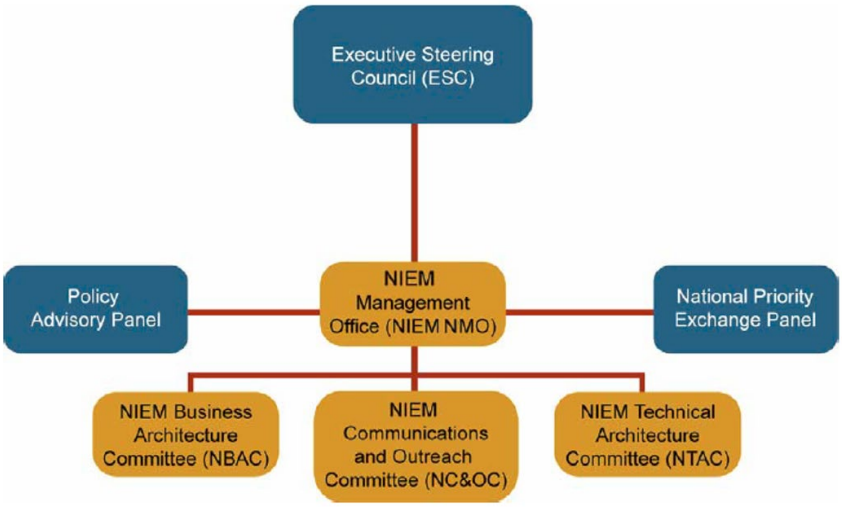

Figure 1: NIEM Biometrics Domain Governance Structure

As the central authority in the federated governance model, NBAC interacts with domain governance groups and provides coordination, policy and technical direction allowing each domain governance group to retain relative autonomy to govern its domain while interacting with its own COI. Per NBAC best practices, context and content of information along with critical policy requirements, (e.g. privacy, security, priority, frequency, urgency, complexity, and confidentiality), should be captured and documented during NIEM development.

Information concerning the Biometrics Domain, issues of domain management, and standing working groups will be communicated to the NMO and NBAC regularly to notify stakeholders of developments and activities. This communication is a primary responsibility of the domain steward and the NBDEC.

3 Data Exchange Standards

The Information Technology Laboratory (ITL) at NIST and ISO are organizations that define data exchange standards to enable interoperability between disparate information technology systems. ITL defined its data exchange model using NIEM naming conventions for the data format exchange of fingerprint, facial and other biometric information. ISO is an independent, non-governmental standards organization with 168-member countries. It is the world's largest developer of voluntary international standards and facilitates world trade by providing common standards between nations. NIEM data element naming, definition, and metadata capture is based on ISO concepts.

3.1 NIST/ITL Standard

The first version of the ANSI/National Bureau of Standards (NBS) - The Institute for Computer Sciences and Technology (ICST) standard 1-1986 was published by NIST (formerly NBS) in 1986. It was a minutiae-based standard. Revisions to the standard were made in 1993, 1997, 2000, and 2007. Updates to the standard are designed to be backward compatible with new versions including additional biometric modalities and associated data. In 2008, XML encoding of the standard was introduced, based upon the 2007 version. The 2007 and 2008 versions of the standard were designed to be the same except for the encoding. The XML encoding was developed using the naming conventions of NIEM. Thus, this encoding is referred to as “NIEM-

conformant XML." Updates were also made in 2011, 2013 and 2015. The NIST ITL 2015 Update is NIEM 4.0.1 conformant.

3.2 ISO Standard

The naming and design rules for NIEM are documented in the Naming and Design Rules (NDR) which specifies the data model, XML components, and XML data for use with NIEM and provides a basis for NIEM conformance. NIEM is based on several concepts from ISO 11179 which provides guidelines for naming and definition of data elements, as well as information about the metadata captured about data elements. Part 5 of the ISO 11179 standard establishes a methodology for naming items in data dictionaries. The ISO 11179-based NIEM NDR naming convention uses object, class, and property representation terms and qualifiers to constitute a multiple-part name called Object Class Term.

Object Class Term represents the object to which the property is applicable. An object class refers to a group of objects which share the same attributes, operations, methods, relationships, and semantics. In NIEM, we interpret that object to be the real-world object. Property Term identifies the property that the data element represents (e.g., last name, expiration date, height, total). The object class and property terms can have qualifiers; i.e., a word or words that help define and differentiate the element name. Representation Term describes the form of the data represented. This term is taken from a list of electronic business XML (ebXML) representation terms, including amount, code, date, time, graphic, identifier, indicator, measure, name, percent, picture, quantity, rate, time.

ebXML is a family of XML based standards sponsored by the Organization for the Advancement of Structured Information Standard (OASIS) and United Nations Center for Trade Facilitation and Electronic Business (UN/CEFACT) whose mission is to provide an open, XML-based infrastructure that enables the global use of electronic business information in an interoperable, secure, and consistent manner by all trading partners.

3.3 International Committee for Information Technology Standards

The INCITS is the central U.S. forum dedicated to creating technology standards for the next generation of innovation in the field of Information and Communications Technologies (ICT). INCITS is accredited by and operates under rules approved by the ANSI. INCITS is the primary US focus of standardization encompassing storage, processing, transfer, display, management, organization, and retrieval of information in the field of ICT. INCITS also serves as ANSI's Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1 (JTC 1), which is responsible for international standardization in the field of Information Technology.
In November 2001, INCITS established M1 – Biometrics with membership open to any organization (e.g., academic institutions, federal agencies, companies) directly and materially affected by M1 activities. As the US TAG to SC 37 Biometrics, INCITS M1 is responsible for establishing US positions and contributions to SC 37, as well as representing the US at SC 37 meetings. M1 – Biometrics presently has four standing Task Groups:

- M1.2 Biometric Technical Interfaces and Profiles — covers the standardization of all necessary interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems. M1.2 is responsible for the development of biometric application profiles. M1.2 will also consider the need for a reference model for the architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their applications

- M1.3 Biometric Data Interchange Formats — focuses on the standardization of the content, meaning, and representation of biometric data interchange formats
- M1.5 Biometric Performance Testing and Reporting — handles the standardization of biometric performance metric definitions and calculations, approaches to test performance and requirements for reporting the results of these tests
- M1.6 Societal Aspects of Biometric Implementations — addresses study and standardization of technical solutions to societal aspects of biometric implementations. Excluded from the TG's scope is the specification of policies, the limitation of usage, or imposition of non-technical requirements on the implementations of biometric technologies, applications, or systems.

3.4 International Civil Aviation Organization (ICAO)

The ICAO is a UN specialized agency, established in 1944 to manage the administration and governance of the Convention on International Civil Aviation to serve as the global forum for international civil aviation. ICAO develops policies and standards, undertakes compliance audits, performs studies and analyses, and aids and builds aviation capacity through many other activities and the cooperation of its stakeholders.

ICAO Document 9303, Machine Readable Travel Documents, addresses the use of biometrics for face (primary biometric), fingerprint, and iris, contactless integrated circuit chips for data storage, a logical data structure for storage, and data security based on public key infrastructure technology. ICAO 9303 requires conformance with ISO/IEC 19794-5 full frontal or token for face image capture. ANSI/NIST-ITL Type-10 records support ISO/IEC 19794-5 images in Subject Acquisition Profiles (SAP) levels 13 and 14.

3.5 NIEM

NIEM allows all kinds of organizations to save time, money, and resources, connect with each other, and focus on what matters most—solving problems, reducing risks, and advancing even the most complex missions. NIEM benefits communication interoperability of information in two primary ways:

Increase efficiency and agility. Organizations can reuse NIEM's common vocabulary, the engineering behind it, and standardized exchange development process to meet their specific requirements. This reduces the number of development efforts, eases long-term maintenance, conserves resources, and promotes consistency—ultimately leading to enhanced mission capabilities.

Facilitate a common understanding. NIEM provides an understanding of data grounded in a consensus-based vocabulary and enables organizations to move information across organizational boundaries to interoperate and act as one while maintaining authority of their own existing systems.

OBIM is the steward for the NIEM Biometric Domain. NIEM provides a common vocabulary for consistent, repeatable exchange of information between agencies and domains. NIEM uses XML, which provides a common framework for information exchange, allowing the structure and meaning of data to be defined through simple, but carefully defined, syntax rules. NIEM has recently adopted JSON (JavaScript Object Notation) as a second standard format for representing data based on the NIEM data model. A NIEM domain is a formally established Community of Interest (COI) with executive stewards to represent the stakeholders, governance, and data model

content oriented around their respective business needs . Each NIEM domain has its own rules, processes, schedule, and priorities for development of the XML schema for its domain.

Becoming the data steward of the NIEM Biometric Domain enables OBIM to take a leadership role in defining the governance, rules, terminology, and content for this Domain. The NIEM Biometric Domain will provide the data standards, architecture, and data exchange packages necessary for interoperable exchange of data with OBIM and other systems in a common, service-oriented architecture (SOA). NIEM will enable OBIM to integrate its data assets using multiple communication techniques and protocols by providing data converters, data extensions, data adapters, data exchanges and data exchange packages necessary for interoperability.

Support for the XML implementation of ANSI/NIST-ITL and other biometric standards including ISO and INCITS is one of the most important aspects of the NBD, from an interoperability and standards perspective. The ANSI/NIST-ITL XML Workgroup (ANXMLWG) was formed in 2011 with the following objectives:

- Ensuring equivalence between the XML and traditional encoding,
- Conformance to NIEM, including NDR,
- Recommendations for the initial content for a NIEM Biometrics Domain schema, and
- Creation of a narrative XML encoding document.

The ANSI/NIST-ITL 2011 Canvassees adopted the NIEM-conformant XML encoding guidelines. Currently, the NBDWG addresses NBD model updates that align with ANSI/NIST-ITL updates. ISO published ISO/TS 19115-3:2016 XML schema implementation for fundamental concepts. INCITS published a technical specification, INCITS/ISO/TS 19115-3:2016[2017], in 2017 enabling XML schema implementation for fundamental concepts. ICAO published an XML Implementation guide for Passenger and Airport Data Interchange (message) standards in 2013. These messages are intended to facilitate the exchange of data relevant to government requirements on Passenger Name Record (PNR) data and airline reservation systems.

3.6 Biometric Standard Types

OBIM's IXM (IDENT Exchange Messaging) is the exchange that provides common interfaces to OBIM stakeholders. IXM leverages existing industry data models, including NIEM 2.1, and ANSI/NIST-ITL 1-2011. IXM also promotes interoperability between OBIM IDENT and the FBI Next Generation Identification (NGI) system (Integrated Automated Fingerprint Identification System (IAFIS) previously known legacy system). The earliest versions of IXM (version 1.0 through version 5.5) used a data model, vocabulary, and an XML schema based on the Global Justice XML Data Model (GJXDM). The GJXDM reference model was deprecated as a DHS standard in 2007 and was replaced by the NIEM.

IDENT has provided fingerprint, palmprint, facial, iris, and scars, marks and tattoos (SMT) identity services. OBIM is in the process of expanding IDENT system capabilities to meet new requirements for biometric services, to include DNA (Deoxyribonucleic acid) as an additional modality. The benefit of using DNA as a biometric identifier is the level of accuracy offered: the chance of two individuals sharing the same DNA profile is less than one in a 100 billion with 26 different bands studied. OBIM is in the process of developing and adopting additional biometric modality capabilities including voice, dental, non-photographic images, contact-less fingerprints and multi-modal fusion.

DHS OBIM is upgrading its identity management system, IDENT, with Homeland Advanced Recognition Technology System (HART) which is an enhanced, scalable, modular, multimodal identity management system. HART system design will provide for the expansion of interoperable services without requiring modifications to its foundational system architecture. HART Increments 1 and 2 will support IXM 6.1 and IXM 6.2 respectively, which are backward-compatible with IXM 6.0.9. The current version of IXM is 6.0.9.0.9.

OBIM must meet the requirements of Executive Order (EO) 12333, entitled "United States Intelligence Activities", National Security Presidential Directive 59 (NSPD-59)/Homeland Security Presidential Directive 24 (HSPD-24) entitled, "Biometrics for Identification and Screening to Enhance National Security." These directives require OBIM and other Federal agencies to "use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law."

OBIM also participates in and supports the NIST process for standards development in order to contribute to and influence the content, publication, and adoption of standards that are of interest to OBIM and its stakeholders. SDOs such as the INCITS M1 – Biometrics Technical Committee, and the ISO Joint Technical Committee 1 (JTC 1)/Subcommittee (SC) 37 Biometrics, revise and develop standards to support additional biometric modalities and advances in biometric technology, including the related areas of biometric sample quality, standards conformance, performance testing; and to provide technical guidance on societal issues associated with the use of biometrics.

Additionally, OBIM participates in the ongoing review and revision of the worldwide American National Standards Institute/NIST Information Technology Laboratory (ANSI/NIST-ITL) standard. Below is the tabular view of the types of biometric standards required for OBIM stakeholder data sharing.

Standard Type	Function	Examples
Data Formats	Specifies the content, meaning, and representation of formats for the interchange of biometric data. Specifies notation and transfer formats that provide platform independence. Separated transfer syntax from content definition.	ANSI/NIST-ITL 1-2011 – Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information ISO/IEC 19794-6:2011 Biometric Data Interchange Formats – Part 6: Iris Image Data
Technical Interfaces	Specifies interfaces and interactions between biometric components and subsystems. Adds plug-and-play capability to integrate system components into functioning systems and swap components as needed without losing functionality.	ISO/IEC 19784- 1:2006 [2007] BioAPI – Biometric Application Programming Interface – Part 1: BioAPI Specification INCITS 398-2008 Common Biometric Exchange Formats Framework (CBEFF)
Transmission Specifications	Facilitates interoperability. Specifies application-specific	Federal Bureau of Investigation (FBI) Electronic Biometric Transmission Specification (EBTS)

	criteria onto a base standard to establish definitive values for performance-related parameters in the base standard (e.g., resolution, maximum compression) or enumerating values for optional or conditional requirements (e.g., full-frontal face vs. token face).	(FBI Criminal Justice Information Services CJIS EBTS) v9.3 DOD Electronic Biometric Transmission Specification (DOD EBTS) v3.0 Interpol Implementation of ANSI/NIST-ITL 1-2007 (INT-I) v5.0 IDENT Exchange Messages (IXM) Specification v6.0.9.0.9
Testing and Reporting	Addresses evaluation of the biometric sample capture process and recognition system performance. Specifies biometric performance metric definitions and calculations, approaches to test performance, and requirements for reporting the results of these tests.	ISO/IEC 19795:2005 [2007] - Biometric Performance Testing and Reporting: Part 1: Principles and Framework Part 2: Testing Methodologies for Technology and Scenario evaluations Part 3: Modality-Specific Testing
Cross-Jurisdictional and Societal	Addresses study and standardization of technical solutions to societal aspects of biometric implementations.	ISO/IEC 24714, Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies ISO/IEC 24779, Pictograms, Icons, and Symbols for Use with Biometric Systems

Below is the tabular view of the biometric standards for each modality required for enabling OBIM stakeholder data sharing.

Biometric Type	Standard	Description
Fingerprints	ANSI/ NIST ITL 1-2011 Type-4 and Type-14	Plain and Rolled fingerprint images and records
Fingerprints	INCITS M1	Plain and Rolled fingerprints
Fingerprints	ISO/IEC JTC 1 / SC 37	Plain and Rolled fingerprints
Fingerprint Minutiae	ISO/IEC 19794-2:2005 [2008]	Storage in and Transmission to Personal Identity Credentials for Match-off-Card
Minutiae	ANSI/ NIST ITL 1-2011 Type-9	ISO/Minutiae data record
Latent Fingerprints	ANSI/ NIST ITL 1-2011 Type-13	Latent finger and palm print Images
Palm	ANSI/ NIST ITL 1-2011 Type-15	Palm-print images (excluding latent palm print images)
Iris	ANSI/NIST-ITL 2-2008 and 1-2011, Type 17	Iris recognition, capture and storage
Face	ANSI/NIST-ITL 2-2008 and 1-2011, Type 10	Partially Implemented

Face	International Civil Aviation Organization (ICAO) 9303 (ISO/IEC 19794-5)	Images captured by USCIS and DOS comply with travel document standards
Scars, Marks and Tattoos (SMT)	ANSI/ NIST ITL 1-2011 Type-10	Images of scars, needle marks and tattoos
Face	International Civil Aviation Organization (ICAO) 9303 (ISO/IEC 19794-5)	Images captured by USCIS and DOS comply with travel document standards
Deoxyribonucleic acid (DNA)	ANSI/ NIST ITL 1-2011 Type-18	This is included in the data model, using ANSI NIST ITL Type 18 record as the standard. But the implementation of the services was not updated, i.e., though one could create a valid request with DNA inside the biometric details, but the current implementation would not know what to do with it.

4 EDSEP Overview

The EDSEP provides a structured framework for organizations to use international and national standards, as well as NIEM, for their information sharing and exchange activities. The process is intended to help an organization evaluate the potential costs and benefits of NIEM and develop a targeted NIEM adoption strategy based on its information sharing capabilities and needs. The EDSEP will provide organizations with the opportunity to perform self-evaluation of information sharing and exchange activities to develop a business case for adopting a NIEM program. The flexibility of this process enables it to be applied to a wide range of organizations with varying capabilities, needs, and technical environments.

Organizations interested in adopting NIEM may develop an EDSEP to obtain an understanding of how NIEM can add value to their information sharing and exchange activities and determine the steps they would need to take to implement NIEM successfully. The EDSEP evaluates NIEM adoption for individual programs. The organization should apply the NIEM process separately to each program they want to assess.

4.1 Roles

The primary EDSEP roles with their descriptions listed below:

Role	Description
Facilitator	An individual or group that carries out the EDSEP on behalf of an organization. Facilitators may be representatives of the NMO or designated individuals within the organization being assessed. The facilitator should have at least a basic understanding of NIEM and be familiar with the NIEM case studies available on NIEM.gov.
Sponsor	A representative of the organization being assessed (typically an executive or program manager) that oversees the EDSEP for an individual program, provides feedback, and validates the results of the process.

Functional / Business Owner	A member of the organization being assessed (e.g., Program Manager) who oversees, has in depth knowledge of, or has continuous collaboration with the business and/or functional operations of the information sharing and exchange activities.
Technical Architect / Technical Expert	A member of the organization being assessed (e.g., Software Architect, Data Architect) who oversees, has in depth knowledge of, or has continuous collaboration with technical operations of the information sharing and exchange activities.

4.2 Methodology

The EDSEP is comprised of a series of repeatable and reusable steps by design. These steps guide the facilitator through a standardized methodology for gathering information about the organization's information sharing and exchange activities, assessing the readiness of the organization to adopt NIEM, analyzing potential costs, and developing a roadmap for adopting NIEM as a data interoperability standard at the enterprise level.

To successfully adopt NIEM and implement information sharing and exchange initiatives within an organization, four core capabilities should be focused on as they define, develop and implement their data standards execution strategy:

1. Business Need(s)
2. Stakeholder Community
3. Planning Process
4. Technical Capabilities

4.2.1 Business Need(s)

The business need(s) of an organization can be defined as its information sharing imperative. An organization's awareness of its current state of information sharing, understanding of the need for change, and a desired end state common agreement are necessary to ensure NIEM helps achieve information sharing and exchange goals and objectives.

4.2.2 Stakeholder Community

Stakeholder community refers to the internal and external stakeholders involved in an information sharing and exchange initiative. Internal stakeholders may include program leadership, technical architects, business owners, project managers and implementers. External stakeholders may include information sharing partners and other organizations with a common mission interest. Establishing clear roles and responsibilities and engaging these stakeholders in an effective and timely manner will facilitate adopting NIEM data standards at the enterprise level.

4.2.3 Planning Process

The planning process for an information sharing and exchange initiative should address timelines, resource requirements, deliverables, and potential risks. An established plan for information sharing and exchange provides direction and enables coordination throughout the development and implementation of the initiative.

4.2.4 Technical Capabilities

Technical capabilities refer to the current state and desired future state of an organization's information sharing and exchange infrastructure. An organization should first analyze its current technical landscape and ability to support information sharing and exchange before

envisioning/planning for their desired future state. Having a clear understanding of the current and future states will enable an organization to determine the steps needed to achieve its desired information sharing and exchange capabilities.

4.3 Tools

The following tools (documents, templates, etc.) should be used to complete an EDSEP. The purpose and intended audience for each document are provided below.

Tool	Description	Audience
User Guide	Provides instructions and guidance for facilitators performing the NIEM Engagement Process (NEP). Gives background information for the facilitator to understand the purpose and objectives of the NEP.	Facilitators
Core Capabilities	Describes the critical elements recommended for successful adoption of NIEM and lays the foundation for the NEP.	Facilitators
Interview Framework	Guides the facilitator in researching the organization's information sharing and exchange activities and conducting stakeholder interviews. Interview and research results are used to complete the NIEM Readiness Assessment and the Cost Model.	Facilitators
Interview Framework (Data Collection Tool)	Provides participants with a complete structure of questions to assist in the evaluation of how and why different aspects of information sharing, and exchange activities are designed for their organization.	Functional / Business Owner Technical Architect / Technical Expert
NIEM Readiness Assessment Tool	Defines a framework for measuring the organization against the Core Capabilities. Once completed, the NIEM Readiness Assessment provides a visual scorecard representation of the NIEM-readiness of a program.	Facilitators
Cost Model	Tool for analyzing the quantitative costs and benefits of NIEM adoption.	Facilitators
Road to NIEM Adoption Template	This document provides a proposed timeline for NIEM adoption. The preparation, adoption and continuous engagement of stakeholders are defined as a foundation plan for adopting NIEM processes.	Sponsors

5 Executing NEP

Organizations adopting NIEM are not required to complete each of the recommended steps below. Each step can be tailored to the needs and priorities of the organization being assessed. Each of the templates and tools mentioned above can be used to assess the enterprise or any process within the enterprise (i.e., specific exchange activity) towards executing standards. If an organization has already adopted NIEM for an exchange activity and yet is looking to expand, one or more of the following steps may not be needed for adopting NIEM.

The steps for executing the NEP are:

1. Perform Research,
2. Conduct Stakeholder Interviews,
3. Complete NIEM Readiness Assessment,
4. Quantify and Qualify the Value of NIEM Planning and
5. Planning, which are outlined below.

The duration times of each step varies depending on the priorities and size of the information sharing and exchange activities being performed.

5.1 Perform Research

The organization/team needs to identify critical data requirements and corresponding data resources. Identification of internal and external data requirements is crucial for sharing information, helping to identify and develop simple scenarios and identify common use cases for sharing information. This research also helps examine existing database schemas, data dictionaries, XML schemas, flat files, paper and electronic forms, workflows, etc., for data requirements. Such data sources can provide insight into what data is currently shared and how it is shared.

The organization/team must conduct comprehensive research regarding the program's mission priorities and current information sharing and exchange activities. Performing thorough research is critical, as it will enable the facilitator to engage in targeted discussions during stakeholder interviews. Together, the information gathered during this initial research and the stakeholder interviews will enable the facilitator to complete the NIEM Readiness Assessment and Cost Model.

5.2 Conduct Stakeholder Interviews

The organization/team should hold interviews with the functional or business owners, technical architect or technical expert, program points of contact (POCs), such as architects or program-level management, all identified by the sponsor. Each interview is a guided discussion exploring the organization's information sharing and exchange activities with respect to the core capability areas. During the interview, the facilitator should draw upon their initial research to discuss both current and potential information exchange(s) with the POC. The interviews should provide the facilitator with the remaining information needed to complete the NIEM Readiness Assessment and NIEM Cost Model.

5.3 Complete NIEM Readiness Assessment

The team then compiles the interview results and initial research to complete the NIEM Readiness Assessment, which measures the organization's readiness to adopt NIEM by comparing the organization's current information sharing and exchange activities with the recommended state for each of the core capability indicators. The results of the assessment are summarized in a scorecard.

The assessment pinpoints specific areas where the organization is well prepared or requires development to adopt the NIEM data standards at enterprise-level.

5.4 Quantify and Qualify the Value of NIEM Planning

The next step is to complete the NIEM Cost Model by inputting cost variables, values from the NIEM Readiness Assessment, and other data gathered through stakeholder interviews and research. The NIEM Cost Model, available on NIEM.gov, compares the potential quantitative costs and benefits of using NIEM vs. custom exchange for information sharing and exchange

over a four-year period, based on the nature of the planned information exchange(s) and the NIEM readiness of the organization.

The team defines performance metrics for the exchange. The facilitator and the organization should collaboratively identify specific items that can be assessed over time to measure the success of the exchange toward meeting business goals and mission objectives. After defining the performance metrics, establish a baseline current state and goal for each metric. Organizations will be able to interact and follow-up with the NMO for future checkpoints and updates on status of the implementation.

5.5 Planning

Finally, the organization/team creates a roadmap for adopting NIEM, analyzes the results of the NIEM Cost Model, NIEM Readiness Assessment, and other research to create a summary of key findings. The key findings include a brief research summary, the results of the NIEM Readiness Assessment, and the NIEM value proposition, including potential qualitative and quantitative costs and benefits. As appropriate, the team will include steps the organization may take to achieve the recommended states for the core capability indicators.

Based on the analysis of key findings, the team will develop a recommendation on whether NIEM offers a good value proposition and should be adopted for the program. This recommendation is a key consideration for the sponsor to decide if they should adopt NIEM.

If NIEM is selected, the organization/team will design a tactical implementation plan that outlines a tailored NIEM adoption strategy, including a timeline and specific actions for the organization to take to apply the NIEM framework to their information sharing and exchange activities.

6 Path to Successful NIEM Data Interoperability Standard Execution

After completing the NEP, the organization should execute and follow the NIEM readiness recommendations provided in the tactical implementation plan. To support successful NIEM adoption, organizations should perform the following activities:

Activity	Description
Monitor Exchange Performance	The organization should periodically assess progress toward meeting goals and objectives for the exchange using the performance metrics identified during the NIEM Engagement Process. By tracking and monitoring performance, both the organization and the NMO can evaluate and report on NIEM adoption success. The roadmap should include a tracking log for recording metric progress.
Hold Check-ins	On a periodic basis, the NMO and the organization should hold check-ins to discuss NIEM adoption successes, challenges, and progress toward meeting performance goals. During check-ins, the NMO can offer advice and help address any challenges.
Engage in the NIEM Community	Organizations are encouraged to get involved in the NIEM community as appropriate based on their needs and interests. Stakeholder engagement is key to the success of NIEM – active

	stakeholder involvement promotes cross-domain coordination and enables NIEM to adapt to changing business needs. Community involvement may range from attending NIEM events to participating in NIEM domain governance activities. The NMO can help the organization to identify opportunities for involvement.
Develop a Long-Term NIEM Strategy	The organization should consider developing a long-term NIEM strategy that explores how current/future business needs might be addressed using NIEM. This may also include plans for engaging with the NIEM community. The strategy should be revised as business needs change over time.

7 Summary

Enterprise-level data standards are a critical factor in improving overall effectiveness, efficiency, consistency, alignment and compliance; which enhances the opportunity for future interoperability. OBIM encourages on-going research in development of data standards and innovative technologies to enhance the public safety and interoperability between its customers by participating in NIEM as the Biometrics Domain steward and sponsoring NIST/ITL. This strategic plan expresses OBIM's commitment to the development and use of enterprise-level and biometric data standards, as well as the proactive collaboration with SDOs, industry and other stakeholders to ensure standards are optimized to support analysis and decision-making. Development and implementation of a comprehensive set of enterprise-level and biometric data standards which meet the technical requirements of OBIM and its stakeholders achieves interoperability for data interchange.

8 References

NIEM: https://reference.niem.gov/niem/
NIEM User Guide: https://reference.niem.gov/niem/guidance/user-guide/vol1/user-guide-vol1.pdf
NIEM Cost Model: https://www.niem.gov/sites/default/files/NIEM_Engagement_Process_CostModelUserGuide_v2.0.pdf
NIST: https://www.nist.gov
ANSI/NIST-ITL Standard History: https://www.nist.gov/itl/iad/image-group/ansinist-itl-standard-history
ISO: https://www.iso.org
ebXML: http://www.ebxml.org/
ICAO: http://www.icao.int
ICAO XML Implementation Guide: https://www.icao.int/Security/FAL/Documents/4-PNRGOV_XML-Implementation-Guide-13-1version-NEW-FOURTH.pdf
INCITS: https://standards.incits.org
DHS Improvements Needed to Promote DHS Progress toward Accomplishing Enterprise-wide Data Goals
OASIS: https://www.oasis-open.org/standards

Appendix A Glossary of Abbreviations, Acronyms, and Initialisms

AD	Assistant Director
ANSI	American National Standards Institute
ANXMLWG	ANSI/NIST-ITL XML Workgroup
CBEFF	Common Biometric Exchange Formats Framework
COI	Community of Interest
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DNA	Deoxyribonucleic acid
EBTS	Electronic Biometric Transmission Specification
ebXML	Electronic Business XML
EDSEP	Enterprise Data Standards Execution Plan
ESC	Executive Steering Committee
EO	Executive Order
FBI	Federal Bureau of Investigation
HART	Homeland Advanced Recognition Technology System
GJXDM	Global Justice XML Data Model
I&A	Intelligence and Analysis
ICAO	International Civil Aviation Organization
ICST	Institute for Computer Sciences and Technology
IDENT	Automated Biometric Identification System
IEC	International Electrotechnical Commission
INCITS	International Committee for Information Technology Standards
ISSGB	Information Sharing and Safeguarding Governance Board
ISO	International Organization for Standardization
ITD	Identity Technology Division
ITL	Information Technology Laboratory
IXM	IDENT Exchange Messaging
JSON	JavaScript Object Notation
JTC	Joint Technical Committee
MOU	Memorandum of Understanding
NBAC	NIEM Business Architecture Committee
NBS	National Bureau of Standards

NBDEC	NIEM Biometrics Domain Executive Committee
NBDWG	NIEM Biometrics Domain Working Group
NC&OC	NIEM Communications and Outreach Committee
NDR	Naming and Design Rules
NEP	NIEM Engagement Process
NGI	Next Generation Identification
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NMO	NIEM Management Office
NPEP	National Priority Exchange Panel
NTAC	NIEM Technical Architecture Committee
OASIS	Organization for the Advancement of Structured Information Standard
OBIM	Office of Biometric Identity Management
OMB	Office of Management and Budget
PNR	Passenger Name Record
POC	Point of Contact
SAP	Subject Acquisition Profiles
SC	Subcommittee
SDO	standards development organizations
TAG	Technical Advisory Group
UN/CEFACT	United Nations Center for Trade Facilitation and Electronic Business
XML	Extensible Markup Language