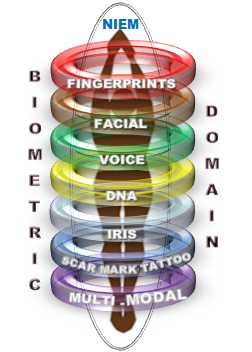


****

**National Information Exchange Model**

**Biometrics Domain Charter**

12 July 2018

Submitted by:

Integral Consulting Services, Inc.

2101 Gaither Road, Suite 410

Rockville, MD 20850

Contract Number: GS00Q14OADS145

Delivery Order Number: HSHQDC-17-F-00189

**Approval**

|  |  |
| --- | --- |
| **DHS OBIM** | **Signatures** |
| Approved by: |  | |
|  | Mr. John Boyd Date  NIEM Biometrics Domain Chair  Identity Technology Division  Office of Biometric Identity Management | |
| Approved by: |  | |
|  | Mr. Thomas Freed Date Information Technology Specialist  Identity Technology Division  Office of Biometric Identity Management | |

**Record of Changes**

| No. | Date | Reference: Page, Table, Figure, Paragraph | A = Add. M = Mod. D = Del. | Change Description |
| --- | --- | --- | --- | --- |
| 1 | 7-12-2018 | All | A | Initial version approval |
| 2 | 1-23-2019 | P 10 | M | Updated the ESC Member names |

**Contents**

[1 Introduction 5](#_Toc505255320)

[1.1.1.1 Overview 5](#_Toc505255321)

[1.1.1.2 Scope of Charter 5](#_Toc505255322)

[1.1.1.3 Intended Audience 5](#_Toc505255323)

[1.1.1.4 Reference Documents 6](#_Toc505255324)

[2 Domain Overview 6](#_Toc505255325)

[2.1.1.1 Domain Mission 6](#_Toc505255326)

[2.1.1.2 Domain Scope 6](#_Toc505255327)

[2.1.1.3 Domain COI 7](#_Toc505255328)

[2.1.1.4 Domain Goals 7](#_Toc505255329)

[3 NIEM Governance Structure 8](#_Toc505255330)

[3.1 Domain Governance Structure 10](#_Toc505255331)

[3.2 Domain Governance and NBAC Relationship 10](#_Toc505255332)

[3.3 Domain Steward 11](#_Toc505255333)

[3.3.1.1 Domain Steward Responsibilities 11](#_Toc505255334)

[3.3.1.2 Domain Steward Mission 13](#_Toc505255335)

[3.4 Domain Members 13](#_Toc505255336)

[3.5 Domain Governance Committee(s) 14](#_Toc505255337)

[3.5.1.1 Committee Membership 14](#_Toc505255338)

[3.5.1.2 Committee Roles and Responsibilities 15](#_Toc505255339)

[3.5.1.3 Domain Dispute and Conflict Resolution Mechanisms 15](#_Toc505255340)

[3.5.1.4 Consensus Agreement and Due Process Representation 16](#_Toc505255341)

[3.5.1.5 Dispute/Conflict Resolution (Appeals) 16](#_Toc505255342)

[4 Domain Charter Modifications 18](#_Toc505255343)

[5 Acronyms and Abbreviations 18](#_Toc505255344)

[6 Additional References 19](#_Toc505255345)

# Introduction

## Overview

The formal establishment of the Biometrics Domain was initiated in July 2012 pursuant to the Domain Stewardship Agreement signed in March 2012 between US-VISIT―now known as the Office of Biometric Identity Management (OBIM) within the National Protection and Programs Directorate (NPPD) of the Department of Homeland Security (DHS) ―and the National Information Exchange Model (NIEM) Program Management Office (PMO). IDENT, the OBIM Automated Biometric Identification System is one of the world’s largest biometric identity repositories, holding biometric identity information about more than 120 million individuals. As OBIM continues to expand its biometric identity management services to include additional biometric modalities and stakeholders, maintaining active participation in standards development organizations, such as the National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST), the International Committee for Information Technology Standards, International Organization for Standardization, and International Civil Aviation Organization, will be important to the OBIM enterprise target long-term service-oriented architecture.

The Biometrics Domain supports information sharing and promotes interoperability between national and international organizations, including federal, state, and local agencies using biometric data and information. It will leverage current and emerging technology, lessons learned, and successes to enhance internal processes and operational effectiveness; improve external sharing and productivity; and support national information sharing programs.

## Scope of Charter

The Biometrics Domain Charter describes the domain’s mission, scope, and governance structure, including frameworks for dispute resolution and mechanisms for member representation (voting). It formalizes the Biometrics Domain and its relationship with primary stakeholders and members of the community of interest (COI). The charter should be referenced alongside the Biometrics Domain Management Plan, which outlines the domain’s processes and procedures for managing and executing domain activities. Section 2.2 describes the scope of the Biometric Domain.

## Intended Audience

This document’s intended audience comprises the Biometrics Domain stakeholders and governance groups, as well as the NIEM PMO for reference purposes.

## Reference Documents

The following reference documents will assist in the establishment and maintenance of the Biometrics Domain:

* NIEM High-Level Version Architecture
* NIEM Concept of Operations
* NIEM Guidance for Designing Domain Governance
* Biometrics Domain Management Plan

# Domain Overview

## Domain Mission

A *domain* is a business enterprise broadly reflecting the government organizations, operational functions, aligned services, and mission-critical information systems that are organized or affiliated to meet common objectives. The NIEM Biometrics Domain supports biometric-related services and activities of the biometric management user community, including DHS, the Department of Defense (DOD), and the Department of Justice (DOJ). Further, the domain supports information sharing and exchange to improve those services, while fostering better collaboration with external partners by enabling timely, accurate, and actionable information sharing using scalable NIEM-conformant exchanges and data.

## Domain Scope

Domain stewards are COI members responsible for actively managing and updating their community’s data model. As the Biometrics Domain steward, OBIM will manage the domain within the NIEM data model in support of the Biometric COI. In cooperation with the domain executive management team and associated committees, OBIM will support the NIEM PMO relative to the NIEM Biometrics Domain issues by:

* Creating a technical infrastructure for domain management activities, including technical development, testing, review, and deployment of the biometric contents to the NIEM data model
* Creating the NIEM High-Level Version Architecture (HLVA), the NIEM Naming and Design Rules (NDR), the NIEM Model Package Description Specification, the NIEM Domain Update Specification, and other documentation, standards, and guidelines to maintain the domain content, and participating in cross-domain harmonization activities
* Recommending new NIEM Core components supporting the Biometrics Domain
* Managing, harmonizing, and reusing NIEM components across the Biometrics Domain COI
* Developing, recommending, and implementing processes to ensure that the Biometrics Domain meets the NIEM conformance requirements, as outlined in the NIEM Conformance document
* Expanding the scope of the Biometrics Domain to incorporate additional data elements, reflecting the evolution and expansion of Biometrics Domain requirements
* Tracking technical issues and requirements to ensure their timely resolution, and as required, incorporation in NIEM releases, documentation, communications and training, tools, etc.

## Domain COI

The NIEM Biometrics Domain COI is diverse and dynamic and includes representatives from international, federal, state, and local organizations and agencies that use biometric data and information to support services and operations. The COI may also include key stakeholders, practitioners, advisors, and subject matter experts from private sector organizations, as approved by the Biometrics Domain Executive Management Committee.

## Domain Goals

The Biometrics Domain goals align with the domain scope and parameters outlined in Section 2.2. To be successful in fostering development and harmony within a domain, the domain must achieve independence, while facilitating self-service.

Domain independence ensures that there are domain specifications and processes that decouple the domain from the NIEM Core development timeline. Such decoupling allows domains to publish specification updates per domain requirement and domain-specific timelines rather than per the Core update timelines. It also allows systems owners and developers to move quickly with the latest Information Exchange Package Document (IEPD) materials and tools.

Domain self-service closely aligns with independence―the domain has the authority, autonomy, and capability to maintain its own content development and management, ensuring proactive engagement within the domain and benefiting NIEM scalability as domains lend to the NIEM Core reach and utility.

This scope of activity and interest supports the following operational and managerial goals:

* Provide access to timely, accurate, and actionable information using scalable NIEM-conformant exchanges and data
* Ensure compatibility with other data standards
* Allow instant reporting from validated partner systems sharing biometric data structure and attributes
* Ensure that data are obtained in readily consumable formats
* Facilitate near real-time digital submittal from diversified systems
* Frame and share an Office of Management and Budget-endorsed, proven best practice
* Encourage harmonization and adoption across agencies and non-government entities

# NIEM Governance Structure

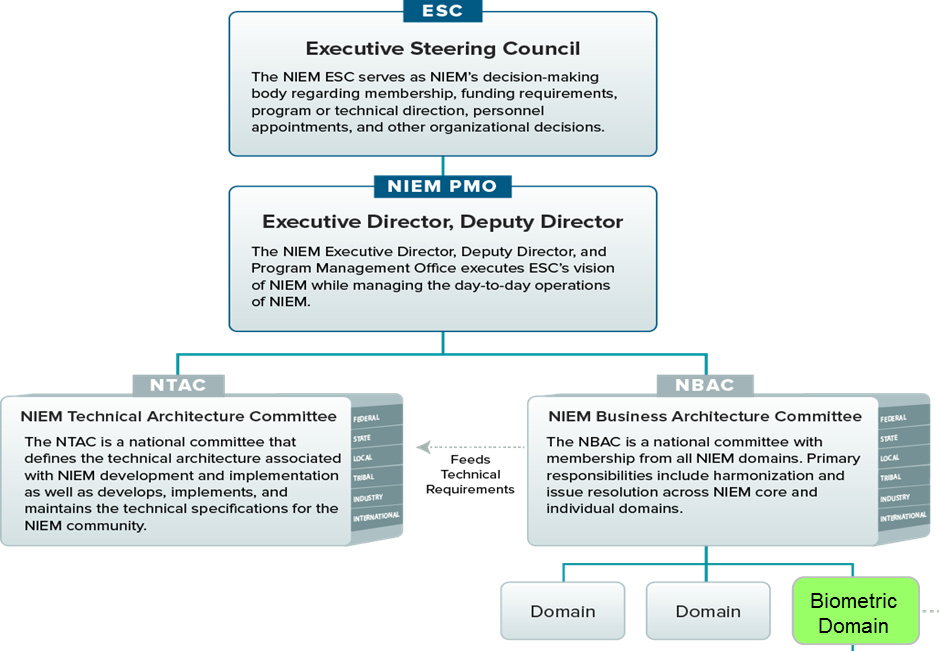
NIEM is governed by federal, state, local, tribal, and private organizations, groups, and committees that support its development, day-to-day operations, and evolution, as depicted in Figure 1. The governance model includes:

*NIEM Executive Steering Committee (ESC):* The ESC serves as NIEM’s decision-making body regarding membership, funding requirements, program and technical direction, personnel appointments, and other organizational decisions supporting NIEM management. The primary sponsors of NIEM are chief information officers of DHS, DOJ, and U.S. Health and Human Services―all members of the ESC.

*NIEM PMO:* The NIEM PMO executes the ESC’s vision for NIEM while managing the program’s day-to-day operations, encouraging adoption and use of NIEM, and overseeing working group and committee activities. The NIEM PMO also coordinates with COIs, principal stakeholders, and other information-sharing initiatives to promote collaboration and interest in NIEM priorities.

*NIEM Business Architecture Committee (NBAC):* The NBAC mission is to establish the NIEM business architecture and requirements, to manage the NIEM Core, and to facilitate the processes for the regulation and support of NIEM domains.

*NIEM Technical Architecture Committee (NTAC):* The primary mission of the NTAC is to define and support the technical architecture that governs NIEM. NTAC members represent operational practitioners and subject matter experts, key stakeholder agencies, domains, and systems developers throughout the levels and branches of government, as well as solution providers. Membership types include co-chairs, voting members, PMO liaison, lead developers, and observers/invited participants.



***Figure 1: NIEM Governance Structure***

The Biometrics Domain executive management team will work closely with the COI and via special working groups, in alignment with the domain governance process, to ensure that technical recommendations are considered from a business perspective and that business decisions are appropriately reviewed for technical feasibility. Domain governance and alignment of the Biometrics Domain within the NIEM content model is essential to the success of the Biometrics Domain.

The Biometrics Domain governance structure aligns with the American National Standards Institute (ANSI)/NIST and NIEM governance frameworks and best practices, including governance bodies and dispute resolution mechanisms and procedures. The Domain Management Plan also provides information on the governance structure as it relates to operations and activities.

Domain governance is formal, robust, and proactive. Dispute and conflict resolution is managed in alignment with and adherence to ANSI/NIST conflict resolution and appeal procedures.

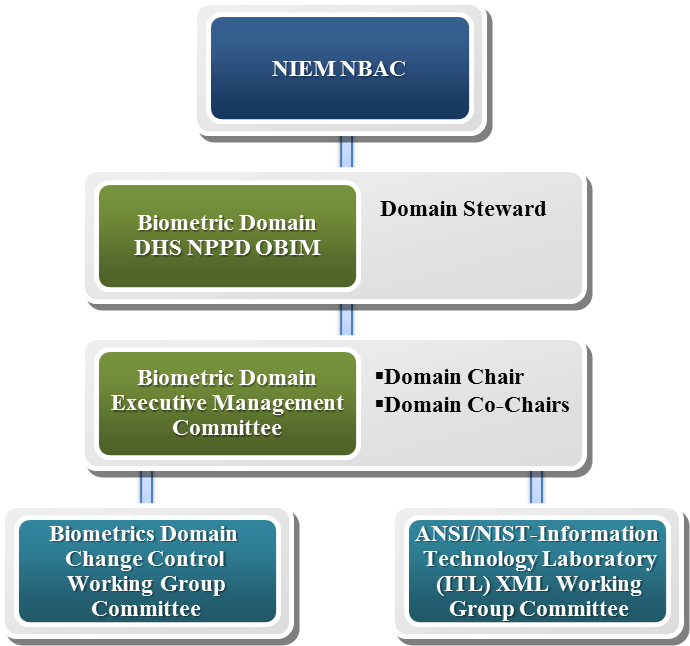
# Domain Governance Structure

OBIM is the domain steward, whose responsibilities are described in Section 3.3. In association with the domain steward, members of the Domain Executive Management Committee are responsible for providing domain guidance.

Domain Executive Management Committee members include the Biometrics Domain chair (John Boyd of OBIM) and two co-chairs (Jennifer Stathakis of DOJ/Federal Bureau of Investigation and William Graves of DOD) and the NIST Ombudsman (Diane Stephens).

Two primary working groups address technical and business/operational issues. Section 3.4 describes the working groups’ structure, membership requirements, and responsibilities.

In addition to the standing technical and business operations committees, the Biometrics Domain may initiate tiger teams composed of COI members to address specific issues in support of either working group or of the domain at large.



***Figure 2: NIEM Biometrics Domain Governance Structure***

# Domain Governance and NBAC Relationship

As the central authority in a federated governance model, NBAC interacts with domain governance groups, providing coordination and policy and technical direction and allowing each domain governance group to retain relative autonomy in governing its domain while interacting with its own COI.

Information concerning the Biometrics Domain and associated issues of domain management and standing working groups will be communicated to the NIEM PMO and NBAC regularly to apprise stakeholders of developments and activities. This communication is a primary responsibility of the domain steward and the Domain Executive Management Committee.

# Domain Steward

OBIM is the NIEM Biometrics Domain steward, pursuant to the NIEM Domain Stewardship Agreement signed in March 2012 by OBIM (previously US-VISIT) and the NIEM PMO.

## Domain Steward Responsibilities

Domain steward responsibilities are broad and include strategic domain planning initiatives in concert with the COI, as well as operational and tactical activities that facilitate daily and ongoing operations.

The NIEM Domain Stewardship Agreement, required for all domains, defines the expectations and responsibilities of the NIEM domain steward, as follows:

* Provide a contact list of all members and organizations represented by the newly established COI who will coordinate and collaborate with the steward and governing body of the new domain; the list shall include primary points of contact who will interface regularly with the NIEM PMO
* Provide a common data dictionary of elements to be included in NIEM that spans federal, state, local, tribal, private, and international boundaries represented by the COI
* Provide a completed executive summary cover sheet and Component Mapping Template (CMT) for the Biometrics Domain, conforming to the NIEM NDR (executive summary and CMT templates are maintained by the NIEM PMO, and the NDR is available at [www.niem.gov](http://www.niem.gov))
* Provide a charter documenting the governance processes related to release management and publication (including a planned schedule), as defined in NIEM HLVA
* Participate in NIEM harmonization and reconciliation activities, as required by NBAC
* Report NIEM technical issues using the issues tracking tools provided by NIEM PMO and NIEM Help Desk
* Use the issue tracking tools to submit all formal comments on technical or policy issues for resolution tracking and auditing
* Support domain reconciliation and cross-domain harmonization resulting in future NIEM releases (major and minor), as needed
* Provide Tier 2 and Tier 3 technical support for domain-specific issues related to NIEM and Information Exchange Package Document (IEPD) development, to assist implementers and developers
* Understand and incorporate related external data standardization initiatives, as appropriate
* Record and track identification of data requirements based on exchange/data modeling and development efforts

Additional specific actions for which the domain steward will be responsible during the initial stages of the Biometrics Domain formation and operation include:

* Establishing the domain within NIEM.gov
* Creating the Domain Charter and Domain Management Plan
* Ensure that governance framework aligns with ANSI/NIST
* Use Biometrics Domain COI to vet, facilitate, and authorize the biometric schema created by NIST Biometrics Working Group and beyond
* Increase COI knowledge of NIEM and IEPD development (training and technical support)
* Create a harmonized interagency biometric roadmap
* Create an IEPD repository to enable reusability
* Develop the domain information exchange governance process
* Ensure external data standardization and collaboration support
* Support domain maintenance and the Change Management Plan
* Initiate the requirements management process and capture change requests
* Support domain-vetting and team-building processes
* Produce and deliver communication materials, implementation guidance, and presentations, as needed
* Provide domain quality assurance and domain stability
* Implement verification for IEPD practitioners
* Maintain synchronicity and understanding of related international data standardization initiatives, as appropriate

## Domain Steward Mission

The OBIM mission is inextricably linked with the mission and objectives of the Biometrics Domain. OBIM supports the DHS responsibility to protect the nation by providing biometric identification services helping international, federal, state, and local government decision makers accurately identify the people they encounter, and determine whether those people pose a risk to the United States. OBIM supplies the technology for collecting and storing biometric data, provides analysis, updates its watchlist, and ensures the integrity of the data.

The stated OBIM vision is “a more secure nation through advanced biometric identification, information sharing, and analysis.”

OBIM operates under the following guiding principles:

* Enhance the security of our citizens and visitors
* Facilitate legitimate travel and trade
* Ensure the integrity of the immigration system
* Protect the privacy of our visitors

# Domain Members

Members of the biometric COI may join the Biometrics Domain as domain members to actively participate in domain decisions and activities. Membership is achieved via sign-up with a threshold review for alignment before acceptance by domain management. Domain member responsibilities are to:

* Spend a minimum of 12 hours per month on tasks, such as reviewing and providing solutions to or comments on technical publications or standard guidance
* Serve a minimum term of one year (renewable)
* Participate in at least one face-to-face Biometrics Domain meeting per year
* Attend formally scheduled meetings (including conference calls)
* Accept action items and task assignments; be willing to expend additional efforts outside the formal Biometrics Domain meetings or conference calls to complete responsibilities by their deadlines
* Support the NIEM Biometrics Domain steward, Executive Management Committee, and other standing committees and working groups, as needed
* Assist in completion of individual and group tasks
* Provide an access point to stakeholders in own community

A member may be asked to leave the Biometrics Domain for failure to meet the membership responsibilities. The NIEM Biometrics Domain Executive Management Committee, with a consensus vote of domain members, makes membership termination decisions.

# Domain Governance Committee(s)

As stated in Section 3.1, OBIM is the NIEM Biometrics Domain steward. In association with the domain steward, members of the Domain Executive Management Committee (named in Section 3.1 are responsible for providing domain guidance.

For organizations interested in active contribution, the NEIM Biometrics Domain has two primary standing working groups: the Biometrics Domain Change Control Working Group (BDCCWG) and the ANSI/NIST-Information Technology Laboratory (ITL) XML Working Group (ANXMKWG). The two working groups are administered by the domain steward in conjunction with the Domain Executive Management Committee, which communicates issues and resolutions among the working groups, the NIEM PMO, and the COI.

During the first year of committee/working group establishment, the Domain Executive Management Committee will appoint a chair for each committee/working group. Thereafter, the chair will be selected annually by members of the committee/working group―by consensus vote, with one vote per participating organization.

## Committee Membership

The Domain Executive Management Committee comprises COI members and domain management. The committee is composed of the domain chair and two co-chairs. The domain chair will be appointed by the domain steward. Co-chair is a rotating position selected by the domain steward and chair, and the individuals selected must be from an organization outside of OBIM as the domain steward.

Participation in the standing committees/working groups (the BDCCWG and the ANXMKWG) is open to members of the COI, including key stakeholders, practitioners, advisors, and subject matter experts.

Organizations must join the group most closely aligned to their operational parameters and interests, and must exhibit their ability to contribute to the group based on subject matter expertise or ongoing operational parameters. COI members will be given a domain and a working group sign-up sheet to express their interest in participation and to provide their interest and capability statements.

A standing committee/working group member may be asked to leave the committee for failure to meet the membership responsibilities. The NIEM Biometrics Domain Executive Management Committee, with a consensus vote of committee members, makes membership termination decisions.

## Committee Roles and Responsibilities

The Biometrics Domain Management Plan presents the structure and operations of the Biometrics Domain. The Biometrics Domain structure and operations are adapted to best address the needs of the Biometrics Domain COI and NIEM PMO priorities.

The Domain Executive Management Committee maintains general domain management, advisory, and communications responsibilities, which include:

* Prioritizing the program goals and tasks related to the Biometric Domain effort
* Facilitating stakeholder participation in the development and maintenance of the Biometric Domain
* Serving as the official liaison and representative for the Biometric Domain in all matters when interacting with NIEM PMO leadership and executive sponsors
* Providing guidance and direction to the domain working groups and standing committees

The technical and operations standing committees have responsibilities closely aligned with their operational areas of interest. The BDCCWG, which meets jointly with the ANXMKWG, presents changes proposed by ANXMLWG to the Biometric Domain executive management team for implementation and official incorporation in the domain. No portions of the Biometric Domain may be removed or altered that affect ANSI/NIST-ITL implementation without the approval of the BDCCWG and the ANXMLWG.

For its part, the ANSI/NIST-ITL Standards Developing Organization will work closely with the Biometrics Domain to ensure that all requirements of the ANSI/NIST-ITL Standard are included in the domain, and that backward compatibility is maintained across versions of the standard and the domain.

## Domain Dispute and Conflict Resolution Mechanisms

For disputes arising within the scope of Biometrics Domain operations, including those regarding domain management and standing committees/working groups, as well as ancillary issues to the domain within the COI (may require domain comment or resolution), the Biometrics Domain has put in place processes aligned with and in adherence to those within the ANSI/NIST conflict resolution and appeal procedures (see Section 3.5.1.5).

Domain dispute and conflict resolution includes a process and framework for adjudication and resolution of higher-level disputes and conflicts, including an appeals process.

## Consensus Agreement and Due Process Representation

This charter relies on the processes promulgated by ANSI (ANSI Canvass Method) and put forth by NIST/ITL in ANSI/NIST-ITL and the Canvass Method (<http://www.nist.gov/itl/iad/ig/ansi_standard-canvass.cfm>).

As stated in the procedures for decision making, standards (or other resolutions) development and general domain activity should satisfy ANSI’s essential requirements for openness, balance, due process, and consensus. According to the ANSI Canvass Method, a consensus body “that includes those who are known to be, or have indicated that they are or would be, directly and materially affected by” domain activities should be used. As with voluntary consensus standards development, efforts are made “to ensure balance on the consensus body, and to implement due process procedures that guard against dominance by one or more interests where dominance means a position or exercise of dominant authority, leadership, or influence by reason of superior leverage, strength, or representation to the exclusion of fair and equitable consideration of other viewpoints.” Thus, each consensus body organization shall have one vote, so that no organization with multiple members on any domain body can exert undue influence on domain activities and decisions.

## Dispute/Conflict Resolution (Appeals)

This charter relies on the NIST appeals process put forth in NIST Procedures for the Development of American National Standards (<http://www.nist.gov/itl/ansi/upload/NISTITLANSProcedures-ReaccreditedMarch182008.pdf>).

Within this framework, “persons who have directly and materially affected interests and who have been or may be adversely affected by a procedural action or inaction of the Domain or any of its standing committees shall have the right to appeal.”

An impartial appeals body composed of at least three individuals knowledgeable of the policy or other concerns related to the appeal will be formed, with care taken to ensure that these individuals do not have demonstrably real or apparent conflict of interest with the subject of the appeal or the person filing the appeal. To commence this process, the following actions must be taken:

1. Filing or submission of complaint via Domain Executive Management Committee

The appellant shall file a written complaint with the committee within 30 calendar days after the date of notification of action, or at any time with respect to inaction. The complaint shall state the nature of the objection(s), including any adverse effects, the clause(s) of these procedures or the standard at issue, actions or inactions at issue, and the specific remedial action(s) that would satisfy the appellant’s concerns. Previous efforts to resolve the objection(s) and the outcome of each shall be noted.

1. Response

Within 30 calendar days after receipt of the complaint, the committee shall respond in writing to the appellant, addressing each allegation of fact in the complaint to the extent of the respondent’s knowledge.

1. Hearing

If the appellant and the respondent are unable to resolve the written complaint informally in a manner consistent with these procedures, the committee shall schedule a hearing with an appeals panel on a date agreeable to all participants, giving at least 10 working days of notice. A hearing will be conducted via teleconference; alternatives to a teleconference may be considered.

4) Appeals panel

The appeals panel shall consist of three individuals who have not been directly involved in the matter in dispute, and who will not be materially or directly affected by any decision made or to be made regarding the dispute. At least two members shall be acceptable to the appellant and at least two members shall be acceptable to the respondent.

5) Conduct of the hearing

The appellant has the burden of demonstrating adverse effects, improper actions or inactions, and the efficacy of the requested remedial action. The respondent has the burden of demonstrating that the consensus body and the Biometrics Domain took all actions in compliance with these procedures and that the requested remedial action would be ineffective or detrimental. Each party may adduce other pertinent arguments, and members of the appeals panel may address questions to individuals. Robert’s Rules of Order (Scott, Foresman and Company, 2000) shall apply to questions of parliamentary procedure not covered herein.

6) Decision

The appeals panel shall render its decision in writing within 30 calendar days, stating findings of fact and conclusions, with reasons therefore, based on a preponderance of the evidence presented to the appeals panel. Consideration shall be given to the following positions, among others, in formulating the decision:

a) Finding for the appellant, remanding the action to the consensus body or the domain with a specific statement of the issues and facts regarding which fair and equitable action was not taken

b) Finding for the respondent, with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant’s objections

c) Finding that new, substantive evidence has been introduced, and remanding the entire action to the consensus body or the domain for appropriate reconsideration

A summary of the nature of the appeal, and the decision and rationale thereof, shall be reported by the Domain Executive Management Committee to the COI.

# Domain Charter Modifications

This charter is subject to change. As the Biometrics Domain and its COI grow, the charter will be revisited and revised as necessary. Review and revision will be coordinated with oversight of the Biometrics Domain steward, in accordance with domain governance rules and frameworks and in cooperation with the Biometrics Domain COI.

# Acronyms and Abbreviations

|  |  |
| --- | --- |
| ANSI | American National Standards Institute |
| ANXNKWG | ANSI/NIST-ITL XML Working Group |
| BDCCWG | Biometrics Domain Change Control Working Group |
| CMT | Component Mapping Template |
| COI | Community of Interest |
| DHS | Department of Homeland Security |
| DOD | Department of Defense |
| DOJ | Department of Justice |
| ESC | Executive Steering Committee |
| HLVA | High-Level Version Architecture |
| IEPD | Information Exchange Package Documentation |
| IDENT | Automated Biometric Identification System |
| ITL | Information Technology Laboratory |
| NBAC | NIEM Business Architecture Committee |
| NDR | Naming and Design Rules |
| NIEM | National Information Exchange Model |
| NIST | National Institute of Standards and Technology |
| NPPD | National Protection and Programs Directorate |
| NTAC | NIEM Technical Architecture Committee |
| OBIM | Office of Biometric Identity Management |
| PMO | Program Management Office |
| US-VISIT | United States Visitor and Immigrant Status Indicator Technology |

# Additional References

* Domain Governance: https://www.niem.gov/communities/domain-governance
* NIEM High Level Version Architecture 3.0: https://reference.niem.gov/niem/specification/high-level-version-architecture/3.0/
* NIEM Domain Update Specification, Version 1.0: http://reference.niem.gov/niem/specification/domain-update/1.0/
* NIEM Model Package Description Specification 3.0.1: https://reference.niem.gov/niem/specification/model-package-description/3.0.1/
* NIEM Naming and Design Rules, Version 4.0: https://reference.niem.gov/niem/specification/naming-and-design-rules/4.0/
* NIEM Conformance Specification 3.0: https://reference.niem.gov/niem/specification/conformance/3.0/