

**IAM@HHS Program Charter**

US Department of Health & Human Services

October 14, 2009 Version 1.0

**Table of Contents**

[Executive Summary 3](#_Toc242788727)

[1 Purpose 4](#_Toc242788728)

[2 Program Overview 4](#_Toc242788729)

[2.1 Problem Statement 5](#_Toc242788730)

[2.2 Program Objectives 6](#_Toc242788731)

[2.3 Expected Benefits 7](#_Toc242788732)

[2.4 Planned Program Milestones 8](#_Toc242788733)

[2.5 Critical Success Factors 9](#_Toc242788738)

[3 Program Governance 10](#_Toc242788739)

[3.1 HHS Governance Bodies 11](#_Toc242788740)

[3.2 IAM@HHS Governance 11](#_Toc242788741)

[3.3 Program Management and Execution 13](#_Toc242788742)

[4 Program Charter Approvals 17](#_Toc242788743)

# Executive Summary

A major recommendation of the HHSIdentity Program Review Board Report (the “Report”) is to create a single, unified Program Management Team (PMT) to manage the full breadth of physical and logical access activities. This recommendation reflects and reinforces the stated desire of the Service and Supply Fund Board (SSFB) to simplify planning and management of the overall Homeland Security Presidential Directive-12 (HSPD-12) efforts. Further, the Report recommends the maximum use of detailed OPDIV/STAFFDIV[[1]](#footnote-1) staff be used to fill critical PMT positions.

The implementation of the PMT and the associated program governance body will ensure the HSPD-12 mandate is fully implemented throughout the Department of Health and Human Services (HHS) by the full enrollment of personnel by October 27, 2009 and full badge issuance by July 1, 2010, or sooner, and reaching all intermediate goals along the way.

This charter formally authorizes the Identity and Access Management at HHS (IAM@HHS) program and grants members of the IAM@HHS PMT authority to apply organizational resources to program activities and tasks. This charter also defines the program’s scope, describes the expected benefits the program intends to deliver to HHS, and defines the program governance structure, roles and responsibilities for managing the program. Although limited to a high-level overview in its initial form, the charter:

* Demonstrates alignment to HHS enterprise strategy, goals and priorities
* Establishes clear success criteria based on expected benefits
* Establishes the program’s guiding principles and processes
* Communicates control mechanisms to stakeholders (e.g., by defining the charter of the key IAM@HHS governance body within the document, the Program Oversight Group)

Changes to this document must be approved by the program’s Executive Sponsor. This program charter formally documents the approval and authority given to the IAM@HHS program. Additional details regarding the program are to be documented in the IAM@HHS Program Management Plan.

# Purpose

This charter formally authorizes the Identity and Access Management at HHS (IAM@HHS) program and grants members of the IAM@HHS Program Management Team (PMT) authority to apply organizational resources to program activities and tasks. This charter also defines the program’s scope, describes the expected benefits the program intends to deliver to the U. S. Department of Health and Human Services (HHS), and defines the program governance structure, roles and responsibilities for managing the program. Although limited to a high-level overview in its initial form, the charter:

* Demonstrates alignment to HHS enterprise strategy, goals and priorities
* Establishes clear success criteria based on expected benefits
* Establishes the program’s guiding principles and processes
* Communicates control mechanisms to stakeholders (e.g., by defining the charter of the key IAM@HHS governance body within the document, the Program Oversight Group)

Changes to this document must be approved by the program’s Executive Sponsor. This program charter formally documents the approval and authority given to the IAM@HHS program. Additional details regarding the program are to be documented in the IAM@HHS Program Management Plan.

# Program Overview

The safety, security, and well-being of all HHS staff and HHS facilities are of the utmost concern to the new Administration and to the entire HHS leadership team. Given the potential threat from multiple sources against HHS personnel, scientific assets, intellectual property, or the potential for tampering with HHS computers and information systems, it is important that all staff at HHS agencies be aware of how important it is that HHS be in full and active compliance with the HSPD-12. The Deputy Secretary restructured and consolidated the Department's HSPD-12 and access management programs into a new unitary structure known as "IAM@HHS."

The IAM@HHS program emerged as a result of a review of the HHSIdentity program. With the adoption of the HHSIdentity Program Review Report (the "Report") by the CIO Council and the ITIRB at the May 19, 2009 combined meeting, and under the guidance in the Deputy Secretary's memorandum to the Heads of Operating and Staff Divisions on July 2, 2009, the new program must begin the process to implement the approved recommendations contained in that report, as well as initiate the incorporation of planning and oversight activities with those that are within the realm of HSPD-12 activities within the scope of Service and Supply Fund Board (SSFB) support. This new name reflects the consolidation and integration of previous HHSIdentity and HSPD-12 programs.

A major recommendation of the HHSIdentity Program Review Report is to create a single, unified PMT to manage the full breadth of physical and logical access activities. This recommendation reflects and reinforces the stated desire of the SSFB to simplify planning and management of the overall HSPD-12 efforts. Further, the Report recommends the maximum use of detailed OPDIV/STAFFDIV[[2]](#footnote-2) staff be used to fill critical PMT positions. The IAM@HHS charter defines the program’s scope, describes the expected benefits the program intends to deliver to HHS, defines the program governance structure (including the charter for the Program Oversight Group) and presents roles and responsibilities for managing the program.

## Problem Statement

Guidance on common terminology for identity cards provided by the Federal CIO Council[[3]](#footnote-3) defines three kinds of personal identity cards:

1. **PIV Card** – an identity card that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV Cards are interoperable with and trusted by all Federal government relying parties. The HHS ID Badge is an example of a PIV Card.
2. **PIV Interoperable (PIV-I) Card** – an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued by Non-Federal Issuers (NFIs) in a manner that allows Federal government relying parties to trust the card.
3. **PIV Compatible (PIV-C) Card** – an identity card that meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not been issued in a manner that assures it is trustworthy by Federal government relying parties. The Common Access Card (CAC) issued by the Department of Defense (DOD) is an example of a PIV-C card.

The IAM@HHS program identifies any other form of facility or local access credentials not conforming to one of these three kinds of identity cards as “*Non-PIV/-I/-C Cards*”.

The IAM@HHS program was established to create Identity and Access Management (IAM) capabilities to securely issue Personal Identity Verification (PIV) credentials to authorized persons, as well as manage physical and logical access to Government facilities, systems and assets in accordance with HSPD-12 and Federal Information Processing Standards (FIPS) 201-1 requirements.

HHS has a need to monitor and address evolving global and national health issues requiring HHS to expand its ability to:

* Gather and process vast amounts of information;
* Collaborate with a diverse set of partners and affiliates; and
* Extend services to a widely dispersed set of constituents.

At the same time, HHS must do this in an environment that requires:

* Reducing the cost of services while improving their efficiency and effectiveness;
* Improving the security of and maintaining the privacy of information and assets;
* Communicating effectively and collaboratively with IAM OPDIV representatives;
* Ensuring the ability to quickly and effectively react to crises and changing environmental conditions; and
* Meeting legislative and executive mandates.

A key enabler for meeting these challenges is to establish integrated and automated IAM capabilities that can span both within and across the HHS enterprise boundaries.

## Program Objectives

The IAM@HHS program combines the HSPD-12 program and the former HHSIdentity program as a single unified initiative. The combined goals of the IAM@HHS program are to:

* Support OPDIVs in the NIST SP 800-79-1 PIV Card Issuing Facility accreditation process;
* Participate in and ensure HHS compliance with external identity management groups, including, but not limited to, the Identity, Credential and Access Management (ICAM) sub-committee of the Federal CIO Council’s Information Security & Identity Management Committee;
* Integrate the HHS and OPDIV Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS);
* Provide IAM foundation services such as directories, IAM repositories, IAM tools and audit capability, and physical HSPD-12-compliant and electronic identity credentials;
* Develop a base service to assign a Department-wide unique person identifier (UPI);
* Coordinate E-Authentication enablement at a system level; and
* Provide the PIV-II card issuance systems and logical access as part of fulfilling the HSPD-12 mandate.

The IAM@HHS program will institute a federated IAM model at HHS that:

* Allows large OPDIVs with significant IAM investments [National Institutes of Health (NIH), Centers for Disease Control and Prevention (CDC), Centers for Medicaid and Medicare Services (CMS) and Food and Drug Administration (FDA)] to continue to develop individual IAM services and ensure these large OPDIVs have the ability to federate with external HHS IAM services and services external to HHS
* Establishes the Enterprise IAM Service supporting:
	+ Office of the Secretary (OS) and Small OPDIVs through the Program Support Center (PSC)
	+ Enterprise Systems
	+ Indian Health Service
* Establishes the virtual Enterprise Repository containing the core set of identity attributes with standards-based exchange of identity information between OPDIVs
* Provides standards-based authentication and system access between IAM services
* Provides standards-based authentication and system access for users external to HHS leveraging the E-Authentication framework
* Provides standards-based PACS.

IAM@HHS will provide these services for:

* All OPDIVs under HHS that opt into the common solution (non-federated solution);
* Other Departments and agencies with which HHS has, or will develop, MOU agreements to provide such services; and
* Other Agencies, if HHS is identified as a line of business provider.

## Expected Benefits

The IAM@HHS program intends to deliver the following benefits to the HHS enterprise and its stakeholders:

* Access to any HHS campus with the use of one PIV card;
* Providing a comprehensive IAM architecture and infrastructure design to allow OPDIVS to share applications and data with authorized users;
* Satisfying applicable regulatory requirements (HSPD-12, NIST, FIPS, etc.) including M-04-04, FIPS 201-1, and NIST SP 800-63, -76, -79-1, -85, -87, -116;
* Aligning and adhering to HHS Enterprise Performance Life Cycle (EPLC), Enterprise Architecture (EA), and federal Identity, Credential, Access Management (ICAM) guidance and requirements.

The following table identifies additional benefits grouped by category.

|  |  |  |
| --- | --- | --- |
| **Business Facilitation Benefits** | **Cost Containment Benefits** | **Risk Management Benefits** |
| **Unique Identifiers Across Agencies** * + Ability to uniquely identify and manage the access for any member of the workforce across all of HHS
	+ Eliminate need to register individuals or entities in more than one people repository.
	+ Unique key for a person across any people or role repository

**Digital Signatures*** + Automation of manual processes
	+ Reduction in paperwork
	+ Increase in speed of transmission

**Single Sign On*** + Fewer usernames and passwords to remember
	+ Faster access to critical information

**Cross-Agency Reporting** – Federation allows for advanced Business and Technical Analytics across the Department | **Single Sign On** * + Reuse of standard services such as password resets
	+ Reduction of development and maintenance costs
	+ Elimination of redundant help desk support services at multiple locations
	+ Savings associated with reduction in password resets

**Information Sharing Network** – Rapid data share reduces costs associated with delays | **Mobile Device Security** – Stronger authentication to mobile devices**Data Encryption of Sensitive Information** – Avoid negative impact to the mission through loss of citizen confidence in our ability to manage sensitive data**Enhanced Auditing Services*** + Resolve systemic security weaknesses repeatedly identified during internal audits
	+ Automated audit and role management capabilities that extend from networks to applications

**Stronger Authentication*** + Adds a higher level of identity proofing with a stronger credential
	+ Non-repudiation to validate that a user is who they say they are
	+ Deters identity fraud, counterfeiting, and identity exploitation
 |
| **Operational Efficiency Benefits** |
| **Application Sharing** * + Provides the capability for application and tool sharing
	+ Streamlined, secure approach to collaboration through resources such as Wikis or SharePoint
	+ Provide access to shared data through standard technology interfaces

**Information Sharing Network** – Increased efficiency in emergencies **Enhanced Revocation*** + Ability to automate across the Department any physical and logical access and role
	+ Timely de-activation and revocation of user accounts and credentials
 |

#

## Planned Program Milestones

The major IAM@HHS milestones currently planned for the duration of the program (2009 through 2013) are summarized below. Additional milestones will be identified and tracked through the program’s iterative planning, execution and monitoring processes.

**Phase 1** **(September 2009 – March 2010):**

* September 26, 2009 – Award multiple statements of work to contractors to execute Identity, Access and Credential Management workstream development activities as well as program management workstreams.
* Develop Charter and Program Communications Plan
* October 27, 2009 – HSPD-12 Enrollment Milestone per OMB
* Create Five (5) Year Program Lifecycle Plan with integrated EPLC and federal ICAM milestones
* Deliver Estimated Program Lifecycle Cost Model for OPDIVs and Department
* Complete Policy Gap Analysis (and Policy/Guidance Drafts as applicable)
* Initiate Identity Management capability upgrades
* Develop Non-PIV-I/-C Use Cases
* Develop Department-level Physical and Logical Access Plan
* Prepare Enterprise Applications for SSO Integration
* Develop 6-Month PMT Status and Recommendations Report

**Phase 2 (March 2010 – October 2011):**

* May 31, 2010 – OPDIV Physical and Logical Access Plans complete
* July 1, 2010 – PIV Card Issuance Status Milestone
* Complete Stand-Up of Identity Management capability
* Complete Bi-Directional National Institutes of Health (NIH) Federation
* Complete Active Directory (AD) consolidation
* 100% PIV enrollment
* Initiate Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS) Integration
* PIV enablement of key enterprise applications and OPDIV external facing systems and OPDIV specific systems
* Complete implementation of basic provisioning for key departmental applications
* Complete federation and/or SSO integration with CDC, FDA and CMS
* Begin review and development of Role Management strategy for HHS and OPDIVs

**Phase 3 (October 2011 – October 2012):**

* Continued PIV enablement of key enterprise applications and OPDIV external facing systems and OPDIV specific systems
* Complete Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS) Integration

**Phase 4 (October 2011 – October 2012):**

* IAM@HHS will continue until project is in O&M

## Critical Success Factors

The following statements describe conditions that must be met to ensure the success of the program.

* Members of the Program Oversight Group (POG, described below) representing the OPDIVs must provide the highest level executive support and contribute resources wherever possible to ensure that program benefits are achieved for all parts of the HHS enterprise.
* The IAM@HHS Program Manager will develop a holistic management view of IAM@HHS that addresses dependencies and critical paths as part of an integrated master schedule and workstream project plans at an appropriate level of detail. The result of this effort will be a documented program management plan. The IAM@HHS Program Manager will use this plan to manage the program.
* Roles within the IAM@HHS Program Management workstream will follow the Enterprise Performance Life Cycle (EPLC) framework and coordinate with the appropriate IT governance bodies to complete any required stage gate reviews.
* The IAM@HHS PMT will collaborate with IAM OPDIV representatives and use the visibility provided by the Program Oversight Group to:
	+ Document business processes for physical and logical access including, for example, identity verification and credential management, as well as any others deemed critical.
	+ Identify unique OPDIV-specific identity and access management solutions and leverage these solutions for possible reuse.
	+ Assist the OPDIVs in planning logical access implementations by identifying dependencies between the Department-level activities and activities undertaken within each of the OPDIVs.

.

# Program Governance

Figure 2 below depicts the key workstreams, roles and governance bodies of the IAM@HHS program and how they are organized to make decisions and execute program tasks. The established Program Management Team workstreams may change as the project moves forward. For example, the program may add, consolidate or remove workstreams that are no longer needed.

1. Program Governance Structure



Governance of the IAM@HHS program activities is organized into three levels:

1. HHS Governance Bodies
2. IAM@HHS Governance
3. Program Management and Execution.

Decision-making capabilities exist at all levels and issues and risks can be escalated whenever higher-level decisions are required.

## HHS Governance Bodies

The following Department-wide governance bodies have input and approval responsibilities that affect and interact with the IAM@HHS program.

### Information Technology Investment Review Board (ITIRB)

The HHS ITIRB is an HHS enterprise-wide executive steering committee made up of IT and business executives from across the Department. This body is responsible for overseeing the management of the HHS IT investment portfolio, approving the allocation of IT resources to best achieve HHS strategic goals and objectives within budget limits, and leveraging opportunities for collaboration within the Operating Divisions (OPDIVs) on IT investments that support common lines of business. As part of the HHS Capital Planning and Investment Control Review process, the Program Oversight Group brings issues of business value to the HHS ITIRB for review and concurrence. The ITIRB shall decide whether to give business approval (including funding level and source) for the IAM@HHS program investment and approve cost, schedule and performance baselines for the program. HHS ITIRB is the governance body for all HHS Enterprise IT Projects. All EPLC stage reviews will be conducted by the ITIRB.

### CIO Council

The HHS CIO Council is chaired by the HHS CIO with membership comprised of all HHS OPDIV CIOs. This body is responsible for reviewing and vetting technological approaches and architectural conformance of IT projects at HHS. As part of the HHS Capital Planning and Investment Control Review process, the Program Oversight Group shall bring issues of IT technical approach to the HHS CIO Council for review. The CIO Council is then responsible for advising the ITIRB regarding the technical soundness of any HHS IT investments requiring Departmental review.

### Service and Supply Fund Board (SSF)

The HHS Service and Supply Fund provides for consolidated operation, financing and accounting for activities involving the provision of common services and commodities to customers. SSF information technology proposals must first be reviewed by the CIO Council and receive an initial funding approval from the Department’s ITIRB, with the final funding decision to occur at the SSF Board meeting. The SSF Board of Directors (“Board”) holds quarterly meetings, is chaired by the HHS Deputy Secretary and is advised by the SSF Fund Manager and participating councils and committees. The Program Oversight Group shall bring budget and financial issues and requests to the SSF Board for review and concurrence. The Board shall review and approve the estimated revenues, costs, budgets, workload estimates and annual rates to be charged to customers by the relevant IAM@HHS program activities (e.g., issuance of PIV credentials).

## IAM@HHS Governance

The Director, Office of Secretary and Strategic Information (OSSI), Office of the Secretary is the Department’s Executive Sponsor for the IAM@HHS program and, along with the Program Oversight Group (POG), provides overall executive leadership for the program. The Director, serving as the Chairperson of the POG, will provide strategic direction by facilitating consensus decision-making among the members of the POG regarding the program’s vision, scope and business objectives.

### POG Charter

The following sections define the charter for the POG. This group’s charter defines the vision, mission, scope, responsibilities, membership, and administrative matters that govern the operation of the POG. All proposed changes to this charter, with supporting rationale, are to be submitted in writing to the IAM@HHS Executive Sponsor.

#### Vision and Mission

The POG intends to ensure the long-term success of identity and access management in the Department to advance the mission of HHS and all its OPDIVs, both separately and together. The mission of the POG is to foster collaboration among all parts of the HHS enterprise to derive the maximum benefit from existing and planned IAM capabilities and enable HHS staff access to the campuses, buildings and applications they need to do their work.

#### Scope

The POG is an advisory board that provides counsel and guidance to the IAM@HHS Program Management Team and advises the appropriate HHS Governance bodies on decisions regarding Departmental policy, strategy, funding decisions and program risks. The POG will listen to and champion the PMT’s recommendations to other Department/OPDIV governance bodies and groups as appropriate. The POG also makes decisions concerning the IAM@HHS milestones, workforce transitions, budget, scope, schedule and staffing. The POG will review program progress on a regular basis and provide input to the PMT for all major program decisions.

#### Responsibilities

The IAM@HHS POG shall:

* Ensure that the Department’s varied and unique business needs and potential impacts of the Identity and Access Management systems are conveyed to both the PMT and the HHS Governance bodies.
* Set criteria for evaluating the priority and quality of individual initiatives and managing the overall portfolio of initiatives supporting the program objectives.
* Promulgate program goals, objectives and needs to OPDIV constituencies.
* Recommend changes to Department policies relevant to identity, credential and access management as well as physical security, personnel security and cyber-security.
* Perform EPLC stage gate reviews, as required.

#### Membership

The Executive Sponsor for the IAM@HHS program shall serve as the chairperson (Chair) for the POG. The total number of POG members may change over time, but the body is envisioned to have between 12 and 15 members, of which at least seven (7) shall serve in the Executive Oversight role, at the discretion of the Chair.

Members of the IAM@HHS POG shall be OPDIV and Department resources selected by the program’s Executive Sponsor. Members shall serve in the capacity of one of two roles:

* **Executive Oversight** – Members in the Executive Oversight role shall provide advisory and consultant services to the Chair of the POG. Members in this role are only expected to vote when providing recommendations to the Chair. The Chair will seek to facilitate a consensus within the POG membership, but the Chair is responsible for making the final decision.
* **Subject Matter Expert** – The Subject Matter Expert (SME) role provides critical insight, in regard to issues dealing with business processes and those technical in nature, to POG decision makers. An example of required SME support is the EPLC state gate reviews, POG SMEs shall conduct detailed analysis of the stage deliverables and advise the Executive Oversight members. All formal stage gate reviews will be conducted by the ITIRB, with is the IT Governance body. Executive Oversight members shall make a consensus recommendation to the Chair of the POG to approve the stage deliverables and certify the completion/exit of a particular stage. IT Governance and Business Owner agree to proceed to the next phase of EPLC.

#### **Administration**

The POG shall meet regularly at a time, place and frequency set by the Chair. In addition, the POG may be convened in an emergency session to address time-critical topics as deemed necessary by the Chair.

The primary or alternative representative of each principal member is expected to attend all meetings. Attendance may be in person or any other two-way, interactive communication means, such as conference call or video teleconference, acceptable to the Chair. While the POG operates via consensus, there may be situations that require a vote. For example, the Chair may call for a vote in an effort to obtain a unified recommendation. The Chair of the POG will make decisions based on the advice of the Executive Oversight membership. A majority of the members, to include the Chair, must attend each meeting to establish a quorum for that meeting.

POG meetings shall be facilitated by a member of the PMT to ensure the efficient and effective use of all POG members’ time. The POG Facilitator shall perform the following:

* Receiving, recording, and tracking all agenda items submitted for consideration.
* Preparing the agenda, supplemental materials, and minutes for each POG meeting.
* Tracking action items from the POG meetings.
* Maintaining current and historical POG logs, distribution lists, and other records.
* Preparing routine and ad hoc reports of POG activities.
* Ensure that any proposed changes in the POG charter are documented and receive a 2/3 concurrence from the then existing POG membership prior to any proposed changes being offered to the Chair of the POG for final approval.

The PMT, with input from the program’s Senior Advisors (a representative from OSSI/Physical Security Division and the ASRT Chief Technology Officer), shall make recommendations to the Program Oversight Group (POG) on the strategic direction of the program and work with the HHS Enterprise Architecture Review Board (EARB) and the HHS ITIRB to help ensure that the program meets Departmental goals and Federal policies and regulations.

Items presented for POG consideration shall be circulated electronically for members' review far enough in advance of the meeting to allow members time to review the documents in a meaningful way. Disposition may be determined by virtual deliberation of the members without convening a POG meeting. Meeting minutes taken at each POG meeting will be reviewed and approved by the Chair and Facilitator for release to the POG members for additional comments. Identified changes and/or comments to be included will be incorporated and reviewed by the POG members. The final notes will be uploaded to the HHS Portal website.

## Program Management and Execution

The IAM@HHS Program Management Team (PMT) consists of the Program Manager (Program Management Workstream Lead), Deputy Program Manager and Leads for the following workstreams:

* Security
* Outreach and Communications
* Policy
* Budget
* Credential Management
* Identity Management
* Access Management

The PMT also includes additional HHS staff and contractors as required to support the management and coordination of all workstreams with each other. Other workstreams may be added or combined as needed. Senior Advisors from the OSSI Physical Security Division and the ASRT Chief Technology Officer are also assigned to set guidelines and advise the IAM@HHS program on Identity and Access Management implementation strategies and risks.

The PMT has primary responsibility for ensuring a successful implementation of IAM capabilities at the HHS Departmental level as well as assisting OPDIVs in their implementations. This includes both physical and logical activities related to identity and access management. The respective workstream leads for the Security (e.g. personnel, cyber and physical), Outreach, Policy, Budget, Credential Management, Identity Management and Access Management manage the day-to-day activities of their individual workstreams. The workstream leads provide the IAM@HHS PMO with critical and timely information related to the planning, development, deployment, and change control activities of their initiatives. The activities of the PMT include:

* Coordinating activities across all program workstreams to achieve overall program goals
* Demonstrating accountability and transparency of deliverables against the HHS strategic program direction
* Ensuring adherence to Enterprise Performance Life Cycle (EPLC), Enterprise Architecture (EA) guidance and requirements
* Participating in external Identity and Access Management Groups, particularly those that influence IAM activities within the Federal Government (e.g., ICAM) to ensure alignment
* Changing program priorities as necessary to align with the recommendations of the HHSIdentity Program Review Board
* Working with IAM OPDIV representatives to understand and provide assistance as needed for information or tasks relating to their identity and access management activities
* Maintaining up-to-date program information in a format accessible to IAM OPDIV representatives
* Working with the Program Oversight Group (POG) and OSSI as necessary to obtain executive approval as needed
* Convening meetings and workshops, and obtaining expert input from Subject Matter Experts (SMEs) as needed
* Drafting, maintaining and updating program documents and artifacts, including policy, and circulating documentation for approval as needed

The PMT shall also track information related to budgets and funding, and make determinations as necessary to stay within the prescribed budget. The PMT is responsible for reporting their progress and status on a regular basis to its oversight groups and the larger HHS IAM community.

A summary description of each of the program governance bodies and associated roles is provided in the table below.

Program Governance Bodies, Roles and Responsibilities Summary

| **Role** | **Description** |
| --- | --- |
| **HHS Governance** |
| **ITIRB** | Responsible for reviewing and approving EITF funds for IAM@HHS activities. |
| **SSF Board** | Responsible for reviewing and approving SSF funds for IAM@HHS activities. |
| **CIO Council** | Responsible for reviewing technical solutions that may impact the HHS enterprise (e.g., IAM@HHS capabilities) and advising the ITIRB on program investment decisions. |
| **Program Advisory Bodies** |
| **Executive Sponsor** | Responsible for providing overall program direction from both a strategic and operational perspective for IAM@HHS. Serves as the chair for the Program Oversight Group. |
| **Program Oversight Group** | IAM OPDIV representatives responsible for providing the PMT and Program Manager with strategic direction for the program. |
| **Program Management Team (staffed by HHS employees)** |
| **Program Manager** | Responsible for managing program from a strategic perspective. As Program Management Workstream Lead also responsible for providing program coordination and guidance across all IAM@HHS workstreams. |
| **Deputy Program Manager** | Responsible for managing the day-to-day operations of the program through providing program coordination and guidance across all IAM@HHS workstreams. Additionally the Deputy Program Manager will be responsible for Enterprise Architecture functions, e.g., alignment of program plans and artifacts with HHS EA program guidance and requirements, as well as other Federal initiatives. |
| **Senior Advisors** | Assigned senior advisors from OCIO and OSSI bring issues to the POG for consideration and provide strategic advice to the PMT for achieving program goals. |
| **Security Workstream Lead** | Responsible for providing guidance on cyber, personnel and physical security requirements across all IAM@HHS workstreams.  |
| **Budget Workstream Lead** | Responsible for managing, monitoring and reporting on the program budget |
| **Policy Workstream Lead** | Responsible for providing policy advocacy for the program, researching, developing or finalizing all mandates, policies, standard operating procedures, business processes, procedures and applications that help manage access to facilities and information for identity and access management. |
| **Identity Management Workstream Lead** | Responsible for acting as the Government’s primary contact for technical management of the Identity Management workstream. Also serves as the IAM@HHS contact point for all OPDIV personnel that work with identity management activities. |
| **Access Management Workstream Lead** | Responsible for acting as the Government’s primary contact for technical management of the Access Management workstream. Also serves as the IAM@HHS contact point for all OPDIV personnel that work with access management activities. |
| **Credential Management Workstream Lead** | Responsible for acting as the Government’s primary contact for technical management of the Credential Management workstream. Also serves as the IAM@HHS contact point for all OPDIV personnel that work with credential management activities. |
| **Contractor Support Roles** |
| **Outreach & Communications Workstream Lead** | Responsible for defining how the program will deliver different types of message and identifying the proposed communication vehicles, message sender, target audience and timing with respect to key program milestones for each type of message. Communicates IAM@HHS program concepts, activities, and progress to promote support for the implementation of improved identity and access management capabilities. |
| **Technical Advisor** | Responsible for providing strategic input on technical and programmatic decisions for IAM@HHS. Also acts as a liaison between the OPDIVs and IAM@HHS capability development workstreams. |
| **System Integrator Project Manager** | Coordinate with the IAM@HHS PMT on project plan(s), technical and management issues, stakeholder participation, strategic and tactical reports, performance measurements, and critical success factors |
| **System Integrator Chief Architect** | Responsible for making sure the project is aligned with the IAM@HHS project vision and is working closely with the HSPD-12 initiative |
| **System Integrator Technical Lead** | Responsible for providing technical leadership and support for the Enterprise Identity Management initiative |
| **System Integrator EIAM Lead** | Responsible for the Architecting the Single Identity concept (VIM), User Provisioning, eAuthentication, Federation, Security and Audit, Enterprise Access Control Model, and Service Registry |
| **Program Management Support** | Responsible for assisting the Program Manager and Deputy Program Manager in executing planning, communications and other programmatic activities for IAM@HHS.  |

#

# Program Charter Approvals

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Director, HHS OSSI

Executive Sponsor Date

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# IAM@HHS Program Manager Date

1. Note that for the purposes of this document, use of the term “OPDIVs” also includes STAFFDIVs. [↑](#footnote-ref-1)
2. Note that for the purposes of this document, use of the term Operating Divisions (OPDIVs) also includes Staff Divisions (STAFFDIVs). [↑](#footnote-ref-2)
3. “Personal Identity Verification Interoperability For Non-Federal Issuers”, May 2009. Page 5. <http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf> - accessed 10/8/09. [↑](#footnote-ref-3)