U.S. Department of Housing and Urban Development

Enterprise Architecture Policy

HUD Handbook 3255.1 | Version 2.0

September 2023

Policy Revision History

Version	Date	Description
3255.1	05/2014	Original
3255.1 Rev 2	10/2022	Updated
Rev 2	03/2023	Updated Format
Rev 2.	09/2023	Incorporated comments

Table of Contents

1. Introduction

Enterprise Architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. Used appropriately, the EA promotes mission success by serving as an authoritative reference, promoting functional integration and resource optimization with both internal and external service partners. Achieving the enterprise architecture objectives requires collaboration, cooperation, and coordination amongst agency business stakeholders, systems developers, partners, and technology infrastructure providers. The U.S. Department of Housing and Urban Development (HUD) Enterprise Architecture is a strategic and operational direction used to manage and align HUD's business processes and Information Technology (IT) infrastructure/solutions with overall strategy.

The Enterprise Architecture requirements implement an information technology framework and repository which defines:

- the models that specify the current ("as-is") and target ("to-be") architecture environments.
- the information necessary to perform HUD's mission, together with the solutions and technologies necessary to perform that mission.
- the processes necessary for implementing modern technologies in response to HUD's changing business needs.

Effective programs are structured with a necessary set of criteria that provide both optimal and useful results to the organizations they support in achieving the change. Straying from these criteria may lead to unexpected and value-deficit activities that render the program to be no more than organizational noise. This document describes HUD'S Enterprise Architecture Framework and provides the minimum criteria needed to structure your Department's EA program to align with the framework.

2. Purpose

This policy supports a Departmentwide Enterprise Architecture (EA) Practice for HUD. Facilitated by the Office of the Chief Information Officer (OCIO), HUD's EA establishes a corporate blueprint that connects strategic plans with individual programs and Information Technology (IT) solutions. It will guide and influence investments in a consistent, coordinated, and integrated fashion that will improve interoperability, reduce duplicative efforts, and optimize mission operations. This policy establishes the basis for tactical direction, procedures, and standards defined within the HUD EA Practice and governance documentation, the updating of which will ensure iterative realignment as changes to federal EA guidance and management directives emerge.

3. Rescission

This policy supersedes the HUD Enterprise Architecture Policy Handbook 3255.1, REV-1 dated May 2014.

4. Applicability

The Clinger-Cohen Act of 1996 mandates the implementation of an effective Enterprise Architecture policy and an associated Enterprise Architecture Practice. This act requires Federal Agency Chief Information Officers to develop, maintain, and facilitate sound and integrated IT

architecture for the agency. Subsequently, the Office of Management and Budget (OMB), in its Circular A-130, issued explicit guidance that requires agency IT investments to be consistent with the Agency's Enterprise Architecture. The E-Government Act of 2002 defines Enterprise Architecture as a strategic information asset base, which defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs, and includes a baseline architecture, a target architecture, and a sequencing plan.

5. Effective Implementation Date

This policy is effective immediately upon the date of approval. Additional resources and information about the EA Practice are available at: http://hudatwork.hud.gov/po/i/ea/resources/index.cfm.

6. Enterprise Architecture Policy

It is the policy of the Department to define, maintain, and adhere to the approved HUD EA principles, procedures, standards, reference models, and guidelines that support HUD's mission, goals, and objectives.

HUD's EA policy:

A. The Department shall develop and maintain a single department-wide EA based on the Department's mission, strategies, goals, and objectives. EA enablement and maturity shall be achieved through segment development in support of HUD programs and initiatives.

B. All HUD organizations shall comply with the principles, procedures, standards, and guidelines of the EA to support IT management, governance, and operations. This includes IT acquisitions, IT portfolio management, risk and security management, and project planning and management.

C. All HUD organizations shall support Departmental efforts to streamline business processes, improve communication with stakeholders, reduce information and capability 'stovepipes', and minimize duplication of effort, investments, systems/applications, and services through the use of HUD's EA Practice.

D. All HUD organizations shall participate in EA efforts to define and implement shared services, establish business and technical standards, and leverage technical capabilities across the Federal government, to reduce cost and maximize return-on-investments for IT products and services.

E. The HUD EA shall adopt data management best practices to ensure that HUD data are well-defined, relevant, reliable, complete, accurate, accessible, and secure, to ensure that HUD data effectively support HUD decision-making, performance improvement, information sharing and government transparency."

F. The EA Practice shall be responsible for implementing and managing EA information in a central repository, accessible to HUD and authorized personnel to support strategic and project planning, decision-making, and reuse of assets and resources across the Department.

G. The HUD EA shall integrate security and privacy considerations into all its architectural layers in compliance with Federal regulations and Departmental security

standards to mitigate and reduce risk and improve security management and operations across the Department.

H. The HUD EA shall assess all current and emerging technologies in support of HUD's business needs in a way that reduces infrastructure complexity and costs. This ensures technical interoperability and continually enhances IT service delivery, scalability, and agility.

I. The HUD EA shall comply with all Federal regulatory mandates, executive directives, and oversight requirements. It shall be consistent with the Federal Enterprise Architecture Framework and its approved reference models as prescribed by the Office of Management and Budget (OMB).

J. This HUD EA policy shall be incorporated into applicable contract language or memoranda of agreement between HUD and its IT service suppliers and contractors to define compliance directive.

K. Every HUD organization shall comply with Section 504 and Section 508 of the Rehabilitation Act. All electronic and information technology developed, procured, maintained, or used by the Department must be accessible to employees and members of the public with disabilities. All technology procured by the HUD shall be assessed, prior to purchase, to determine compliance with the accessibility standards published by the U.S. Access Board.

L. All HUD organizations shall provide reasonable accommodation for employees with disabilities in accordance with the requirements of Section 501 of the Rehabilitation Act. This includes, for example, providing an employee with a disability a different type of IT than others if needed as a reasonable accommodation - such as assistive technology, software that works more effectively with the employee's screen reader or other assistive technology, or hardware - and making exceptions or modifications to policies that may be needed because of an individual's disability.

M. HUD EA aligns with the Federal Cloud Computing Strategy, Cloud Smart, for adoption of cloud solutions. The acquisition of cloud services will be based on business, technical, and privacy considerations. The adoption of these services must be guided by the following requirements:

    1) Cloud services shall have FedRamp (Federal Risk and Authorization Management Program or equivalent certification to ensure that the level of information security will meet or exceed that of the On-Premises computing services.
    2) HUD shall maintain a list of standard solutions that include cloud solutions. HUD projects, systems and applications must employ these standard solutions or proceed through the Technical Review Subcommittee (TRC) and Configuration Change Management Board (CCMB) processes for approval of new solutions prior to acquiring and implementing non-compliant solutions.
    3) HUD shall consider integration with on-premises and cloud services, including identity and access management, networking, and storage. The Department will make decisions based on the interoperability of systems across the different platforms.
    4) Cloud services will be chosen based on the deployment models listed in the NIST SP 800-145, The NIST Definition on Cloud Computing, with the following order of preference depending on HUD's level of maturity:
        a. Software-as-a Service (SaaS)
        b. Platform as a Service (PaaS)
        c. Infrastructure as a Service (IaaS)

7. Roles and Responsibilities

HUD's Enterprise Architecture practice is a Department-wide mandate that involves the active participation of all program offices. HUD's EA is developed in a cooperative, managed and coordinated effort facilitated by the Office of the Chief Information Officer, with the participation of HUD Program Offices and technical experts from subject domains.

This HUD EA policy outlines organizational roles and responsibilities for ensuring compliance with legislative and executive level guidance on Enterprise Architecture (EA). The following describes the roles and responsibilities for organizations that contribute to the development, implementation, and the operational integration of HUD EA Practice across the Department.

A. Chief Information Officer (CIO)

The Chief Information Officer (CIO) establishes HUD's EA Practice and manages the development, implementation, and maintenance of HUD's enterprise architecture. The Office of the Chief Information Officer (OCIO) shall also create EA advisory and collaboration groups to support the OCIO and governance framework.

Responsibilities

1) Establish HUD's EA practice and appoint the Chief Architect to lead the EA practice in the development, implementation, maintenance, and usage of HUD's EA across the Department.

2) Ensure compliance with HUD EA policy, principles, procedures, standards, and guidelines, in collaboration with HUD Program Office staff, OCIO functional areas, and communities of practice.

3) Ensure availability and management of resources and training opportunities sufficient to fulfill EA responsibilities of the HUD EA practice, HUD program offices and other OCIO functional areas.

B. Chief Architect

The HUD Chief Architect leads the EA practice in developing, maintaining, governing, and evolving the Department's EA. The HUD Chief Architect manages the EA practice under authority delegated by HUD CIO. The Chief Architect establishes, plans, and directs the HUD EA practice and oversees the development,, verification, and adoption of the EA. The Chief Architect (or designee) is the HUD representative to intra- and inter-governmental advisory bodies on EA-related matters.

Responsibilities

1) Develop, maintain, and disseminate HUD's EA policy, procedures, standards, and guidelines to promulgate EA foundational principles and best practices Department-wide

2) Develop the HUD EA framework which aligns with the Federal EA (FEA) reference models, describing HUD's performance, business, data, systems, technology, and security components.

3) Ensure the integrity of HUD's enterprise architectural processes and work products, which include ensuring compliance with HUD EA requirements practice on IT investments, systems, and projects.

4) Assist business and technical managers in identifying cost-saving alternatives for existing (legacy) systems, and for new applications or systems, identifying solutions to meet business needs.

5) Ensure the integration of the HUD EA within the Department's Capital Planning and Investment Control (CPIC), IT governance, and the project planning and management (PPM) processes of the Department.

6) Collaborate with HUD acquisition managers and contracting officers to ensure that contractors and vendors are informed of their responsibilities to comply with the HUD EA, providing EA documentation as applicable.

7) Ensure the adherence to performance and compliance mandates from Government review and policy organizations, including the Government Accountability Office (GAO), OMB, and Office of the Inspector General (OIG).

C. Chief Technology Officer (CTO)

The HUD CTO leads the development and management of strategic priorities and policies to support the business program using current and emerging technologies.

Responsibilities

1) Manage the Information Technology infrastructure Library (ITIL) for service delivery in collaboration with IT Operations (IOO)

2) Establish and approve technical standards in collaboration with EA.

3) Identify and implement technical enterprise solution architectures in collaboration with EA.

4) Identify technology capabilities based on business requirements and needs in collaboration with EA and IT Operations.

D. Chief Information Security Officer (CISO)

The HUD CISO is responsible for compliance with the Federal Information Security Management Act (FISMA) and acting as the agency-wide information security liaison. The CISO and CTO will ensure appropriate guidance is developed for incorporating security into the enterprise and segment architectures.

8. Definitions

This section includes definitions associated with the terms within this policy.

Terms	Definitions
Agency	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or

	other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency.
Assessment	The testing or evaluation of security or privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Availability	Ensuring timely and reliable access to and use of information.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Controlled Unclassified Information	Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government -wide policies that adhere to Executive Order 13556 which establishes a program for managing CUI across the Executive branch to ensure compliance of CUI implementation.
External System Service	A system service that is implemented outside of the authorization boundary of the organizational system (i.e., a service that is used by, but not a part of, the organizational system) and for which the organization typically has no direct control over the application of required security and privacy controls or the assessment of security and privacy control effectiveness.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information	Information is stimuli that has meaning in some context for its receiver. Information is created when data are processed, interpreted, organized, structured, or presented to make them meaningful or useful. Information provides context for data
Information Security	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Information Technology	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, which are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
Integrity	Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
Least Privilege	The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. Examples include: a virus, worm, Trojan horse, or other code-

	based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Privacy Control	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.
Privacy Plan	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, which would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management incorporates threat and vulnerability analyses and analyses of privacy-related problems arising from information processing and considers mitigations provided by security and privacy controls planned or in place.
Risk Management	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
Security Control	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
Security Policy	A set of criteria for the provision of security services.
Sensitive Information	Sensitive information is data that must be protected from unauthorized access to safeguard the privacy and security of an individual or organization. Sensitive information could be Personally Identified Information (PII) data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers. Another type of sensitive information could be business information that includes anything that poses a risk to the organization in question if discovered by a competitor or the public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities. The last type of sensitive information is classified information that pertains to a government body and is restricted according to level of sensitivity (for example, restricted, confidential, secret, and top secret). Information is classified to protect national security.

Software	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Supply Chain	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.
System Component	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
User	Individual, or (system) process acting on behalf of an individual, authorized to access a system
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

9. Authorities and References

Federal Regulations

- **The Clinger-Cohen Act of 1996 (CCA)** requires agencies to use a disciplined Capital Planning and Investment Control (CPIC) process to acquire, use, maintain, and dispose of information assets. OMB's policy for management of federal information resources is in Circular A 130, Management of Federal Information Resources, and Section 53 of A-11. The CCA aims to improve the productivity, efficiency, and effectiveness of federal programs through improved acquisition, use, and disposal of IT resources.
- **The GPRA Modernization Act of 2010 (GPRAMA)** updates the Government Performance and Results Act of 1993 (GPRA) to establish a stronger foundation for strategic planning, performance management and budgeting in support of agency missions and priority goals. GPRAMA strengthened requirements for agencies to address performance challenges and improve management function in five areas: financial, human capital, information technology, procurement and acquisition, and real property.
- **The Government Performance and Results Act of 1993 (GPRA - 1993)** establishes the foundation for budget decision-making to achieve strategic goals to meet agency mission objectives. Instructions for preparing strategic plans, annual performance plans, and annual program performance reports are provided in Part 6 of this Circular (see Section 220).

- **The Federal Acquisition Streamlining Act of 1994, Title V (FASA V - 1994)** requires agencies to establish cost, schedule, and measurable performance goals for all major acquisition programs, and achieve, on average, 90 percent of those goals. OMB policy for performance-based management is also provided in this section. If a project falls out of tolerance (failure to meet 90 percent of cost, schedule, or performance goals), FASA gives the Agency head the authority to review and, if necessary, terminate the project.
- **The Government Paperwork Elimination Act of 1998** develops procedures for the use and acceptance of electronic signatures by executive agencies.
- **The Government Information Security Reform Act (GISRA - 2000)** focuses on the project management, implementation, and evaluation of systems security. It requires federal agencies to assess the information security control techniques of their systems. Specifically, agencies must support the cost-effective security of federal information systems by promoting security as an integral component of each Agency business operations.
- **The Federal Information Security Modernization Act (FISMA - 2014)** requires agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. OMB and the Department of Homeland Security (DHS) collaborate with interagency partners to develop the Chief Information Officer (CIO) FISMA metrics, and with IG partners to develop the IG FISMA metrics to facilitate these processes. OMB also works with the Federal privacy community to develop Senior Agency Official for Privacy (SAOP) metrics. These three sets of metrics together provide a more comprehensive picture of an agency's cybersecurity.
- **The E-Government Act of 2002 (P.L. 107-347)** requires agencies to develop performance measures for implementing E-Government. The Act also requires agencies to support Government-wide E-Government initiatives and to leverage cross-agency opportunities to further E-Government. In addition, the Act requires agencies to conduct, and submit to OMB, Privacy Impact Assessments for all new IT investments administering information in identifiable form collected from or about members of the public.
- **The Rehabilitation Act of 1973** requires access to programs and activities that are funded by Federal agencies and to Federal employment. Section 508 of the Rehabilitation Act requires that all electronic and information technology developed, procured, maintained, or used by the Department must be accessible to employees and members of the public with disabilities. The law established the U.S.Access Board.
- **NIST Special Publication 800-145** (September 2011), which defines cloud computing and the different models and implementations of cloud services.

10. OMB Regulations and Guidance Documents

- **OMB Circular A-11, Part 7** - Capital Planning Budget Reporting, Exhibits 53 and 300. The OMB Capital Programming Guide provides guidance on the principles and techniques for effective capital programming. The Capital Programming Guide integrates various Administration and statutory asset management initiatives (including GPRA, Clinger/Cohen Act, FASA, and others) into a single, integrated capital programming process to ensure that capital assets contribute to the achievement of agency strategic goals and objectives.

- **OMB Circular A-109,** Major Systems Acquisitions, establishes policies for acquiring major systems. Major systems are defined as those programs that are critical to fulfilling an Agency mission, entail the allocation of large resources, and warrant special management attention.

- **OMB Circular A-123,** Management Accountability and Control, provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.

- **OMB Circular A-127,** Financial Management Systems, prescribe policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.

- **Circular A-130**, Management of Federal Information Resources, establishes policies for the management of federal information resources to include procedural and analytical guidelines for implementing specific aspects of the circular.

- **OMB Circular A 130, Section 8b,** establishes additional requirements for enterprise architectures, planning and control of information systems and technology investments and performance management. Agencies must develop, implement, and use a capital programming process to develop their capital asset portfolio.

- **OMB Memorandum M-00-07** dated February 28, 2000, Incorporating and Funding Security in Information Security Investments, reminds agencies of OMB principles for incorporating and funding security as part of agency information technology systems and architectures an of the decision criteria that will be used to evaluate security for information systems investments.

- **Common Approach to Enterprise Architecture** dated July 2012 provides guidance on the practice and delivery of business value throughout the Executive Branch of the U.S. Federal Government. Federal law and policy require Agency leaders to develop and maintain an agency-wide enterprise architecture that integrates strategic drivers, business requirements, and technology solutions.

- **Federal Enterprise Architecture (FEA)** reference models dated January 2013 are taxonomies used to classify and inventory identified aspects of any segment. These classifications and inventories are used in the planning and design of various segment aspects. The aggregation of data through the use of these taxonomies enables enterprise architects to establish *lines of sight* between business and technology as well as identify gaps, redundancies and opportunities for organizational design and performance improvement. It comprises a framework for describing important elements of the FEA in a common and consistent way.

- **OMB Enterprise Architecture Assessment Framework (EAAF) v3.1Improving Agency Performance Using Information and Information Technology**, dated June 2009 focuses on the role of the EA to achieve target performance improvements. It also addresses other practice areas, such as strategic planning, capital planning and investment control (CPIC), and program and project management. These processes must be fully integrated with an agency, EA Practice. It prescribes the development of a results-oriented architecture within the context of the Performance Improvement

Lifecycle**.**

- **OMB FEA Practice Guidance** dated December 2006 is an OMB guidance to assist architects to develop and use segment architecture in describing the current and future state of the agency and its segments; defining the desired results for each segment; determining what resources are used for an agency's core mission areas and common or shared services, leveraging resources across the agency; and developing a transition strategy to achieve the desired results.

- **OMB 25 Point Implementation Plan to Reform Federal Information Technology Management** dated December 2010 is an action plan to deliver more value to the American taxpayer. It addresses many of the most pressing, persistent challenges of the federal government in IT management. The plan is divided into two sections: Achieving Operational Efficiency and Managing Large-Scale IT Programs Effectively. The first section outlines the steps being taken to adopt cloud solutions and leverage shared services. The second section covers the structural areas that impact the success rates of large IT programs across government.

11. Glossary

Term	Definition
Annual Select	The decision-making process within which all new, ongoing, and operational IT projects are considered for inclusion in the HUD IT investment portfolio. The select process combines rigorous technical reviews of project proposals and performance with the application of uniform portfolio selection criteria.
Community of Practice	A group of individuals who communicate because they share work practices, interests, or aims. Communication within the community of practice is facilitated though regular systems of interchange such as email, meetings, and working sessions. This process of collaboration raises the level of knowledge within the community of practice and raises the level of related resources and services across the enterprise.
Current Architecture	A dynamically updated representation of the "as-is" business, data, and IT environment. The current architecture is one of three maintained states of HUD's enterprise architecture.
Domain Team	Applies the collective knowledge and experience of its individual members, industry best practice, and other knowledge sources to define and document a specific component of HUD's enterprise architecture.
EA Core Team	The technical component of the EAPMO. Develops formal standards and manages architectural processes. The EA Core Team includes technical architects, architecture consultants and technical writers.
EA Practice	A framework of policy and process to define, implement and leverage the enterprise architecture for IT planning and investment. Established by the OCIO, HUD's EA practice facilitates the definition and approval of the enterprise architecture, and the execution and monitoring and control of the principles, guidelines and standards defined by the EA.
EAMS (Enterprise Architecture Management System)	A web-based repository used to store and access architectural information and the relationships between architectural elements.
EAMS Baseline	An official, static version of the current architecture that is established each year prior to the annual select.
EAMS Target	An official, static version of the target architecture that is established each year prior to the annual select.
Enterprise Architecture (EA)	A strategic asset base that defines the business, the information necessary to operate the business, the technologies necessary to support business operations, and the transitional processes necessary for implementing new technologies in response to the changing business needs.
Enterprise Architecture Program Management Office (EAPMO)	A dedicated team within the Office of the Chief Information Officer (OCIO) with the principal responsibility for establishing HUD's EA practice and defining the Department's enterprise architecture. The EAPMO is led by the Chief Architect.
Enterprise Data Management	A principle of HUD's Enterprise Architecture. This principle expresses that HUD's data resources should be managed as a valuable enterprise-wide asset.
Enterprise Data Management Plan	A stepwise process to implement, monitor, and review a department-wide data management practice. Each step in the plan represents a specific task

	or milestone. Major milestones include the definition of an organizational structure, framework for governance, and principles, guidelines, standards, and procedures for enterprise data management.
Enterprise Data Management Practice	An organizational framework to establish, monitor and enforce principles, guidelines, standards, and procedures for enterprise data management.
Gap Analysis	A structured process to define the differences between the current architecture and target architecture. The results of a gap analysis provide valuable input to the prioritization of IT projects and the definition of the interim target architecture.
ITIPS (Information Technology Investment Planning System)	HUD's web-based IT Investment Management System.
Information Technology (IT)	Hardware and software operated by an organization that processes information to accomplish a business function, regardless of the technology involved, whether computers, telecommunications, or others
IT Project	The defined set of activities and resources surrounding or supporting the use of information technology to address HUD's strategic and programmatic objectives, and to support managerial and administrative functions. An IT project should be described in a project plan, with articulated goals and performance objectives; cost, schedule, and technical baselines; and a clear discussion of project risks, impacts, and risk management and mitigation measures.
Interim Target Architecture	A representation of one instance of progression towards the "to be" (target) business, data, and IT environment. Official interim targets are established annually after the annual selection and are updated following quarterly control review actions. The interim target architecture is one of three maintained states of HUD's enterprise architecture.
Quarterly Control	The management of IT projects that are not yet operational, including the on-going monitoring of project performance against cost, schedule and technical baselines, and the continuous identification, management, and mitigation of project risk. Lessons learned from the control phase are fed back into the selection phase to further refine and improve the formulation and maintenance of the HUD IT Investment Portfolio.
Target Architecture	A dynamically updated representation of the "to-be" business, data, and IT environment achieved at a future time. The target architecture is one of the three maintained states of HUD's enterprise architecture.

12. Getting Help/Responsible Office

Additional resources and information about the EA Practice are available at http://hudatwork.hud.gov/po/i/ea/resources/index.cfm.

Contact information for the Enterprise Architecture program are provided at http://hudatwork.hud.gov/HUD/cio/po/i/ea/aboutus/index.