

UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

FSIS DIRECTIVE

1301.1

5/15/23

ENTERPRISE ARCHITECTURE

I. PURPOSE

A. This directive provides guidance for the Food Safety and Inspection Service (FSIS) Agency-level processes relating to Enterprise Architecture (EA). EA is a collection and contextualization of information regarding FSIS business process, applications, technologies, and data that support the FSIS program areas. This directive aligns with the USDA EA Directives ([DR3185-001](#), [DR3815-002](#), and [DR3815-003](#)) and applies to all FSIS, program areas, systems, information technology (IT) assets, employees, contractors, and others who work for, or on behalf of, FSIS and are responsible for the design, development, implementation, and oversight of information technology and/or EA.

B. This directive provides definitions and standards regarding the EA and IT data element requirements. These requirements establish the baseline guidance and definitions for the IT assets being requested, captured, modified, or stored within the Enterprise Architecture Vision Environment (EAVE). EAVE is an EA tool, which the U.S. Department of Agriculture's (USDA) Office of the Chief Information Officer (CIO) selected and implemented. This tool will serve as the certified repository for capturing EA artifacts including IT assets for decision making purposes. However, this repository will not be considered or be used as software/hardware asset management software, but it will be used to capture, modify, and display asset data through dashboards, models, and analytical reports.

C. This directive also provides the guidance on how to apply IT asset definitions found in [OMB Circular A-130](#), [NIST SP 800-37](#), and [NIST SP 800-53](#). The FSIS Office of the Chief Technology Officer (OCTO) established and approved the terms and brief definitions listed below, along with the detailed definitions listed in [Attachment 1](#), "Definitions" and the authorities for OCTO's processes found in [Attachment 2](#), "Authorities." Additionally, this directive is intended to help interpret and lend clarity to the existing NIST definitions, allowing for easier and more accurate categorization and reporting of IT assets.

1. System: An organized assembly of resources and procedures united and regulated by interactions, interdependences, financial funding, technology requirements, or other means to accomplish a set of specific business functions. Additionally, a System also means a tangible IT asset that is comprised of hardware devices, software, applications, databases, users, processes (automated and manual), and security controls. Furthermore, Systems generally receive Accreditation, Approvals to Operate (ATOs), require Architectural Design and Diagramming, and often have investment lines of funding;
2. Application: An assembly of multiple software programs used to provide at least one business capability. Typically, applications are assembled for a specific purpose to solve a need created by combining multiple smaller very specific software programs to provide a business capability. Most applications contain multiple parts and numerous steps, including related manual processes and automated processes. Applications are usually part of a single system; however,

DISTRIBUTION: Electronic

OPI: OPPD

they can be used to fulfill the needs of multiple systems. Applications typically do not receive ATO, or have separate lines of funding;

3. Software: An organized assembly of computer instructions that are typically compiled of programming code used to assist with performing a function by means of a computer or electronic device; and
4. Platform: A platform is an integrated hosting environment that systems, applications, websites, components, and data are built upon.

II. BACKGROUND

A. The information and instruction in this directive are consistent with the following Departmental Regulations (DR):

1. [DR 3185-001](#), *Enterprise Architecture*;
2. [DR 3185-002](#), *Enterprise Architecture IT Asset Definitions*; and
3. [DR 3185-003](#), *Enterprise Architecture IT Asset Data Element Requirements*

B. EA is a methodical collection of the organization's strategy plans, business documentation and information technology assets including their relationships to each other throughout the organization and is described in "Current, Transitional, and Future" state diagrams, EA reports, and EA/IT portfolios. EA is mandated by the [Clinger-Cohen Act of 1996](#) and requires Federal agencies to focus more on the results achieved through IT investments. [Federal Information Technology Acquisition Reform Act \(FITARA\)](#) requires Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) to have a significant role in IT decisions, including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions. In addition, [OMB Circular A-130](#) requires a complete inventory of the Agency information resources, including personnel, equipment, and investment funds devoted to information technology and resources management.

III. ENTERPRISE ARCHITECTURE WITHIN FSIS

A. The Enterprise Architecture Team within FSIS designs, captures, analyzes, and contextualizes information and data regarding the Agency, program areas, business operations, capabilities, gaps, roadmaps, and supporting technologies. EA supports and provides information for FSIS's IT investment and management processes and seeks to reduce unnecessary duplication of both material expenditures and efforts.

B. The Enterprise Architecture Team within FSIS is to:

1. Comply with all legislation, mandates, initiatives, and requirements at the Federal, Departmental, and Agency level, which includes but not limited to the Federal Enterprise Architecture Framework Version 2 (FEAF v2), Technology Business Management (TBM) taxonomy, and The Open Group Architecture Framework (TOGAF);
2. Align the business and operational needs, with the requirements, and priorities expressed through the [USDA Strategic Plan](#), [USDA Information Technology Strategic Plan](#), [FSIS Strategic Plan](#), and the [FSIS Information Technology Strategic Plan](#);

3. Conform to the Baseline Standards Profile as approved by the USDA Enterprise Architecture Committee (USDA EAC);
4. Incorporate capturable required security controls for all systems and applications to ensure the authorization, integrity, completeness, and accuracy of transactions;
5. Develop architectural designs and implementations that will be in alignment with EA standards;
6. Utilize existing change/configuration management process for all IT Assets (i.e., Systems, Applications, Technology, and Data);
7. Ensure organizational data is an asset that has value to the enterprise and is managed accordingly;
8. Utilize the EAVE to develop and maintain the agency, IT asset inventory and their attributes;
9. Identify legacy systems that include IT assets with an expected decommission date of less than five years;
10. Maintain legacy system classifications within EAVE (e.g., expected decommission dates, actual decommission dates and an expected decommission reason) for all applicable IT assets within FSIS;
11. Develop and maintain the FSIS application roadmap or strategy to support strategic goals and technology modernization efforts, to include modernizing legacy systems by re-architecting, rebuilding, or replacing; and
12. Provide the USDA OCIO and USDA Enterprise Architecture Division (EAD) with the most current application roadmap or strategy for inclusion into the USDA OCIO Target Architecture to facilitate effective decision-making.

IV. ROLES AND RESPONSIBILITIES

A. Under the direction of the FSIS Assistant Chief Information Officer (ACIO), the FSIS Office of the Chief Technology Officer (OCTO) oversees FSIS Enterprise Architecture responsibilities. The Enterprise Architecture team works collaboratively with the USDA EAD, OCIO, and Program Areas to provide oversight and governance on FSIS EA processes and IT assets. The following outlines the roles and responsibilities of each participant in the EA process:

B. The FSIS Assistant Chief Information Officer (ACIO) is to;

1. Serve, or designates a representative to serve, as the principal liaison with the USDA CIO;
2. Provide sufficient support to ensure the FSIS's Enterprise Architecture Team is effectively and efficiently governed;
3. Work with the USDA CIO to align Agency Capital Planning and Investment Control (CPIC) processes and procedures with USDA policies and Federal regulations and guidelines;
4. Support the implementation and usage of tools used to capture EA information;

5. Ensure that the EA program complies with applicable laws, Office of Management and Budget (OMB) policies and memorandums, USDA policies and procedures, and has an effective governance process; and
6. Ensure tight integration of FSIS's Enterprise Architecture, CPIC program management, and the IT waiver process.

C. The FSIS Chief Technology Officer (CTO) is to:

1. Ensure that EA practices, principles, and information are incorporated into IT governance, portfolio management, capital planning, investment management, and other processes related to the planning, acquisition, maintenance, end of life and disposition of information technology;
2. Address FSIS's information and IT requirements as collaborative and integrated processes, and work in concert with the USDA Enterprise Architecture Committee (EAC);
3. Disseminate artifacts and information created by FSIS's EA program;
4. Provide day-to-day management and stewardship of FSIS's EA program;
5. Ensure creation and dissemination of detailed operating procedures, policies, and other core EA artifacts that define the operation of FSIS's EA program;
6. Ensure tight integration of FSIS EA, CPIC, program management, and IT waiver processes;
7. Ensure that FSIS Classifications and Standards align with USDA and OMB EA Standards for compliance;
8. Provide management and oversight activities related to the IT asset definitions listed in this directive and develop requirements and guidance for using these definitions; and
9. Serve as Advisor on the FSIS Enterprise Architecture Review Board and signatory representative.

D. The FSIS Office of the Chief Technology Officer Enterprise Architects (OCTO - EA) is to:

1. Serve as the point of contact for all EA-related correspondence with USDA;
2. Establish new or maintain existing IT systems and application review thresholds based on criteria to include, but not limited to, cost assessment, life cycle, dependencies, technology, security risks and performance metrics;
3. Identify opportunities to utilize shared IT services;
4. Work with program managers to document and identify IT solutions that can be delivered to customers;
5. Develop plans of action and milestones that clearly describe decision making information for actions to be taken to revitalize poorly performing projects or modernization;
6. Provide EA discipline expertise, such as industry standards and federal government approved frameworks and methodologies;

7. Serve as Advisor and Representative for FSIS at the Department EA Review Boards;
8. Ensure collaboration and coordination of EA functions across agency Enterprise Architects, and the USDA EAD;
9. Ensure each IT project aligns with FSIS EA vision, principles, and standards; is consistent with agreements reached through collaborative decision-making processes; and is represented in the USDA EAVE;
10. Develop internal policies, procedures, and controls to support the EA function;
11. Ensure Enterprise Architects and decision makers share a consistent understanding of the unique requirements for each EA subject area;
12. Remain current on trends, developments, and innovations pertaining to EA-related tools, methods, and frameworks in the public and private sectors;
13. Collaborate with FSIS CIO, CTO, and program areas to establish guidance for using IT asset definitions, including updating and modifying IT asset definitions contained within this directive; and
14. Establish instructions for using IT asset definitions and develop internal controls and procedures in support of this directive.

E. FSIS program areas, system owners, business managers, employees, contractors, and others who work for, or on behalf of FSIS are to:

1. Support and maintain an effective FSIS EA program;
2. Comply with all Federal, USDA, and FSIS EA guides;
3. Assist in conducting Annual EA Portfolio reviews within the Agency;
4. Use approved USDA and FSIS tools and processes to support EA activities;
5. Incorporate EA policies, requirements, and standards into agency IT governance process;
6. Support the established FSIS EA governance framework, processes, and structure for Programs, Systems and Applications, Investments, and Technology;
7. Share information with FSIS OCTO to ensure solution architects are appropriately following FSIS EA Standards and Processes;
8. Include FSIS Enterprise Architecture Team during new project development phases and system/application modernization processes; and
9. Incorporate the IT asset definitions throughout the Agency.

V. QUESTIONS

Refer questions regarding this directive to FSIS OCTO at email address: EG-FSIS-EAB-EAWG@usda.gov.

A handwritten signature in black ink, reading "Rachel A. Edelstein". The signature is written in a cursive, flowing style.

Assistant Administrator
Office of Policy and Program Development

DEFINITIONS

Enterprise Architecture (EA) – Four key distinct definitions of EA

1. Federal Enterprise Architecture Framework (FEAF): Defines EA as – EA supports planning and decision-making through documentation and information that provides an abstracted view of an enterprise at various levels of scope and detail.
2. Federal Enterprise Architecture Framework Command Approach v2 (FEAFv2-CA): Defines EA as – A business-based framework for Governmentwide improvement developed by OMB to facilitate efforts to transform the Federal Government to one that is citizen-centered, results-oriented, and market-based. The Federal EA is constructed through a collection of interrelated “reference models” designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies. These models are defined as: Performance Reference Model, Business Reference Model, Application Reference Model, Infrastructure Reference Model, Data Reference Model, and Security Reference Model.
3. The Open Group Architecture Framework (TOGAF): is the most used framework for enterprise architecture as of 2020 that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture. TOGAF is a high-level approach to design. It is typically modeled at four levels: Business, Application, Data, and Technology. It relies heavily on modularization, standardization, and already existing, proven technologies and products.
 - a) TOGAF defines EA as – It can be used to denote both the architecture of an entire enterprise, encompassing all its information systems, and the architecture of a specific domain within the enterprise. In both cases, the architecture crosses multiple systems, and multiple functional groups with the enterprise. A good definition of "enterprise" is any collection of organizations that has a common set of goals and/or a single bottom line. In that sense, an enterprise can be a government agency, a whole corporation, a division of a corporation, a single department, or a chain of geographically distant organizations linked together by common ownership.
4. OMB, Circular A-130: Defines EA 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 process for implementing new technologies in response to changing mission needs. The EA includes baseline architecture, target architecture, and a sequencing plan. It is a framework for streamlining business processes, information flows, applications, and infrastructure to support Agency and interagency goals. An EA is the explicit description and documentation of the current and desired relationships among business and management processes and IT. It describes the “current architecture” and “target architecture” to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency or staff office wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the Mission Areas, agency, or staff office to support its current state, and act as the roadmap for transition to its target environment. These transition processes will include a Mission Area, agency, or staff office CPIC process, a Mission Area, agency, and staff office EA planning process, and a Mission Area, agency, and staff office systems life cycle methodologies. The EA

will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, and compliance with the Government Paperwork Elimination Act (GPEA, 44 U.S.C. 3504), end user satisfaction, and IT security. The Mission Area, agency, or staff office must support the EA with a complete inventory of Mission Area, agency, and staff office information resources, including personnel, equipment, and funds devoted to information resources management and IT, at an appropriate level of detail. (Source: OMB, Circular A-130)

Enterprise Architecture Vision Environment (EAVE) – Background & Definition

1. In September 2019, USDA's Office of the Chief Information Officer (CIO) selected a department-wide enterprise architectural tool. The EA tool was implemented as part of USDA Directive DR3185-003 Enterprise Architecture IT Asset Data Element Requirements. The new EA tool was named the Enterprise Architecture Vision Environment (EAVE). EAVE is a software platform that the USDA use to manage, govern, and visualize business and IT transformation details. This tool will serve as the certified repository for EA and IT assets, used to capture, modify, and display assets data through dashboards, models, and analytical reports. Also, this software allows the USDA to leverage existing Agency approved applications and technologies. In addition, the EA tool includes capabilities for importing data directly into the repository from those applications. EAVE is being used to support application rationalization processes and procedures at USDA. The Enterprise Architecture Division (EAD) team has led in the development, implementation, maintenance, and deployment of EAVE.

Approval to Operate (ATO) – Definition:

1. The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

IT Assets – Definitions:

1. System: An organized assembly of resources and procedures united and regulated by interactions, interdependences, financial funding, technology requirements, or other means to accomplish a set of specific business functions. Additionally, a System also means a tangible IT asset that is comprised of hardware devices, software, applications, databases, users, processes (automated and manual), and security controls. As additional information for clarity, Systems receive Accreditation, Approvals to Operate (ATO), require Architectural Design, and do have separate lines of funding.
 - a) Sub-System: Some complex Systems can be comprised of multiple smaller Systems, these smaller Systems that make up a larger system can be referred to as sub-systems. These sub-systems are full systems, however due to the lines of funding, accountability, business functionality, business alignment, or security requirements, means these sub-systems are incorporated and grouped under larger systems.
2. Application: An assembly of multiple software programs used to provide at least one business capability. Applications are typically built “in-house” specifically “fit for purpose”, by combining

multiple smaller software programs to provide a business capability. Most Applications contain multiple parts and numerous steps including related manual processes as well as automated processes. Applications usually reside as part of a single System, however in special cases they can be used to fulfill the needs of multiple systems. As additional information for clarity, Applications do not receive ATO, they do not require architectural diagramming, or have separate lines of funding.

- a) Application Components: Application components are the lower-level decomposition of capabilities within an application that work together to deliver a function such as, but not limited to a software package, a web service, or a web resource that encapsulates a set of related functions.
- 3. Software: An organized assembly of computer instructions that are typically compiled of programming code used to assist with performing a function by means of a computer or electronic device. Additionally, the most common forms of software are commercial off the shelf packages. This is software that can be purchased at the local electronics store or online.
- 4. Platform: A platform is an integrated software development hosting environment that systems, applications, websites, components, data, etc. are built upon.

AUTHORITIES

- The Clinger-Cohen Act of 1996, 40 United States Code (U.S.C.) Section 11101, et seq.
 - <https://www.fismacenter.com/Clinger%20Cohen.pdf>
- E-Government Act of 2002, 44 U.S.C. 3501
 - <https://www.justice.gov/opcl/e-government-act-2002>
- Federal Information Security Modernization Act of 2014 (FISMA 2014), 44 U.S.C. 2521
 - <https://www.congress.gov/bill/113th-congress/senate-bill/2521/text>
- Federal Information Technology Acquisition Reform Act (FITARA)
 - <https://www.congress.gov/bill/113th-congress/house-bill/1232>
- Government Paperwork Elimination Act (GPEA), 44 U.S.C. 3504
 - https://obamawhitehouse.archives.gov/omb/fedreg_gpea2/
- NIST, SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations
 - <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
- NIST, SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
 - <https://csrc.nist.gov/news/2014/nist-special-publication-800-53-revision-4>
- OMB, Circular A-130, Managing Information as a Strategic Resource
 - https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
- OMB, The Common Approach to Federal Enterprise Architecture
 - https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf
- OMB, Federal Enterprise Architecture Framework Version 2 (FEAF v2)
 - https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf
- Technology Business Management Council, Technology Business Management (TBM) Taxonomy
 - <https://www.nist.gov/system/files/documents/2017/05/12/doc2017financialmanagementconference-tbm.pdf>
- USDA, Baseline Standards Profile
 - <https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/opm-fitara-common-baseline-implementation-plan.pdf>
- USDA, DM 3185-001, Enterprise Architecture Procedures
 - <https://www.usda.gov/directives/dr-3185-001>
- USDA, DM 3180-001 Information Technology Standards Procedures
 - <https://www.usda.gov/directives/dm-3180-001>
- USDA, DR 3105-001, USDA Chief Information Officers Council
 - <https://www.usda.gov/directives/dr-3105-001>
- USDA, DR 3107-001, Management of USDA IT Enterprise Initiatives
 - <https://www.usda.gov/directives/dr-3107-001>
- USDA, DR 3130-010, United States Department of Agriculture Enterprise Information Technology Governance
 - <https://www.usda.gov/directives/dr-3130-010>
- USDA, DR 3130-011, Information Technology Program and Project Manager Certification Requirements
 - <https://www.usda.gov/directives/dr-3130-011>
- USDA, DR 3130-013, Information Technology Capital Planning and Investment Control
 - <https://www.usda.gov/directives/dr-3130-013>
- USDA, DR 3180-001, Information Technology Standards

- <https://www.usda.gov/directives/dr-3180-001>
- USDA, DR 3185-001 Enterprise Architecture
 - <https://www.usda.gov/directives/dr-3185-001>
- USDA, DR 3185-002 Enterprise Architecture IT Asset Definitions
 - <https://www.usda.gov/directives/dr-3185-002>
- USDA, USDA Information Technology Strategic Plan
 - https://www.usda.gov/sites/default/files/documents/usda_it_strategic_plan_final.pdf
- USDA, USDA Strategic Plan
 - <https://www.usda.gov/sites/default/files/documents/usda-fy-2022-2026-strategic-plan.pdf>
- USDA, FSIS Strategic Plan
 - <https://www.fsis.usda.gov/about-fsis/strategic-planning>