

***IPv6 Transition Guide***

**DEPARTMENT OF VETERANS AFFAIRS**

By the

**VA IPv6 Working Group**

Version History

| **Version #** | **Version Description** | **Release Date** |
| --- | --- | --- |
| 3.0 | 1. Section 1.2, Updated title of section and content entirely 2. Section 2.0, updated link for item #10, broken link 3. Section 3.1.1, FEA Framework, FEA, OMB Memo M-14-15, and FITARA guidance links Added 4. Section 3.1.2, removed obsolete link, and added FEA Framework, FEA, OMB Memo M-14-15, and FITARA guidance links 5. Section 3.2, updated broken link to FICAM Roadmap and Implementation Guidance 6. Section 4.2, updated PWS language paragraph 7. Section 5.0, updated numbered list regarding tunneling, NAT, and CGN | September 01, 2016 |
| 2.0 | 1. Section 1.0, updated paragraphs 1 and 2, and two paragraphs on following up with the mandate on page 6, removed paragraph concerning general VA information on page 6 2. Section 1.0, fixed broken link in footnote 1 3. Section 1.0, added additional timeframes on page 8 4. Section 1.0, added Sections 1.1 and 1.2 5. Section 1.3, added #3 in numbered list, added FIPS to number 4, and revised paragraph and numbered list on what “VA anticipates” 6. Section 2.0, updated broken links 7. Section 2.0 updated #10 OneVA Enterprise Technology Strategic Plan 8. Section 2.0 Added #11 VA Enterprise Roadmap and #12 IPv6 FAR Requirements 9. Section 3.1, added link to FEAF-II 10. Section 3.1.1 fixed broken link 11. Section 3.1.3, updated reference and links to OneVA EA Vision and Strategy and FY2013-2015 Enterprise Roadmap 12. Section 3.2, updated broken link 13. Section 4.0 added new language 14. Section 4.2, updated the excerpt language from the TAC Performance Work Statement Template 15. Section 6.0, updated POC listing | October, 17, 2014 |
| 1.0 | Initial Version Release | January 11, 2013 |

Contents

[1.0 INTRODUCTION 5](#_Toc460503322)

[1.1 DEFINITION OF IPV6 CAPABILITY 8](#_Toc460503323)

[1.2 SELECTING IPV6 COMPLIANT PRODUCTS AND CAPABILITIES 9](#_Toc460503324)

[1.3 CURRENT ACTIONS, PROCESSES, ACCOMPLISHMENTS, MILESTONE, ISSUES, AND PLANS TO DATE 11](#_Toc460503325)

[2.0 REFERENCE DOCUMENTS 14](#_Toc460503326)

[3.0 IPV6 STATUTORY AND REGULATORY MANDATES 14](#_Toc460503327)

[3.1 FEDERAL ENTERPRISE ARCHITECTURE 14](#_Toc460503328)

[3.1.1 INCORPORATION OF FEDERAL SEGMENT ARCHITECTURE METHODOLOGY (FSAM) COMPONENTS INTO A One-VA TO-BE DESIGN 14](#_Toc460503329)

[3.1.2 ENTERPRISE ARCHITECTURE ASSESSMENT FRAMEWORK 15](#_Toc460503330)

[3.1.3 One-VA ENTERPRISE ARCHITECTURE AND IT DASHBOARD PUBLIC LAW MANDATES 16](#_Toc460503331)

[3.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT(FICAM) 16](#_Toc460503332)

[4.0 ACQUISITION CONSIDERATIONS 17](#_Toc460503333)

[4.1 FEDERAL ACQUISITION REGULATION REFERENCES 19](#_Toc460503334)

[4.2 TECHNOLGOY ACQUISITION CENTER PERFORMANCE WORK STATEMENT TEMPLATE LANGUAGE 19](#_Toc460503335)

[5.0 GUIDELINES FOR THE SECURE DEPLOYMENT OF IPV6 20](#_Toc460503336)

[6.0 VA POINTS OF CONTACT 20](#_Toc460503337)

# INTRODUCTION

This Transition Guide is designed to aid you as you navigate through the transition to Internet Protocol Version 6 (IPv6). Background information concerning IPv6 and the Federal Government can be found at: <https://apps.fcc.gov/edocs_public/attachmatch/DOC-303870A1.pdf>

derived from a paper written by Robert Cannon, Office of Strategic Planning and Policy Analysis, Federal Communications Commission, December 2010, ***Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition.***

IPv6 is the replacement for IPv4 which is commonly known and referred to as the addressing and communication protocol for accessing systems and resources on the Internet. The Internet today is the result of ARPANET (Advanced Research Projects Agency Network) developed by ARPA (later DARPA, the D for Defense), well over thirty years ago by DoD. In fact some research was done in the 1960s. IPv5 was not skipped, but did include an experimental protocol called ST, better known as Stream Protocol, although these capabilities are now included in IPv6. IPv6 was invented by Steve Deering and Craig Mudge at Xerox PARC, and IPv6 was adopted by the Internet Engineering Task Force or IETF in 1994. In addition to supporting Multiple Protocol Label Switching (MPLS), there is enough address space for each person on earth to be assigned well over one million IP addresses each with IPv6. IPv4 & IPv6 Compared:

Internet Protocol – version 4

IPv4 possible addresses: 4,294,967,296

A text version of the number of possible IPv4 addresses: 4 billion, 294 million, 967 thousand, and 296

Internet Protocol – version 6

IPv6 possible addresses: 340,282,366,920,938,463,463,374,607,431,768,211,456

A text version of the number of possible IPv6 addresses: **340 undecillion, 282 decillion, 366 nonillion, 920 octillion, 938 septillion, 463 sextillion, 463 quintillion, 374 quadrillion, 607 trillion, 431 billion, 768 million, 211 thousand and 456**

Stated yet one other way, IPv6 can theoretically hold 2128 addresses.

**This guide contains a listing of reference documents, a listing of mandates, and detail on the implementation of the acquisition requirements with the VA Office of Acquisition Operations, Technology Acquisition Center.**

The initial IPv6 mandate can be found at: <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>

As a follow up to the mandate, the 2010 Federal CIO Memorandum can be found at:

<http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf>

The above referenced documents specify requirements which agencies must adhere to for the implementation of IPv6 capability in all relevant devices, as well as the acquisition of technologies affected. All goods, services, products, and data information exchange shall comply with VA ‘IPv6 Capable’ specifications.

The memo was issued on 2 August 2005 as: OMB Memorandum M-05-22 which in part states:

“SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies’ infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency’s IT infrastructure, beginning February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Recent reports from the Government Accountability Office (GAO) and Department of Commerce’s National Telecommunications and Information Administration (NTIA) discuss the benefits, complexity, costs, and risks organizations may encounter during the transition to IPv6. Additionally, the Department of Homeland Security’s US-CERT has recently issued an advisory of security issues concerning IPv6. You should review these reports and the advisory to familiarize yourselves with the transition issues and ensure that risks are appropriately mitigated during your transition so the benefits are fully realized. 1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1 References may be found at [*http://www.gao.gov/new.items/d05471.pdf*](http://www.gao.gov/new.items/d05471.pdf), and [*http://www.ntia.doc.gov/report/2006/technical-and-economic-assessment-internet-protocol-version-6-ipv6*](http://www.ntia.doc.gov/report/2006/technical-and-economic-assessment-internet-protocol-version-6-ipv6)*.* The IPv6 vulnerability advisory from US-CERT was distributed via the Federal CIO Council and Small Agency Council list on April 5, 2005 and may be obtained from the secure US-CERT Portal.

What must agencies do and by when?

Following the guidance in the attachments to this memorandum, agencies must take the following actions by:

November 15, 2005

* Assign an official to lead and coordinate agency planning.
* Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details);
* Begin an inventory of all other existing IP compliant devices and technologies not captured in the first inventory (see Attachment A for details); and
* Begin impact analysis to determine fiscal and operational impacts and risks of migration to IPv6 (see Attachment B for details).

February 2006

* Using the guidance issued by Chief Information Officers Council Architecture and Infrastructure Committee (see below), address each of the elements in Attachment C in your agency’s IPv6 transition plan and provide the completed IPv6 transition plan as part of the agency’s Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency’s EA submission will be forthcoming.
* Provide a progress report on the inventory and impact analysis, as part of the agency’s Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency’s EA submission will be forthcoming.

June 30, 2006

* Complete inventory of existing IP compliant devices and technologies not capture in first inventory, and
* Complete impact analysis of fiscal and operational impact and risks.

June 30, 2008

* All agency infrastructures (network backbones) must be using IPv6 2 and
* Agency networks must interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2 Meaning the network backbone is either operating a dual stack network core or it is operating in a pure IPv6 mode, i.e., IPv6-compliant and configured to carry operational IPv6 traffic.

Additional required actions ([September 28, 2010 CIO Memorandum](http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf))

September 30, 2012

* *Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6.*

September 30, 2014

* *Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6.*

Immediate & Ongoing

* *Designate an IPv6 Transition Manager and submit their name, title, and contact information to* [*IPv6@omb.eop.gov*](mailto:IPv6@omb.eop.gov)*. The IPv6 Transition Manager is to serve as the person responsible for leading the agency’s IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary.*
* *Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.*

Selecting Products and Capabilities

To avoid unnecessary costs in the future, you should, to the maximum extent practicable, ensure that all new IT procurements are IPv6 compliant. Any exceptions to the use of IPv6 require the agency’s CIO to give advance, written approval. An IPv6 compliant product or system must be able to received, process, and transmit or forward (as appropriate) IPv6 packets and should interoperate with other systems and protocols in both IPv4 and IPv6 modes of operation. Specifically, any new IP product or system developed, acquired, or produced must:

* Interoperate with both IPv6 and IPv4 systems and products,
* If not initially compliant, provide a migration path and commitment to upgrade to IPv6 for all application and product features by June 2008, and
* Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

The National Institute for Standards and Technology (NIST) will develop, as necessary, a standard to address IPv6 compliance for the Federal government. Additionally, as necessary, the General Services Administration and the Federal Acquisition Regulation Council will develop a suitable FAR amendment for use by all agencies.”

## **DEFINITION OF IPV6 CAPABILITY**

IPv6 Product Capability is defined as a product’s ability to interoperate with other IPv6 capable products on networks supporting IPv4 only, IPv6 only, or dual stack (IPv4 and IPv6). In addition, an IPv6 Capable Product meets the following criteria:

* Conforms with the latest [USGv6 Profile](http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf) requirements according to designated capability sets, if available, as defined by the expressed capabilities requirements
* Conforms with any VA approved Conformance Matrix Requirements which may be introduced as an extension of USGv6 Profile, in accordance with VA Enterprise Architecture requirements.
* Ensures product developer has IPv6 technical support available.
* For all evolving standards related to IPv6, product developer provides a commitment and/or migration path signed by the developer Vice President or equivalent, and/or Suppliers Declaration of Conformity (SDoC) which certifies product will undergo compliance testing against any related and newly introduced USGv6 test selections.

## **SELECTING IPV6 COMPLIANT PRODUCTS AND CAPABILITIES**

IPv6 Compliant Products are defined by two OMB MEMOs –

M-05-22 OMB IPv6 Original Memo August 2, 2005

<https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>

IPv6 COMPLIANT – content extraction…

“Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval. An IPv6 compliant product or system must be able to receive, process, and transmit or forward (as appropriate) IPv6 packets and should interoperate with other systems and protocols in both IPv4 and IPv6 modes of operation. Specifically, any new IP product or system developed, acquired, or produced must:

• Interoperate with both IPv6 and IPv4 systems and products,

• If not initially compliant, provide a migration path and commitment to upgrade to IPv6 for all application and product features by June 2008, and

• Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management. “

MEMORANDUM Subject: Transition to IPv6 September 28, 2010

<https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf>

This IPv6 OMB Memorandum describes:

Specific steps for agencies to expedite the operational deployment and us of IPv6

* Enable the successful deployment and expansion of key Federal information technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks;
* Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;
* Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems; and,
* Enable the Internet to continue to operate efficiently through an integrated, well-architected networking platform and accommodate the future expansion of Internet-based services.

In order to facilitate timely and effective IPv6 adoption, agencies shall:

* Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 20121;
* Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
* Designate an IPv6 Transition Manager and submit their name, title, and contact information to IPv6@omb.eop.gov by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency’s IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and,
* Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future.

Additional IPv6 Compliance – must be augmented by the accompaniment of one or more of the following deliverables as proof of conformance (depending upon the class of acquisition as defined in Section 4.0):

* SDoC indicating that a product has been tested against the minimum USGv6 profile requirements for hosts, routers, or network protection devices (NPD) by an accredited 3rd party laboratory as designated by the National Institute for Standards and Technology (NIST).
* In the event that no USGv6 test selection is available for a specific requirement, an SDoC indicating that a product has been self-tested against any extended capabilities (i.e. VA Conformance Matrix requirements.
* In the event that no USGv6 capability set has been defined for a product (i.e., IP capable medical device, Telehealth device, etc.), a letter certifying that the developer has self-tested according to conformance requirements defined by the approved VA Conformance Matrix.
* An IPv6 Letter of Commitment to upgrade and test product accordingly as IPv6 standards evolve, signed by developer vice president or equivalent.
* SDoC claiming product will be tested according to USGv6 capabilities for any related, newly introduced test specifications or major test specification version numbers, within 24 months of NIST publication.

## **CURRENT ACTIONS, PROCESSES, ACCOMPLISHMENTS, MILESTONE, ISSUES, AND PLANS TO DATE**

1. Milestones for VA have been established and critical tasks identified to accomplish each combined with a responsible workgroup or individual assigned.
2. The VA achieved IPv6 capability across the VA backbone in March 2008.
3. The VA achieved IPv6 capability for public facing services in early 2012.
4. VA must adjust and adapt to organizational structure change as well as redesign and development in VA with VistA, MyHealtheVet, Composite Health Care System (CHCS), among others.VA must ensure migration to the IPv6 environment in VA uses a methodical, practical and tested phased approach, which strictly adhere to FISMA, Federal Information Processing Standards (FIPS), HIPAA and all other related compliance directives governing data & information security.
5. VA must apply Schedules, Tasks and Measures logically in each Phase and provide evidence that each milestone has been accomplished.
6. VA must ensure migration/transition of implementing IPv6 is transparent to users, scalable, mobile and seamless, and that there is NO instance of Denial of Service or denial of access by authorized users.

IPv6 provides a variety of increased features and capabilities over that of IPv4. Over a period of time, this expanded optimization can be achieved with less effort than now.

Security alone could be reason enough for transition, as IPv6 provides the potential for much greater security, notably Authentication and Privacy.

As previously stated, there are also numerous related areas of compliance required with directives such as: FISMA (Federal Information Security Management Act), HSPD-12 (Homeland Security Presidential Directive-12 / intended as a standard to enhance security in providing “Secure and reliable forms of identification”), and HAIPE (High Assurance Internet Protocol Encryptor), based on IPsec. All of which, can be more easily implemented and incorporated with IPv6, or can be an embedded function.

The benefits of the IPv6 environment to VA will be exploited (although with ensured Information Assurance (IA) security) with development of new techniques, products, and even services, although as stated, the transition to IPv6 replacing IPv4 will be in a gradual, measured, and seamless manner, and completely transparent to the end user above all.

In VA, all plans and efforts have been, are, and will be made with full consideration that life and limb depend upon data and information availability in a timely and also in a secure manner to include both internal and external health data and information exchange.

Also, over time, there will be benefits which directly result from implementing IPv6 in the way of simplified and automatic addressing, greater security, and simplified access connection that is verified in the scope of information assurance. The integrated management of non-medical systems and devices is also expected to provide savings of time and effort for heating systems, cooling systems, lighting systems, and other feature possibilities using smart building technology.

Many benefits with IPv6 enhance features and expanded functionality will result from the communications or transport delivery methods transitions to a Unified Communications infrastructure, including:

1. Routing will be easier to manage, yet be more secure.
2. More forms of mobile computing and access will be possible, some now known, and others not yet developed.
3. The added protocol suite will enable many sensor devices to notify as well as provide a means to manage or respond to events or circumstance remotely.
4. The expansion of WiFi and WiMax has just begun. Future wireless access can be thought of much the same as plug-n-play of the past. The difference will be that a physical connection will not be necessary, and also user authentication and information access will be an embedded automatic function, combined with automatic configuration, and with automatic IP number assignment.

A new dual-stack IPv4 IPv6 environment will provide a basic benefit in that no transmission protocol layer will have a dependency, which now exists with IPv4 alone.

With integration and convergence, video transmission will become standard IP capable and provide the ability for desktop-to-desktop video conferencing.

Also, an eventual investment savings should be realized, with reduced operation expense and costs avoidance by reduced duplication of systems purchased and maintained.

And there will be real-time capability for combining, voice, data, in day to day use with devices, services, and products.

VA anticipates a predominantly dual stack environment:

1. On an exception basis, tunneling 6 to 4 & 4 to 6 may initially be required, although this is a second choice to dual-stack (DSTM) since it cannot be as secure with deep packet inspection. Security measures (and hardening) must be implemented with tunneling in all cases of transmitted data or information
2. Tunneling will be superseded by a Predominate Dual-Stack IPv4/IPv6 mode node environment for the foreseeable future; although all new systems produced, purchased or obtained now require IPv6 addressing, due to the non-existence of IPv4 available addressing space.

Additionally, because IPv4 and IPv6 are not compatible, it is essential that VA migrate to and toward IPv6 native communication transmission using a viable replacement plan for all legacy and stove-pipe IT systems, while maintaining the ability to receive and transmit IPv4 whenever use of IPv4 for critical information is still required.

The continued oversight and management of IPv6 by the VA IPv6 Transition Office is key for success, by monitoring, assisting and measuring continued progress. Major effort and work is underway to provide a comprehensive IPv6 Training opportunity, combined with a VA wide IPv6 Communication Plan that is planned for 2013 to include consideration of:

1. Strengths
   1. Highly knowledgeable and capable VA National & Regional Network Personnel.
2. Weaknesses
   1. Lack of knowledge and/or limited impact awareness for a fully migrated IPv6 network environment across the VA.
3. Common elements of any transition to IPv6 will play a part in VA migration and some areas of focus will require extensive consideration, such as:
   1. Acquisition of requisite Training and corresponding Certification by specialty for staff. Sites’ Certification and Accreditation, Systems-Certification.
   2. Acquisition of IPv6-enabled Services will likely be required in VA throughout migration to IPv6.
   3. Hardware, Software, Services, and Support Maintenance are now in planning stages.
   4. A strong Awareness Campaign and a thorough Training Plan, which incorporate a train-the-trainer approach & just-in-time training, will be used, and is believed to be a tool for gaining the most in VA, as well as sustaining continuity with core IPv6 knowledge.

# REFERENCE DOCUMENTS

The following documentation can be found at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>

or at the indicated link below.

1. VPN IPv6 Implementation Plan Final.pdf (8 MB)
2. IPv6 Compliance Test Capability Draft 2-23-12 PDF.pdf (3 MB)
3. IPv6 Applications Test Plan Best Practices-Draft.pdf (1 MB)
4. OMB 2010 IPv6 memo.pdf (297 KB)
5. Signed VA IPv6 Memo.pdf (28 KB)
6. Common\_Approach\_to\_Federal\_EA.pdf (2 MB)
7. OMB 2005 M-05-22 IPv6 Memo
8. NIST Special Publications (800 Series)

http://csrc.nist.gov/publications/PubsSPs.html

1. VA Technical Reference Model (TRM), <http://www.va.gov/trm/TRMHomePage.asp>
2. OneVA Enterprise Technology Strategic Plan Version 1.0 <http://www.ea.oit.va.gov/EAOIT/docs/Enterprise-Technology-Strategic-Plan-FY17-21_Final.pdf>
3. Department of Veterans Affairs FY 2013-2015 Enterprise Roadmap, <http://www.ea.oit.va.gov/docs/VA_Enterprise_Roadmap_2_FINAL_20140409.pdf>
4. IPv6 FAR Requirements

# IPV6 STATUTORY AND REGULATORY MANDATES

## FEDERAL ENTERPRISE ARCHITECTURE

FEA is now referred to as the Federal Enterprise Architecture Framework-II

(FEAF-II). IPv6 Transition remains a major element of the FEAF-II. Federal Enterprise Architecture information can be found at: <http://www.whitehouse.gov/omb/e-gov/fea>

The “Common Approach to Federal Enterprise Architecture” can be found at the above site, or directly at <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf>. The FEAF-II can be found at <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf>.

### INCORPORATION OF FEDERAL SEGMENT ARCHITECTURE METHODOLOGY (FSAM) COMPONENTS INTO A One-VA TO-BE DESIGN

Federal Segment Architecture Methodology (FSAM) can be found at:

<http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/prod01_007706.pdf>.

Mandatory IPv6 compliance is contained in the following:

1. Federal Enterprise Architecture Framework Version 2 January 29 2013
   1. [Federal Enterprise Architecture Framework version 2](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf) (January 29, 2013) (.PDF, 9.3 mb)
      1. THE FEDERAL ENTERPRISE ARCHITECTURE CONSIST OF:
      2. Six Basic Model Framework Element
      3. PRM  Performance Reference Model
      4. BRM  Business Reference Model
      5. DRM  Data Reference Model
      6. ARM  Application Reference Model
      7. IRM Infrastructure Reference Model
      8. SRM Security Reference Model
2. Federal Enterprise Architecture May 2, 2012
   1. [The Common Approach to Federal Enterprise Architecture](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf) (May 2, 2012) (.PDF, 1.9 mb)
      1. THE FEDERAL ENTERPRISE ARCHITECTURE CONSIST OF:
         1. Six Basic Model Framework Element
         2. PRM  Performance Reference Model
         3. BRM  Business Reference Model
         4. DRM  Data Reference Model
         5. ARM  Application Reference Model
         6. IRM Infrastructure Reference Model
         7. SRM Security Reference Model
3. Guidance for the Federal Information Technology Acquisition Reform Act (FITARA) and related information technology (IT) management practices.
   1. Office of Management and Budget (OMB) Memorandum M-15-14, June 10, 2015, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>
   2. A New Foundation for Technology Management , June 10, 2015, <https://www.whitehouse.gov/blog/2015/06/10/new-foundation-technology-management>
   3. Management and Oversight of Federal Information Technology, <https://management.cio.gov/>

### ENTERPRISE ARCHITECTURE ASSESSMENT FRAMEWORK

**Federal Enterprise Architecture Framework Version 2 January 29 2013:**

[Federal Enterprise Architecture Framework version 2](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf)  (January 29, 2013) (.PDF, 9.3 mb)

**Federal Enterprise Architecture May 2, 2012:**

[The Common Approach to Federal Enterprise Architecture](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf) (May 2, 2012) (.PDF, 1.9 mb)

**Federal Information Technology Acquisition Reform Act (FITARA) and related information technology (IT) management practices:**

Office of Management and Budget (OMB) Memorandum M-15-14, June 10, 2015, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>

A New Foundation for Technology Management, June 10, 2015, <https://www.whitehouse.gov/blog/2015/06/10/new-foundation-technology-management>

Management and Oversight of Federal Information Technology, <https://management.cio.gov/>

### **One-VA ENTERPRISE ARCHITECTURE AND IT DASHBOARD PUBLIC LAW MANDATES**

The OneVA EA Vision and Strategy and the Department of Veterans Affairs FY2013-2015 Enterprise Roadmap, from the Office of Information and Technology (OI&T) can be found at:

<http://vaww.ea.oit.va.gov/wp-content/uploads/2013/12/OneVAEAVisionandStrategy092920131.pdf> and <http://vaww.ea.oit.va.gov/wp-content/uploads/2014/04/VA_Enterprise-Roadmap_2_FINAL_20140409.pdf>.

Office of E-Government & Information Technology

<http://www.whitehouse.gov/omb/e-gov>

IT Dashboard

<http://www.itdashboard.gov/>

## FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The FICAM Roadmap and Implementation Guidance Document can be found directly at:

<https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNNBAA4&field=File__Body__s>

# ACQUISITION CONSIDERATIONS

As mentioned in Section 1 above, the OMB Mandate M-05-22 and subsequent CIO Memorandum dated September 28, 2010 indicate the requirement for agencies to: “*Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.“*

The [USGv6 Testing Program User’s Guide (NIST SP 500-281)](http://www.nist.gov/itl/antd/upload/NIST-SP-500-281-v1-0.pdf), page 16, describes the following relationship between the acquisition of networked IT devices and claims of product compliance: “*USG agencies seeking to buy products with USGv6-compliant capabilities are advised to require the submission of the Supplier’s Declaration of Conformity (SDOC) as documentation of compliance to requirements.*”

It is important to understand that the USGv6 Profile managed by NIST provides specifications for three device types in the profile: Hosts, Routers and Network Protection Devices. Furthermore, as indicated by NIST SP 500-267 “A Profile for IPv6 in the U.S. Government”, the USGv6 Profile is meant to “*assist agencies in the development of more specific acquisition and deployment plans*”. It also states that the USGv6 Profile is meant to “*define minimal mandatory IPv6 capabilities*”. Therefore, conditional specifications indicated in the profile are not intended to serve as a blanket requirement for all host, router, network protection devices; and furthermore, node requirements outlined in the profile should be reviewed by agencies, according to individual Enterprise Architecture, network, and system requirements.

The USGv6 Profile, referenced by the following FAR regulations, states: “*It is fully expected that agencies will further augment and/or modify these specifications to meet their own requirements when making IT system specifications and policies. To assist in such a process, this profile defines a number of configuration options that a user (e.g., acquisition authority) must specify to fully articulate the IPv6 capability requirements of specific procurements.*”

USGv6 Interoperability Testing Laboratories (IOLs) that have been certified to test vendor products test for conformance and interoperability, test only, and any SDOCs provided as proof of IPv6 compliance should not be mistaken as certification of regression, security, stress, integration or other generally required testing capabilities.

The following excerpt is from the [NIST USGv6 Buyer’s Guide](http://www-x.antd.nist.gov/usgv6/BuyersGuide.html), and helps by categorizing the above in terms of “Default Acquisitions” and “Expressed Acquisitions” for clarification:

*Default Acquisition: request for host, router, network protection product capability as recommended by NIST default capabilities checklist.*

*The buyer should point to the recommended Host OR Router OR Network Protection capabilities as published in the checklist, which originates in NIST SP 500-267 the USGv6 profile. The documentation accompanying the acquired product must include a "Suppliers Declaration of Conformity": this is a document summarizing the capability support of the product and the testing it has undergone. For a default acquisition, the vendor's completed SDOC must match the capabilities of the appropriate category specified in the default capabilities.*

*When the purchase is conducted through the Acquisition department, the RFP asks for bids that include the vendors Suppliers Declaration of Conformity (SDOC), so these can be compared against each other to the extent that the IPv6 technical information is material to the buy. Buyers will receive an SDOC for each vendor response, in the case of a competitive bid, or the winning SDOC in case of a pre-qualified bid.*

*In some Agencies "small" purchases may not need a priori sign-off by Acquisition, and the purchaser or purchaser's agent have authority to buy particular items direct. The buyer goes to the supplier for his tablet or laptop or operating system DVD. An SDOC may be supplied, and the buyer may read the information presented on it. In these cases it is more crucial that the Agency CIO has published policy on what equipment can and cannot be attached to the Agency network. All buyers are urged to review and heed that policy.*

*It seems most likely that buyers with least knowledge of network infrastructure will be interested only in buying simple host systems to plug directly to the network. Buyers who have a need to articulate more sophisticated capabilities, and particularly buyers who need to buy routers will be more aware of IPv6 capabilities and their uses, and these people will be better equipped to extend the capabilities checklist with their additional architectural requirements.*

*Expressed Acquisition: complex IT requirement, where architecture requires additional features such as; specific routing algorithms or DNS services/intrusion detection capabilities.*

*The more elaborate cases of IT equipment acquisition including USGv6 involve large infrastructure buys, or blanket purchase agreements. Even before contacting the acquisition department, the buyer develops a network design in accordance with Agency enterprise architecture, and this includes the requirements for USGv6 capabilities for one or more, perhaps many, computer systems. For example, some hosts will need DNS client capabilities, some routers will need internal or external routing capabilities, one or more nodes will need DNS server capabilities. All these are additional to the defaults, and need to be expressed in the capabilities checklist. The buyer works with the Agency acquisition department to communicate the equipment and capabilities requirements for the fully architected solution. Bids are tendered, with SDOCs included in the documents, and these are compared against the expressed capabilities, as one component of the evaluation.*

## FEDERAL ACQUISITION REGULATION REFERENCES

The FAR has four specific part changes stemming from Public Law regarding IPv6, which were put in place December 2011 at: <http://edocket.access.gpo.gov/2009/E9-28931.htm>. These requirements have been met through the Performance Work Statement (PWS) template language and the Acquisition Plan template language.

* 1. FAR Part 7.105(b)(4)(iii)  Contents of Written Acquisition Plans – Acquisition Considerations for Information Technology using Internet Protocol <https://www.acquisition.gov/far/html/Subpart%207_1.html>
  2. FAR Part 11.002 (g)  Include appropriate IPv6 standards in agency acquisitions, <https://www.acquisition.gov/far/html/Subpart%2011_1.html>
  3. FAR Part 12.202(e) Special Requirements for the Acquisition of Commercial Items, Information Technology using Internet Protocol <https://www.acquisition.gov/far/current/html/Subpart%2012_2.html>
  4. FAR Part 39.101(e) Acquisition policies and procedures for acquiring Information Technology using Internet Protocol, <https://www.acquisition.gov/far/html/Subpart%2039_1.html>

## **TECHNOLGOY ACQUISITION CENTER PERFORMANCE WORK STATEMENT TEMPLATE LANGUAGE**

To implement the changes to the FAR (reference 4.1 above), the Technology Acquisition Center (TAC) updated the Acquisition Plan template to include the IPv6 requirements. In addition, the IPv6 IPT and the TAC developed the following template language that shall be used in all PWS documents. Always go to the VOA website to download the latest Acquisition Plan and PWS templates to ensure you are using the most recent guidance.

**Excerpt from the TAC *Performance Work Statement Template, October 2014:***

***(The requiring activity must obtain a signed waiver from the VA OIT CIO office if the following IPv6 requirement cannot be met due to patient safety, patient care, or other exception. If a signed waiver is obtained, the following IPv6 language can be removed from the PWS.)***

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 (<http://www-x.antd.nist.gov/usgv6/index.html>), the Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>), and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack IPv6 IPv4 connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) shall support native IPv6 and/or dual stack IPv6 IPv4 users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack IPv6 IPv4 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

# GUIDELINES FOR THE SECURE DEPLOYMENT OF IPV6

Information Security must be sustained at the same current level or greater, using a “do no harm” philosophy consistent with OMB Memorandum M-05-22, August 2005. NIST SP 800-119, Guidelines for the Secure Deployment of IPv6, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf>, addresses security impacts of IPv6 features, provides a survey of mechanisms that can be used for the deployment of IPv6, and a suggested deployment strategy. Specific highlights are:

1. Tunneling breaks the security model, as specified in the SP 800-119
2. Network Address Translation (NAT), including Carrier Grade NAT (CGN), breaks the security model
3. Just as important – NAT and/or CGN prohibits full IPv6 implementation

# VA POINTS OF CONTACT

1. [Robert](mailto:Robert) Green Robert.green@va.gov
2. Wes Crum [wes.crum2@va.gov](mailto:wes.crum2@va.gov)
3. Derrick Evans [derrick.evans@va.gov](mailto:derrick.evans@va.gov)
4. John Deltognoarmanasco [john.deltognoarmanasco@va.gov](mailto:john.deltognoarmanasco@va.gov)
5. Toni Toomer [toni.toomer@va.gov](mailto:toni.toomer@va.gov)