18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Sponsored by:

Department of Veterans Affairs

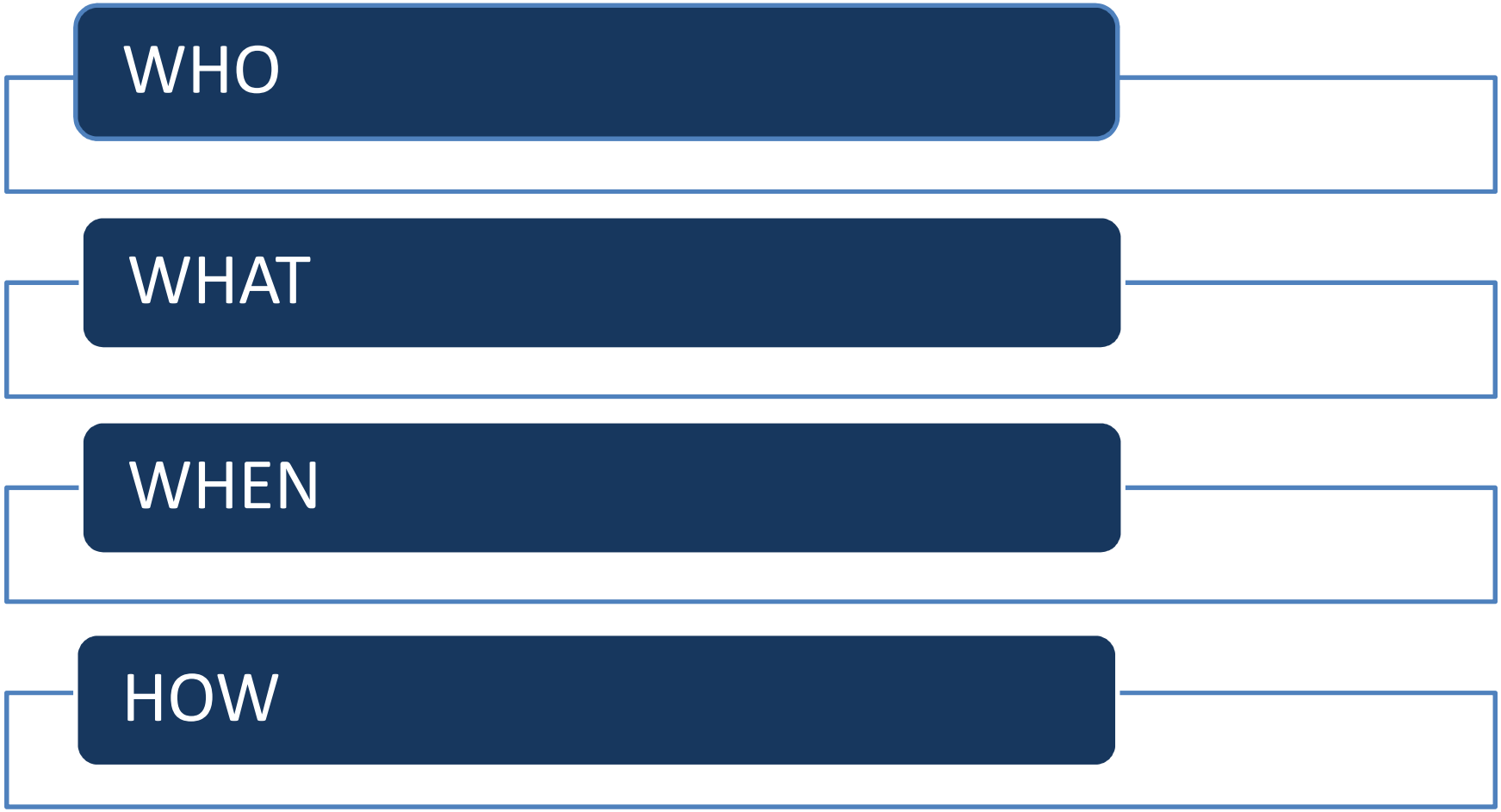
IPv6 Steering Committee

Mr. Steve Pirzchalski, Chair & Department Lead

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Federal Government OMB IPv6 Mandate M-05-22



18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Part 1

Methodology and Approach aligned with:

- VA Core Mission
- VA Major Initiatives
- VA Five Year Strategic Plan
- VA Primary Goals & Objectives
- Government Major Initiatives
- IT Reform 25 Point Plan
- Federal Enterprise Architecture FEA & Federal Transition Framework FTF
- IT Dashboard
- FISMA, FISCAM, RMF, FSAM and Fiscal Year Budget Cycle Funding
- IPv6 dual stack – communication plan, integration, and deployment
- IPv4 and IPv6 are not compatible – design must be implemented accordingly

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Part 1 – Continued

- Incorporate FSAM components into OneVA To-Be design
  - PRM Performance Reference Model
  - BRM Business Reference Model
  - SRM Service Component Reference Model
  - DRM Data Reference Model
  - TRM Technology Reference Model
- Continue Certifications
  - Sites
  - System
  - Staff
- Obtain and provide up to date IPv6 Training
- Insure all acquisition adhere to statutory and Federal Acquisition Regulation changes
  - FAR Part 7.105 Contents of Written Acquisition Plans – Technical, Business…
  - FAR Part 11.002(g) Include appropriate IPv6 Standards – define how & where…
  - FAR Part 12.202 Special requirements – acquisition of commercial items…
  - FAR Part 39.101 Foster sustainable technology – strengthen energy, transportation.

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Federal Government OMB IPv6 specific objectives for agencies - December 2011

- 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 efficient through and integrated, well-architected networking platform and accommodate the future expansion of Internet-based services.

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Federal Government OMB IPv6 compliance directives - December 2011

- 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 **2012** ;
- 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.

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Federal Task Force definition for 2012:

The intent of the FY 2012 requirement is to ensure that any and all networked services that agencies provide to the general public over the Internet are seamlessly accessible via both IPv6 and IPv4. That is, a service that is both accessible external to the agency (i.e., over the Internet) and accessible to general public users.

Internal services (i.e., accessible only within an agency enterprise or intra-net) and external services that are only accessible to sites/users employing virtual private network (VPN) technologies, or to closed user groups (e.g., requiring an out-of-band establishment of a login account) are not in scope of the FY 2012 requirement.

In summary, if there is a USG provided network service that is currently available to all users of the public Internet, that service must be available to a user who only has IPv6 capabilities.

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

VA Expounded Compliance – FY 2012

We believe the intent of the FY 2012 requirement is to securely and seamlessly provide external access for both IPv6 and IPv4 to any and all networked services that the Department of Veterans Affairs now provides to the general public over the current internet with external connection and we have opted implementing dual stack IT infrastructure.

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 **2012** ;

Interagency IPv6 Meeting

Federal Task Force definition for 2014:

The intent of the 2014 requirement is to ensure that public IPv6-enabled network services that are provided external to an agency, are accessible to USG users residing in their agency enterprise networks. The definitions of what is meant by "public" are the same. That is, in this case, the same service that an USG client/application is trying to access, is available to everyone on the Internet. The agency clients applications, host operating systems, and supporting networking infrastructure should be IPv6-enabled such that it is possible to establish native IPv6 end-to-end communication between client application and the external IPv6-enabled public server/service.

Typical examples of client applications that access public Internet servers/services include external web (browsers), email (mail user agents), DNS (resolvers), and their host operating systems. Messaging and social media applications that access publicly available network servers are also within scope.

In summary, if there is an IPv6-enabled external network service that is currently available to all users of the public Internet, that service must be available to an Agency network user who only has IPv6 capabilities. Of course, this requirement does not override agency policies that might restrict employee access to such services. But if such a service is permissible to access using IPv4, it must be possible to access the same service using IPv6.

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

VA Expounded Compliance – FY 2014

We believe the intent of the FY 2014 requirement is to securely, seamlessly and transparently provide internet access for both IPv6 and IPv4 to any and all external networked services that the Department of Veterans Affairs is to provide to the general public and for VA internally by establishing native IPv6 end-to-end communication between client application and the IPv6-enabled public services including:

- **Agency applications**
- **Host operating systems**
- **Supporting networking infrastructure**
- **Public facing servers**
- **Support of both IPv4 and IPv6**

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**;

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Part 2

Preparing IPv6 Deployment aligned with FEA, FTF, FSAM, FISMA, FISCAM, CRISP

- VA two primary component concurrent approach
  - Core Departmental IT Infrastructure
  - Major System & Program design, integration and implementation

- Structure IPv6 address allocation using the developed schema
  - VA developed IPv6 schema based on ARIN allocation of: /24
  - Set-aside /20 address allocation space before or after

- Plan and coordinate a non-IT IPv6 implementation plan
  - Supply
  - Equipment
  - Utilities
  - Floor Space
  - Other items, products and services not previously considered

18 & 19 April 2012 Charleston South Carolina

Interagency IPv6 Meeting

Part 3

Integrated Internet Access

- POA&M Plan of Action & Milestones
  - Methodical, Monitored and Measured Progress
- IPAM IP Address Management – IPal Tool with IPv6 address allocation
- Assessment - Continual built-in RMP Risk Management Process including VA CRISP
- Phased Deployment Transition – Realistic approach that is manageable
- Training – Utilizing both: Just-in-Time & Train-the-Trainer
- Non-IT Aspects
- Integrated Services Oriented Infrastructure Maturing – Infrastructure-as-a-Service IaaS
- Continued Focus on Benefits of Functions and Feature with IPv6 – Exploit where possible
  - Integrated Security/Fire/Storm Alert/Remote Utility Management
    - Vivint, Comcast, ADT Verizon, Charter
  - Integrated Internet Cloud Based services
    - SmartGrid Technology – IP based access for home, business, government
    - Multicast and Anycast
  - IPv6 Video Conferencing, RFID, Sensor & Embedded Technology, Supply, Inventory