DFC

U.S. International
Development
Finance Corporation

Office of Information Technology (OIT)

DFC Internet Protocol Policy IPV6

February 2, 2023

Document History

Version Number	Release Date	Summary of Changes	Section/ Page	Changes Made By
1	2/2/2023	Initial draft	All	PGD Team

Approval

This policy has been approved and issued under the authority granted to the Vice President & Chief Information Officer, Office of Information Technology (OIT) in accordance with DFC Office Function Directives-IT, Directive OD-13 Other Internal Rules, Handbooks, Template; and the Federal Information Security Modernization Act (FISMA) of 2014.

TINA DONBECK

Digitally signed by TINA DONBECK
Date: 2023.02.08 15:28:43 -05'00'

Chief Information Officer (CIO)

Date

Review policy/procedure by: February 2024

Table of Contents

SCOPE

This policy defines agency efforts to be compliant with federal guidance for IPv6.

OVERVIEW

Beginning in 2005, the Federal government began an initiative that served as a catalyst to commercial development and adoption of Internet Protocol Version 6 (IPv6). Designed to replace IPv4, which has been in use since 1983, these protocols are globally unique numeric identifiers necessary to distinguish individual entities that communicate over the Internet.

AUTHORITIES

The regulatory authorities include:

a. OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), November 19, 2020
b. OMB Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6), August 2, 2005 (rescinded by M-21-07)
c. OMB Memorandum dated September 28, 2010, Transition to IPv6
d. OMB Circular A-130, Managing Information as a Strategic Resource
e. Federal Acquisition Regulation; FAR Case 2005-041, Internet Protocol Version 6 (IPv6)

ROLES AND RESPONSIBILITIES

The memorandum identifies clear activities agencies must conduct with indication of roles required to take action.

a. The **Chief Information Officer (CIO)** in the Office of Information Technology (OIT) will develop this policy and incorporate required language. The CIO is responsible for establishing an agency-wide integrated project team (including acquisitions, and IT technical members). This team will be required to govern and enforce IPv6 efforts.
b. The **Chief Information Security Officer (CISO)** is responsible for privacy incident response and incident reporting.
c. The **Vice President of the Office of External Affairs (OEA)** is responsible for providing

assistance in publishing this policy on the public website.

d. The **Vice President of the Office of Administration (OA)** is responsible for providing assistance in ensuring IT acquisitions adhere to IPV6 standard on all new IT Acquisitions starting in FY23.

ENTERPRISE POLICIES

Network information systems

By the end of Fiscal Year (FY) 2023, all new networked Federal information systems will be IPv6-enabled at the time of deployment. The agency's strategic intent is to phase out the use of all IPv4 systems.

External Partner

As DFC interacts with external partners, we will work to encourage migration to IPv6 for all network interfaces.

Public/External Facing Systems/Server

DFC has an active project in flight (as of 2/2/2023) to complete upgrading all public/external facing servers and services, and internal client applications that communicate with public Internet services and supporting enterprise networks to operationally use native IPv6.

FAR Compliance

DFC shall follow all guidance in the FAR regarding future acquisitions of networked information technology with IPv6 requirements. DFC shall:

a. Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements document must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of confidence defined in the USGv6 Test Program.

b. Continue to use the USGv6 Profile to define agency or acquisition specific requirements for IPv6 capabilities when purchasing networked information technology and services. Going forward, this should include specifying the requirement for hardware and software to be capable of operating in an IPv6-only environment.

c. Continue to require potential vendors to document compliance with such IPv6 requirement statements through the USGv6 Test Program.
d. In rare circumstances where requiring demonstrated IPv6 capabilities would pose undue burden on an acquisition action, provide a process for agency Chief Information Officers to waive this requirement on a case-by-case basis. In such cases, the purchasing agency shall request documentation from vendors detailing explicit plans (e.g., timelines) to incorporate IPv6 capabilities to their offerings.

IT Security

DFC will follow best practices in securing networked information technology utilizing IPv6. DFC shall:

e. Ensure that plans for full support for production IPv6 services are included in IT security plans, architectures, and acquisitions.
f. Ensure that all systems that support network operations or enterprise security services are IPv6- capable and can operate in IPv6-only environments.
g. Follow applicable Federal guidance and leverage industry best practices, as appropriate, for the secure deployment and operation of IPv6 networks.
h. Ensure that all security and privacy policy assessment, authorization, and monitoring processes fully address the production use of IPv6 in Federal information systems.