United States Government Accountability Office

Report to Congressional Committees

June 2020

INTERNET PROTOCOL VERSION 6

DOD Needs to Improve Transition Planning

GAO Highlights

Highlights of GAO-20-402, a report to congressional committees

June 2020

INTERNET PROTOCOL VERSION 6

DOD Needs to Improve Transition Planning

Why GAO Did This Study

An internet protocol provides the addressing mechanism that defines how and where information moves across interconnected networks. Increased use of the internet has exhausted available IPv4 address space, spurring the adoption of its successor protocol, IPv6. OMB has required that agencies plan for transitioning from IPv4 to IPv6.

Senate and House reports accompanying the 2020 National Defense Authorization Act included provisions for GAO to review DOD's IPv6 transition planning efforts. This report (1) identifies past DOD attempts to transition to IPv6, (2) examines the extent to which DOD has completed OMB's planning requirements for its current transition effort, and (3) identifies DOD's progress in completing its own IPv6 transition activities. To do so, GAO assessed DOD's IPv6 transition plans and documentation against OMB's requirements, reviewed DOD's planned IPv6 transition activities, and interviewed agency officials.

What GAO Recommends

GAO is making three recommendations to DOD to develop an inventory of IP compliant devices, an estimate of the IPv6 transition costs, and an analysis of IPv6 transition risk. DOD agreed with the recommendations to develop a cost estimate and risk analysis, but disagreed with the recommendation to develop an inventory of IP-compliant devices. Nevertheless, GAO believes the recommendation to develop an inventory is warranted.

View GAO-20-402. For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

The Department of Defense's (DOD) current initiative to transition to Internet Protocol version 6 (IPv6), which began in April 2017, follows at least two prior attempts to implement IPv6 that were halted by DOD. In one effort that began in approximately 2003, DOD initially did make progress implementing IPv6 on its systems, but then the department ended the effort due to security risks and a lack of personnel trained in IPv6. DOD initiated another attempt in response to 2010 OMB guidance. However, this initiative was terminated shortly thereafter, again due to security concerns.

For its current initiative, DOD has not completed three of four longstanding OMB requirements (see table). Without an inventory, a cost estimate, or a risk analysis, DOD's plans have a high degree of uncertainty about the magnitude of work involved, the level of resources required, and the extent and nature of threats, including cybersecurity risks.

Status of the Department of Defense's (DOD) Efforts to Complete Selected Office of Management and Budget (OMB) Internet Protocol version 6 (IPv6) Transition Planning Requirements, as of March 2020

OMB requirement	Completed?
Assign an official to lead and coordinate agency planning	Yes
Complete an inventory of existing IP compliant devices and technologies	No
Develop a cost estimate	No
Develop a risk analysis	No

Source: GAO analysis of DOD documentation. | GAO-20-402

In February 2019, DOD released its own IPv6 planning and implementation guidance that listed 35 required transition activities, 18 of which were due to be completed before March 2020. DOD completed six of the 18 activities as of March 2020. DOD officials acknowledged that the department's transition time frames were optimistic; they added that they had thought that the activities' deadlines were reasonable until they started performing the work. Without an inventory, a cost estimate, or a risk analysis, DOD significantly reduced the probability that it could have developed a realistic transition schedule. Addressing these basic planning requirements would supply DOD with needed information that would enable the department to develop realistic, detailed, and informed transition plans and time frames.

Contents

Tables

Figures

Abbreviations

CIO	chief information officer
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DREN	Defense Research and Engineering Network
IG	Inspector General
IoT	Internet of Things
IP	internet protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 1, 2020

Congressional Committees

The increasing use of the internet has promoted a dramatic expansion in the number of users and types of devices that communicate with each other through an internet protocol (IP). An IP is one of the primary mechanisms used to define how and where information such as text, voice, and video moves across networks. Proper functioning of this protocol is dependent upon devices having unique identifiers, or addresses, to properly transmit and receive information. Without unique addresses, information transmitted to or from these devices could inadvertently be sent to unintended destinations. These destinations could include individuals or entities with malicious intent. Further, without unique addresses defining each destination, the internet could become unreliable and chaotic.

The Department of Defense (DOD), like many organizations and federal agencies, currently uses an older protocol, known as Internet Protocol version 4 (IPv4), to support its mission requirements. IPv4 is approaching obsolescence due to expanded internet use and the exhaustion of IPv4 addresses available for distribution.

The inadequate supply of IPv4 addresses spurred the development and global adoption of its successor protocol, Internet Protocol version 6 (IPv6). In comparison to IPv4's approximately 4.3 billion addresses, IPv6 provides approximately 340 undecillion (i.e., 340 trillion, trillion, trillion or 3.4×10^{38}) possible unique addresses, which is enough to assign many trillions of addresses to every person on Earth.

IPv6 is expected to provide improved, more efficient information technology (IT) services, mobility, and security. Leading technology firms, major corporations, and foreign governments have been implementing the protocol. For example, China announced its goal to establish the world's largest IPv6 network by the end of 2025. Further, DOD has begun efforts to transition its networks and systems from IPv4 to IPv6.

Senate Report 116-48[1] and House Report 116-120[2] included provisions for us to review DOD's continued use of IPv4 and its transition to IPv6. This report specifically (1) identifies DOD's past attempts to transition to IPv6, (2) examines the extent to which DOD has completed Office of Management and Budget (OMB) transition planning requirements, and (3) identifies DOD's progress in completing its own required activities for transitioning to IPv6. The scope of our review focused on DOD's department-wide IPv6 transition initiative led by officials within multiple offices and components, including DOD's Office of the Chief Information Officer (CIO) and the Defense Information Systems Agency. We did not review the efforts or plans of individual DOD component agencies or military services unless they pertained to department-wide transition requirements.

To identify DOD's past attempts to transition to IPv6, we consulted OMB's IPv6 implementation guidance to give context and establish a timeline of DOD's past transition deadlines. Further, we reviewed DOD reports, policies, and other documentation pertaining to the department's past and current IPv6 transition initiatives. For instance, we reviewed DOD's December 2014 Inspector General (IG) report on DOD's IPv6 transition efforts.[3] Further, we interviewed and received written responses from the DOD officials leading the transition to IPv6 about the history of DOD's transition attempts, as well as the background of the department's current transition initiative.[4] We then used this information to describe the history of DOD's past IPv6 transition efforts.

To examine the extent to which DOD has completed OMB transition planning requirements, we first reviewed OMB guidance related to IPv6

[1] U.S. Congress, Senate, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2020: Report (to Accompany S. 1790)*, 116th Congress, 1st sess., 2019, S. Rep. 116-48, p. 23.

[2] U.S. Congress, House of Representatives, Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2020: Report together with Additional and Dissenting Views (to Accompany H.R. 2500)*, 116th Congress, 1st sess., 2019, H. Rep. 116-120, p. 276.

[3] DOD, Office of Inspector General*, DoD Needs to Reinitiate Migration to Internet Protocol Version 6*, DODIG-2015-044 (Alexandria, VA: December 2014).

[4] The officials leading the transition to IPv6 that we contacted and interviewed included the department-wide lead for DOD's IPv6 transition, the lead of the Defense Information Systems Agency's transition to IPv6, and representatives from the DOD Office of the CIO and the Defense Information Systems Agency, among others.

transition planning, including OMB memorandum M-05-22, "*Transition Planning for Internet Protocol Version 6 (IPv6)*."[5] While our work was ongoing, we confirmed with OMB that the criteria were still applicable and that OMB had not replaced or rescinded them.[6] We also requested and reviewed DOD's policies and plans related to its department-wide IPv6 transition efforts. In addition, we reviewed publicly available documentation related to DOD's IPv6 planning efforts. Further, we met with, and received written responses from, the DOD officials leading the transition to IPv6 about the department's transition planning efforts.

Using this information, we first selected the applicable criteria in OMB memorandum M-05-22 that pertained to IPv6 planning. These criteria called for agencies to: (1) assign an official to lead and coordinate agency planning, (2) complete an inventory of existing IP-compliant devices and technologies, and (3) develop an impact analysis containing both a cost estimate and a risk analysis. We then requested and analyzed DOD's responses and documentation regarding the extent to which it had completed the IPv6 planning activities required by the criteria we selected from the OMB memorandum.

To identify DOD's progress in completing its own required IPv6 transition activities, we reviewed the department's February 2019 "DOD CIO IPv6 Guidance Memo." According to the memorandum, it provides initial direction and guidance for DOD's IPv6 transition. The memorandum lists 35 transition activities and includes due dates for 27 of them. Over the course of the engagement, we routinely inquired about the progress DOD made against all the activities listed in the memorandum, including the activities that did not have specific due dates. If DOD submitted evidence for completing an activity, we evaluated the actions taken and compared them to the specific transition activities. From our analysis, we determined which activities had sufficient evidence to support completion and which

[5] OMB, *Memorandum for Chief Information Officers: Transition Planning for Internet Protocol Version 6 (IPv6)*, M-05-22 (Washington, D.C.: August 2005).

[6] In March 2020, OMB released updated IPv6 draft guidance for comment in the Federal Register (85 FR 12347). This draft guidance would rescind and replace previous OMB IPv6 guidance such as OMB memorandum M-05-22; however, this guidance had not been finalized as of May 2020. Thus, M-05-22 remained valid criteria for the purpose of our audit work. [OMB, *Memorandum for Heads of Executive Departments and Agencies: Completing the Transition to Internet Protocol Version 6 (IPv6)*, draft (Washington, D.C.: March 2020).]

activities were past due. The full results of this analysis are shown in appendix I.

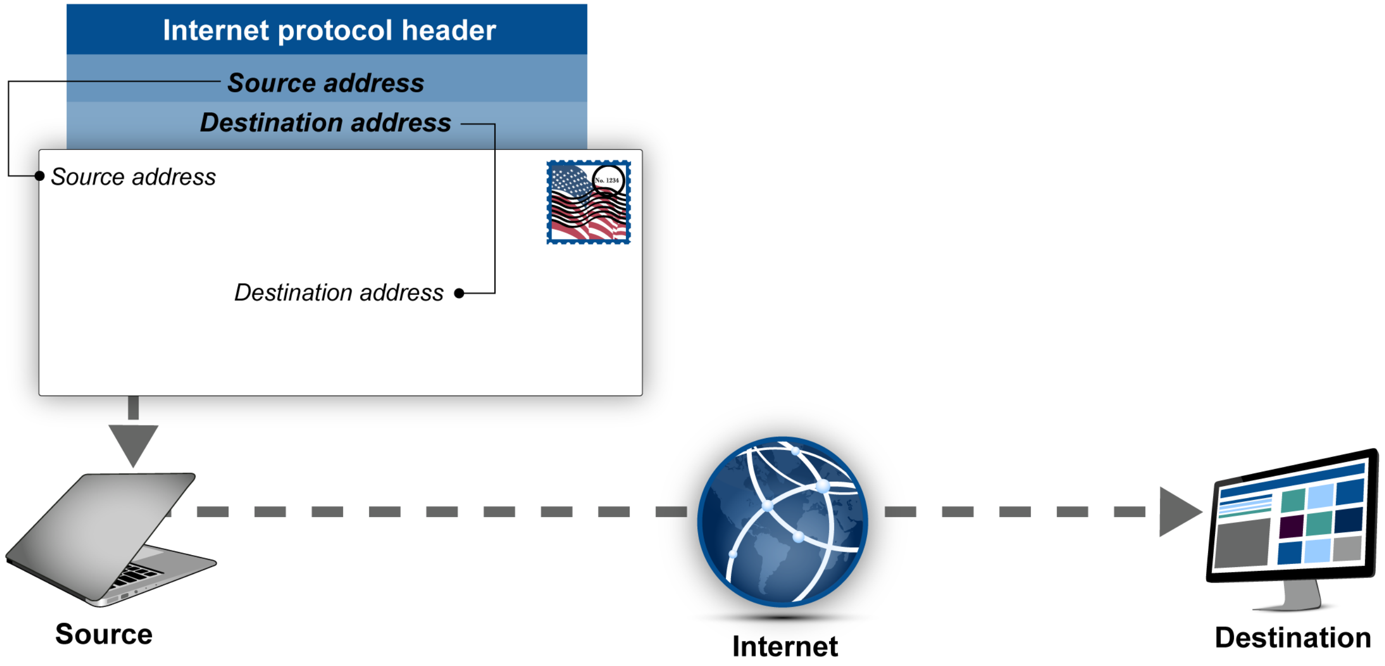
We conducted this performance audit from June 2019 to June 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The internet is a worldwide network of networks comprised of backbone networks, servers, and routers. Network addresses are used to help send information from one internet-connected device, such as a computer, to another by routing the information to its final destination. The protocol that enables the administration of these addresses is the IP.

IP addresses provide a numerical description of the location of networked devices such as computers, routers, and smartphones. These numerical descriptions allow devices to be distinguished from each other over the internet. In some ways, an IP address is like a physical street address. For example, in the physical world, if you want to send a letter from one location to another, the contents of the letter must be placed in an envelope that lists both the sender’s and the recipient’s addresses. Similarly, if data is transmitted across the internet from one device to another, IP addresses must be placed in an IP header with sender and recipient information. In addition to containing the addresses of the sender and the receiver, the header also contains a series of fields that provide information about what is being transmitted. Figure 1 provides a simplified illustration of this concept.

Figure 1: An Internet Protocol (IP) Header Contains IP Addresses for the Source and Destination of Information Transmitted across the Internet



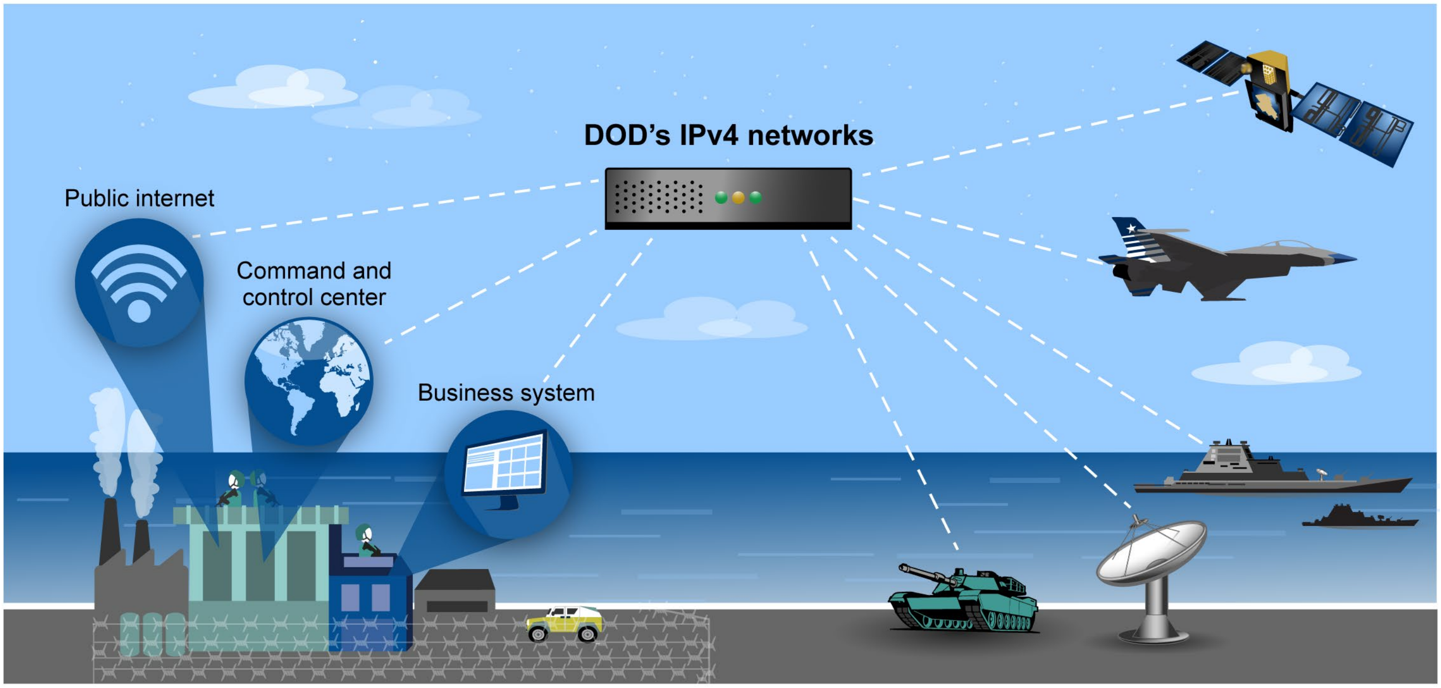
Source: GAO. | GAO-20-402

The Internet Engineering Task Force, the principal body engaged in the development of internet standards, developed IPv6 in the 1990s to address IPv4's limited address space, among other things. Although IPv6 has been available for over 20 years, IPv4, the older IP, is still more widely deployed. Nevertheless, IPv6 deployment is rising worldwide amidst the exhaustion of available IPv4 addresses.[7] However, IPv6 is not backwards compatible with IPv4, which means that organizations such as DOD have to change their network infrastructure and systems in order to deploy IPv6.

[7] The Internet Assigned Numbers Authority allocates the global pool of IP addresses to Regional Internet Registries, which in turn manage and distribute the addresses for specific geographic areas. The authority administered the last unallocated IPv4 internet addresses in February 2011, signaling the top-level exhaustion of IPv4. The American Registry for Internet Numbers, which is the Regional Internet Registry responsible for distributing IP address space in the United States, no longer has available IPv4 addresses. Its free pool of IPv4 address space was depleted in September 2015.

DOD relies on its current IPv4 networks to fulfill its mission to provide the military forces needed to deter war and ensure our nation's security. According to DOD officials leading the transition to IPv6, the department utilizes IPv4 for enterprise-wide and mission partner wired and wireless communications, including infrastructure, technologies, and devices supporting large-scale globally dispersed command and control systems, naval vessels, aircraft, satellites, and ground operations. Figure 2 presents a simplified depiction of the department's use of IPv4.[8]

Figure 2: The Department of Defense's (DOD) Uses of Internet Protocol version 4 (IPv4) to Support Its Mission



Source: GAO analysis of Department of Defense information. | GAO-20-402

DOD's mission requires considerable IP address space. The department currently has 300,149,760 IPv4 addresses—more than any other

[8] Figure 2 is a simplified depiction of DOD's IPv4 networks so as not to reveal classified information.

organization in the world.[9] These approximately 300 million addresses are divided into blocks; each block contains a series of multiple addresses. DOD has 13 particularly large blocks of addresses, each containing 16,777,216 addresses.[10] Also included in the approximately 300 million addresses are 59,767,040 IPv4 addresses that currently are unused. These addresses are reserved for future use by DOD and its components.

DOD has stated that it expects to exhaust its reserve of unused IPv4 addresses by 2030. According to the officials leading the IPv6 transition effort, the department expects to have to support IPv4 after it exhausts its IPv4 address space in 2030 due to mission system modernization and replacement timelines, as well as new emerging technologies that may require IPv4 resources while the department transitions to IPv6.[11]

[9] DOD provided the data on the numbers and ranges of its IPv4 addresses. We did not independently verify this information.

[10] These series of approximately 16.8 million addresses, referred to as /8 blocks, are the largest blocks of IPv4 addresses that can be assigned to an organization. An /8 block contains all of the IPv4 addresses that have the same number before the first period. DOD's /8 blocks are 6.0.0.0/8, 7.0.0.0/8, 11.0.0.0/8, 21.0.0.0/8, 22.0.0.0/8, 26.0.0.0/8, 28.0.0.0/8, 29.0.0.0/8, 30.0.0.0/8, 33.0.0.0/8, 55.0.0.0/8, 214.0.0.0/8, and 215.0.0.0/8. According to DOD officials leading the IPv6 transition initiative, these large blocks of addresses are assigned to the department itself, as well as to components such as the Army and the Defense Information Systems Agency. Three of these /8 blocks, 26.0.0.0/8, 28.0.0.0/8, and 30.0.0.0/8, are currently unassigned and reserved for future use.

[11] If DOD has unused or excess IPv4 addresses in the future, other organizations could be interested in acquiring these addresses. Due to the exhaustion of available IPv4 addresses, there is currently a private sector marketplace for selling and purchasing IPv4 addresses. We are not aware of any statutory requirements that directly address the ability of a government agency to transfer or sell IP addresses to a third party, but DOD would face legal and policy constraints to any potential sale or transfer of the addresses to a third party outside of the government. Among other things, this is because DOD entered into an agreement with the American Registry for Internet Numbers. Specifically, this agreement states the department must return unused addresses to the registry.

IPv6 May Improve Functionality and Provide Benefits

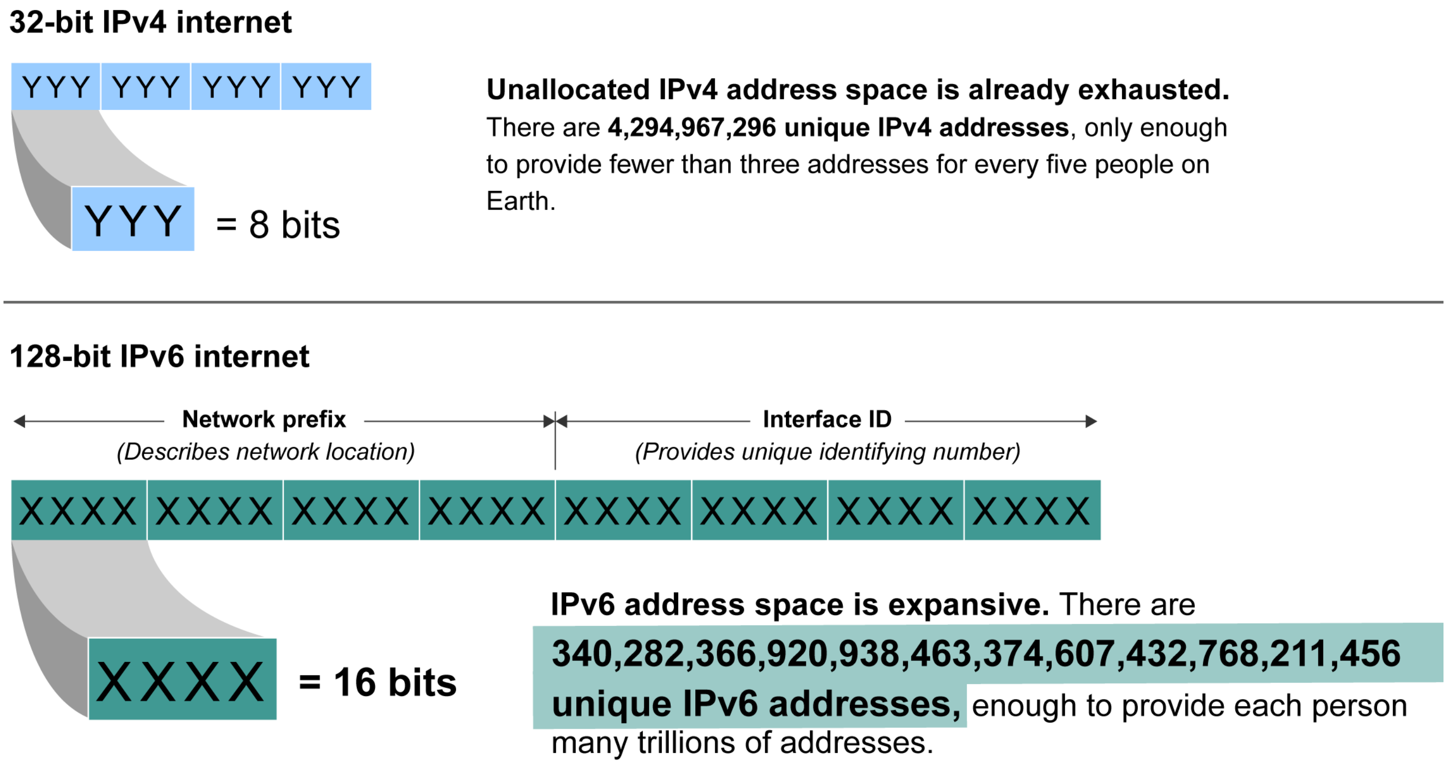
According to prior government reports and DOD documentation, IPv6's improved functionality would benefit the department in many ways. In addition to the general benefits of eliminating IPv4 address space limitations, enhancing mobility features, and integrating IP security, IPv6 has the potential to enhance DOD battlefield operations, improve decision-making with the increased reliance on the Internet of Things (IoT), support U.S. global technological competitiveness, and enhance mission partner interoperability.[12]

- **IPv6 eliminates address space limitations.** As previously mentioned, IPv6 dramatically increases the amount of possible address space from 4.3 billion addresses in IPv4 to approximately 340 undecillion (3.4×10^{38}) addresses. The massive increase in addresses is due to the larger amount of information, or bits, in each address: IPv6 uses a 128-bit address scheme instead of IPv4's 32-bit address scheme. 128 bits of information have the ability to create an immense number of possible unique number combinations. Figure 3 compares IPv4 and IPv6 address spaces and illustrates how the increase in bits resulted in the extensive IPv6 address space.

In addition, transferring unused IP addresses to another entity besides the registry would violate the government's stated policy position articulated by the National Telecommunications and Information Administration, which is the agency principally responsible for advising the President on telecommunications and information policy issues. According to this agency, IP addresses assigned to the government should be returned to the American Registry for Internet Numbers' pool of available IP addresses when no longer in use. [Statement of Assistant Secretary for Communications and Information and National Telecommunications and Information Administration Administrator Lawrence E. Strickling, (Dec. 3, 2012), accessed Sept. 16, 2019, https://www.ntia.doc.gov/blog/2012/united-states-government-s-internet-protocol-numbering-principles.] Finally, both GAO and the Department of Commerce have asserted that the addresses are not U.S. government property that a federal agency could transfer or sell. [GAO, *Property Implications of Proposed Transition of U.S. Government Oversight of Key Internet Technical Functions*, B-327398 (Washington, D.C.: Sept. 12, 2016.)] Therefore, even though there is a private sector marketplace for selling IPv4 addresses, DOD would not be able to participate.

[12] The IoT refers to networks of objects that communicate with other objects and with computers through the internet. Two features make objects part of the IoT—a unique identifier and internet connectivity. Such "smart" objects each have a unique IP address to identify the object sending and receiving information. Smart objects can form systems that communicate among themselves, usually in concert with computers, allowing automated and remote control of many independent processes and potentially transforming them into integrated systems.

Figure 3: Comparison between the Size of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) Address Spaces



Unallocated IPv4 address space is already exhausted. There are **4,294,967,296 unique IPv4 addresses**, only enough to provide fewer than three addresses for every five people on Earth.

IPv6 address space is expansive. There are **340,282,366,920,938,463,374,607,432,768,211,456 unique IPv6 addresses,** enough to provide each person many trillions of addresses.

Source: GAO. | GAO-20-402

In contrast to IPv4, the massive address space available in IPv6 will allow almost any device to be assigned a unique IP address. This change fosters greater end-to-end communication abilities between devices with unique IP addresses and can better support the delivery of data-rich content such as voice and video.

- **Enhanced mobility improves connectivity.** IPv6 improves mobility features by allowing each device to have a unique IP address independent of its current network or connection point to the internet. This enables mobile IPv6 users to move from network to network while keeping the same unique IP address. The ability to maintain a constant IP address while switching networks is cited as a key factor for the success of a number of evolving capabilities, such as telephone technologies, laptop computers, and internet connected automobiles.

- **Added IP security helps to protect data.** IP security—a means of authenticating the sender and encrypting the transmitted data—is better integrated into IPv6 than it is in IPv4. This improved integration, which helps make IP security easier to implement, can help support broader data protection efforts. This extra security is accomplished through the use of two header extensions that can be used together or separately to improve the authentication and confidentiality of data being sent via the internet. These headers serve to provide the receiver with a greater assurance of the sender's identity and provide encryption protection for the transmitted data.

- **Enhanced capabilities could improve DOD battlefield operations.** According to the 2014 DOD IG report on DOD's IPv6 transition efforts, use of IPv6 could provide DOD with several potential benefits related to battlefield operations, such as improved communication, warfighter mobility, situational awareness, and quality of service.[13] IPv6 auto-configuration capabilities provide secure ad hoc networking and mobility, as well as improved end-to-end security and simplified network management capabilities. This could potentially enable individuals and entire units to disconnect from military base networks, travel into theater, and quickly establish communications.[14] Additionally, IPv6 capabilities could allow warfighters and commanders to improve situational awareness and mission execution during deployment and battle operations, allowing units to securely move from one wireless network to another.

- **Increased use of the IoT may improve decision-making.** The increased address space available with IPv6 enables the increased connectivity necessitated by the proliferation of the IoT. DOD's IoT could include any object for which remote communication, data collection, or control might be useful, such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems. According to DOD's Digital Modernization Strategy from July 2019, IoT could be significant to the department's decision-making processes because the assortment of connected objects that comprise IoT could enable technology to gain the ability to sense, predict, and respond to DOD's

[13] DODIG-2015-044.

[14] A theater is a geographical area under the responsibility of a unified or specified command with a broad continuing mission.

needs.[15] The department could use computers to track, count, and analyze data from these objects in order to reduce waste, loss, and cost. DOD managers could also know whether these objects were running well or needed replacing, repairing, or recalling.

- **IPv6 could support U.S. global technological competitiveness.** According to a DOD presentation, the transition to IPv6 could allow the department to remain technologically competitive globally.[16] Interest in IPv6 is gaining momentum around the world, particularly in parts of the world that have limited IPv4 address space to meet their industry and consumer communications needs. Regions that have limited IPv4 address space, such as Asia and Europe, have undertaken efforts to develop, test, and implement IPv6. For example,
  - China has been aggressive at deploying IPv6.
  - Japan has set up an IPv6 Promotion Council, using tax incentives to encourage research and adoption of IPv6 by its private sector.
  - Europe has a task force that has the dual mandate of initiating country and regional IPv6 task forces across European states and seeking global cooperation around the world.
- **Transitioning to IPv6 may preserve mission partner interoperability.** According to an August 2017 report from DOD's CIO, deploying IPv6 capabilities is essential to preserve interoperability with mission partners in the private sector and in other countries and to assure future access to technology.[17] Since the pools of unassigned IPv4 addresses are exhausted, DOD's mission partners may increasingly rely on IPv6 addresses in the future, furthering the department's need to increase its IPv6 capabilities.

Transitioning to IPv6 Could Also Present Challenges

Along with the potential benefits, the National Institute of Standards and Technology (NIST) has indicated that transitioning to IPv6 also could present challenges for organizations such as DOD. These challenges

[15] DOD*, DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23* (Washington, D.C.: June 2019).

[16] Defense Information Systems Agency, *DISA IPv6 Background* (July 17, 2019).

[17] Director, Department of Defense Information Network Modernization and the Office of the DOD CIO, *Achieving the Joint Information Environment Vision: Modernizing DoD's IT and Associated Enterprise-wide Operations, version 1.3* (Washington, D.C.: August 2017).

include the complexity added by dual IPv4 and IPv6 operations and the immaturity of IPv6 security products and processes.[18]

- **Complexity added by dual IPv4/IPv6 operations.** DOD plans to deploy IPv6 while still supporting IPv4 for legacy applications, services, and clients. This will result in a dual protocol environment and increased complexity. With two protocols, DOD would have to ensure the proper functioning of two separate, but interrelated, networks instead of only one network. Further, hackers and other online adversaries could exploit either the department's IPv4 or IPv6 network connections when launching cyberattacks.
- **Immaturity of IPv6 security processes.** While IPv6 could offer enhanced security, NIST states that its deployment could also lead to new challenges with respect to the types of threats facing an organization such as DOD.[19] For example, organizations in the process of transitioning to IPv6 may lack robust IPv6 security controls and may have security staff members who lack an overall understanding of IPv6. This could allow attackers to exploit IPv6 assets or leverage IPv6 access to exploit IPv4 assets. While general security concepts are the same for both IPv4 and IPv6 protocols, it may take time and effort for transitioning organizations such as DOD to acquire the level of operational experience and practical deployment solutions that have been developed for IPv4 over the years.

OMB Issued Guidance for Federal Agencies' IPv6 Transition Planning

In August 2005, OMB issued a memorandum to federal CIOs specifying a series of IPv6 transition planning and implementation requirements and associated due dates for federal agencies to enable the use of IPv6.[20] Specific to planning for the transition, the memorandum required agencies to assign an official to lead and coordinate IPv6 transition planning efforts, complete an inventory of IP-compliant devices and technologies, and complete an impact analysis comprised of a cost

[18] Sheila Frankel, Richard Graveman, John Pearce, and Mark Rooks, *Guidelines for the Secure Deployment of IPv6: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-119 (Gaithersburg, MD: December 2010). In May 2020, an official in OMB's Office of General Counsel informed us that OMB had asked NIST to review this publication to determine if any updates are needed to ensure that it continues to reflect current security trends.

[19] NIST Special Publication 800-119.

[20] OMB, *Memorandum for the Chief Information Officers: Transition Planning for Internet Protocol Version 6 (IPv6)*, M-05-22 (Washington, D.C.: August 2005).

estimate and a risk analysis by specific due dates during fiscal year 2006.[21] Table 1 lists the transition planning requirements and due dates defined in the OMB memorandum.

Table 1: The Office of Management and Budget's (OMB) Planning Requirements for Federal Agencies' Internet Protocol version 6 (IPv6) Transition and Associated Due Dates

Requirement	Due date[a]
Assign an official to lead and coordinate IPv6 transition planning.	November 2005
Complete an inventory of internet protocol-compliant devices and technologies	June 2006
Develop a cost estimate (as part of the impact analysis)	June 2006
Develop a risk analysis (as part of the impact analysis)	June 2006

Source: OMB. | GAO-20-402

[a] OMB memorandum M-05-22 originally gave multiple due dates for developing the inventory and impact analysis requirements. The due dates listed in this column are the final deadlines for the completed requirements.

DOD Has Engaged in IPv6 Transition Efforts since 2003

Aware of the limitations of IPv4, DOD first began planning for the implementation of IPv6 in June 2003. At that time, the department's CIO issued the memorandum, "Internet Protocol Version 6 (IPv6)." According to this memorandum, the department's initial goal was to complete its transition to IPv6 by fiscal year 2008.

Within a month of the issuance of DOD's June 2003 memorandum, the department designated the Defense Research and Engineering Network (DREN) as the first DOD IPv6 pilot network.[22] DREN, being a research and development network, is not connected to DOD's operational networks, such as the department's nonclassified IP router network, which transmits nonclassified operations traffic. According to a DOD report about the DREN pilot, the entire DREN wide-area network was

[21] A cost estimate is the summation of individual cost elements, using established methods and valid data, to estimate the future costs of a program, based on what is known at the time. A risk analysis enables an agency to assess the significance of potential threats to the success of a program, as well as assess how these threats could be mitigated or avoided.

[22] DREN's purpose is to provide robust, high capacity, low latency connectivity between DOD Supercomputing Resource Centers and user sites.

routinely supporting end-to-end IPv6 traffic by July 2005.[23] According to the department, DREN remains DOD's only IPv6-enabled network.

Further, DOD's IG reported that the department had undertaken an initial transition effort that temporarily satisfied OMB's August 2005 implementation requirement to demonstrate IPv6 on its infrastructure by the end of June 2008.[24] Specifically, DOD was able to demonstrate IPv6 within the department's Defense Information Systems Network.[25] However, according to the report, the department's IPv6 transition manager said DOD disabled IPv6 functionality due to a lack of trained personnel and potential security risks. We received additional information about why DOD disabled the IPv6 functionality, but we are not including it in the report due to the information being marked as for official use only.

DOD began its next effort to plan and implement IPv6 in response to OMB's subsequent 2010 guidance.[26] In this guidance, OMB gave agencies—including DOD—requirements intended to further their transitions to IPv6. Two of these requirements stated that agencies were to:

- upgrade their public-facing IT servers and services (e.g., web and email) to IPv6 by the end of September 2012; and

[23] DOD, High Performance Computing Modernization Program—Defense Research and Engineering Network, *DREN Helps Make the Transition to Internet Protocol version 6 (IPv6)* (Lorton, VA).

[24] DODIG-2015-044.

[25] The Defense Information Systems Network is DOD's global enterprise network that enables the U.S. military and mission partners to leverage, sustain, and exercise distinct advantages over adversaries. The network also supports command and control, intelligence, logistics, medical, and other essential missions across the full spectrum of military operations.

[26] OMB, *Memorandum for Chief Information Officers of Executive Departments and Agencies: Transition to IPv6* (Washington, D.C.: September 2010).

- upgrade internal client applications that communicate with public internet servers and supporting enterprise networks to IPv6 by the end of September 2014.[27]

According to DOD, the department originally planned to meet the 2010 OMB requirements; however, it decided not to complete the upgrades due to security concerns. Again, we received additional information about the department's security concerns; however, we are not including those details in this report because they were marked as for official use only.

DOD Had Not Completed Most of the Selected OMB Planning Requirements

OMB's IPv6 transition guidance requires federal agencies, such as DOD, to perform specific tasks as part of their IPv6 planning efforts. These tasks include: (1) assigning an official to lead and coordinate agency planning, (2) completing an inventory of existing IP-compliant devices and technologies, (3) developing a cost estimate (as part of an impact analysis), and (4) developing a risk analysis (as part of an impact analysis). Although these requirements were originally due in 2005 or 2006, they are still applicable; OMB has not replaced or rescinded them.[28]

Assigning an official to lead and coordinate agency planning can help agencies better manage their transition to IPv6. Specifically, a senior-level focal point to lead IPv6 transition efforts can provide assurance that the program is based on a coherent strategy and is well coordinated. A lead official may also help an agency avoid duplicative, overlapping, and fragmented efforts, which can result in avoidable additional costs.

According to NIST, having an inventory of IP-compliant assets is crucial to IPv6 transition planning because it helps determine transition requirements and give an agency a clear understanding of the IP capabilities of the devices on the network.[29] Specifically, an inventory helps determine which assets will transition to IPv6, the order in which

[27] OMB's March 2020 draft IPv6 guidance states that it would rescind OMB's 2010 guidance in addition to memorandum M-05-22. However, the draft guidance specifies that these two implementation requirements from the 2010 guidance remain valid and that agencies should complete these actions as soon as possible, if they have not already done so.

[28] OMB's draft IPv6 guidance, which states that it would rescind these OMB requirements, has yet to be finalized. The four planning requirements described in this section were valid as of May 2020.

[29] NIST Special Publication 800-119.

assets will transition, the transition methods selected, and the security controls that would need to be implemented.

Further, cost estimates are critical to decision-makers not only because they help establish budgets, but also because they are integral to determining and communicating a realistic view of likely cost and schedule outcomes that could be used to plan the work necessary to develop, produce, install, and support a program. As we have previously reported, without the ability to generate reliable cost estimates, agencies are at risk of experiencing cost overruns, missed deadlines, and performance shortfalls.[30] In addition, a risk analysis enables an agency to assess the significance of potential threats to the success of its transition to IPv6, as well as assess how those threats could be mitigated or avoided. Further, without a risk analysis to help the agency understand the potential threats and obstacles facing the IPv6 transition initiative, agencies run the risk of creating goals and plans that are too optimistic.

According to DOD, the department began its most recent effort to transition to IPv6 in April 2017. As part of this effort, in November 2019, the department released its IPv6 implementation strategy, which articulates DOD's overarching vision for its IPv6 transition initiative: to provide secure and reliable IPv6 services that enable innovation for competitive advantage.[31] According to the strategy, DOD's goals for the effort include implementing an interim solution of using both IPv4 and IPv6 and then planning for an eventual IPv6-only environment.

As of March 2020, DOD had not yet completed three of the four selected transition planning requirements. Specifically, the department had completed the requirement of appointing an agency lead for its IPv6 transition efforts. However, it had not yet completed the three other requirements: complete an inventory, develop a cost estimate, and develop a risk analysis. Table 2 summarizes the status of DOD's completion of the four selected OMB IPv6 transition planning requirements.

[30] GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs,* GAO-09-3SP (Washington, D.C.: Mar. 2, 2009).

[31] DOD*, Department of Defense (DOD) Strategy to Implement Internet Protocol version 6 (IPv6)* (Washington, D.C.: November 2019).

Table 2: Status of the Department of Defense's (DOD) Efforts to Complete Selected Office of Management and Budget (OMB) Internet Protocol version 6 (IPv6) Transition Planning Requirements, as of March 2020

OMB requirement	Completed?
Assign an official to lead and coordinate agency planning	Yes
Complete an inventory of existing internet protocol-compliant devices and technologies	No
Develop a cost estimate (as part of the impact analysis)	No
Develop a risk analysis (as part of the impact analysis)	No

Source: GAO analysis of DOD documentation. | GAO-20-402

DOD completed OMB's requirement to have an official lead the IPv6 planning efforts by first assigning its Joint Information Environment Executive Committee responsibility for overseeing the department's transition to IPv6 in August 2017.[32] The committee, in turn, established the DOD IPv6 Working Group in November 2017 to coordinate and manage department-wide IPv6 planning, implementation, and testing. An official in the Office of the CIO serves as the chair of the working group, and, according to the group's charter, is responsible for leading meetings, soliciting and prioritizing issue topics for review, and overseeing the coordination of working group activities supporting the department-wide transition to IPv6.

However, DOD did not complete the requirement to develop an inventory of existing IP-compliant devices and technologies. In November 2005, DOD provided a memorandum to OMB that indicated that the department would not complete the inventory of IP-compliant devices and technologies; instead, DOD would continue following its existing transition plan, which did not require an inventory.[33] Further, the DOD officials leading the IPv6 transition effort informed us that the department had not developed such an inventory and that it still does not plan to do so. The

[32] The Joint Information Environment Executive Committee sets the goals and provides oversight for DOD's objective to provide a single, secure, reliable, timely, effective, and agile command, control, communications, and computers enterprise information environment. As part of this effort, it provides oversight for the department's transition to IPv6.

[33] DOD, *Memorandum for Office of Management and Budget: Transition Planning for Internet Protocol Version 6 (IPv6)* (November 2005).

officials said that conducting a task of this size would be impractical given DOD's size and the number of IP-compliant devices in the department.

The officials leading the IPv6 transition also said that DOD has been mitigating the risk of not having an inventory by ensuring that the department has only been acquiring IPv6-capable IT devices since December 2009.[34] However, while only acquiring IPv6-capable devices and applications could help the transition move forward, it would not be as complete as an inventory, given that an inventory would include technology purchased before December 2009.

DOD also did not complete a cost estimate or a risk analysis. According to the DOD officials leading the IPv6 transition effort, the initiative was not a top priority until the CIO released the "Internet Protocol Version 6 Implementation Direction and Guidance" memorandum in February 2019. This memorandum, which was developed to guide the department's IPv6 transition planning and implementation efforts, gave the transition initiative greater attention in the department. Prior to the issuance of the memorandum, the officials stated that they did not have sufficient resources to conduct the cost estimate and did not have enough understanding to complete the risk analysis. DOD officials leading the IPv6 transition effort explained that the department plans to develop these requirements by the end of May 2020; however, we have not received any documentation confirming this deadline.

Until DOD develops an inventory of IP-compliant technologies and devices, a cost estimate, and a risk analysis, the department's IPv6 transition initiative may have an increased likelihood of cost overruns, schedule delays, and security vulnerabilities. Specifically, not having an inventory of IP-compliant devices and technologies may lead to the department developing plans without being aware of all the system and infrastructure requirements necessary to successfully transition a large organization such as DOD to IPv6. Further, without a cost estimate, DOD may be making decisions without the benefit of relevant information on the initiative's potential cost and schedule outcomes, thereby introducing unnecessary risk into the implementation process. Finally, by moving

[34] As of December 10, 2009, agencies such as DOD were required to follow a new rule that mandates the inclusion of IPv6-compliant products in all new IT acquisitions using IP unless the agency CIO granted a waiver to the use of IPv6. This rule is found in Section 11.002(g) of the Federal Acquisition Regulation. The Federal Acquisition Regulation contains the policies and procedures governing executive agencies' acquisitions, including DOD's.

forward without a risk analysis, DOD increases the probability that it is not proactively managing potential threats that could disrupt the transition or introduce new IT security vulnerabilities.

DOD Had Not Completed Most of Its Own Required Transition Activities

DOD's February 2019 memorandum lists 35 required activities for transitioning to IPv6 that DOD's various components or offices, such as the Office of the CIO, are to complete or work on during fiscal years 2019 through 2021. Of these 35 activities, 18 were to be completed prior to March 2020.

However, DOD had not completed most of the required activities. Specifically, of the 18 activities that were to be completed by March 2020, the department had completed six and had not completed 12. In addition, the department had completed one of eight other activities that did not have specific due dates.[35] Table 3 outlines the department's seven IPv6 transition activities that had been completed as of March 2020. (See appendix I for a full list of DOD's transition activities and their completion status.)

Table 3: The Department of Defense's (DOD) Completed Internet Protocol version 6 (IPv6) Transition Activities, as of March 2020

Completed transition activity	Component or office responsible
Lead development of a DOD IPv6 Strategy for Joint Information Environment Executive Committee endorsement and DOD Chief Information Officer (CIO) signature.	DOD CIO
Determine U.S. interagency collaboration and cybersecurity information sharing opportunities (e.g., best practices, product assessments, and roadmaps).	DOD CIO
Designate an IPv6 lead for the Defense Information Systems Agency (DISA) and establish a virtual program management office.[a]	DISA
Provide an electronic means for DOD components to submit, manage, and de-conflict IPv6 priorities, plans, and requirements.	DISA
Provide on demand IPv6 familiarization training and assess commercial advanced training resources for network engineers and cybersecurity personnel.	DISA
Provide on demand advanced IPv6 training resources for network engineers and cybersecurity personnel.	DISA
Provide IPv6-enabled Cyber Security Range services.[b]	DISA

Source: GAO analysis of DOD documentation. | GAO-20-402

[a] The DISA-led Virtual Program Management Office reports to the DOD IPv6 Working Group and the Joint Information Environment Executive Committee. According to its charter, the Virtual Program Management Office is to create a single, synchronized effort across DOD to implement IPv6 using subject matter experts and integrated product teams.

[35] Of the remaining nine activities that the department did not complete, seven required activities had due dates after March 2020, and two activities were canceled.

[b]DOD’s Cyber Security Range provides a virtual space in which cyber warriors can conduct cyber training, testing, and exercises in an environment identical to their daily field of battle.

One notable required activity that DOD completed was to develop a CIO-approved strategy to implement its transition to IPv6. DOD’s strategy outlines, among other things, the overall goals for the IPv6 transition initiative. These goals include implementing a network that is both IPv4 and IPv6 capable; planning for an IPv6-only environment; and establishing and optimizing training for IPv6.

In addition, DOD’s Defense Information Systems Agency leveraged online training providers to offer on demand IPv6 training courses for network engineers and cybersecurity personnel. In addition to basic familiarization training for those new to IPv6, select training courses are labeled as being at the advanced level.

However, the department had not completed 12 of 18 activities that were due prior to March 2020. Notably, DOD missed its original September 2019 deadline to enable IPv6 on all commercially hosted public facing unrestricted services.[36] According to the department officials leading the IPv6 transition, DOD expects to be able to complete this task by the end of July 2021. The department also missed its original June 2019 deadline for identifying the public facing unrestricted services hosted by DOD. The officials leading the IPv6 transition initiative stated that DOD currently plans to complete this activity by May 2020. Other activities that were past due in March 2020 include: developing supplemental guidance for the acquisition of IPv6-capable products, updating and maintaining IPv6 standards and implementation profiles, and determining DOD’s cybersecurity architecture and posture impacts, among others.

DOD officials leading the IPv6 transition effort stated that the department had not yet completed its required activities because the original time frames that the department had established were unrealistic. Although the activities were initially thought to have been reasonable, DOD adjusted the activities’ due dates after the department began executing the tasks and realized that it would take a large amount of work to accomplish their goals and complete the activities.

One contributing factor for the unrealistic due dates is that DOD developed this list of required activities without the benefit of an inventory

[36] Public facing services are the networked services that DOD currently provides, or will provide, to the general public.

of IP-compliant devices and technologies, a cost estimate, or a risk analysis. Without completing these basic planning requirements, DOD significantly reduced the probability that it could have developed a realistic transition schedule. Addressing requirements would supply DOD with sources of meaningful information that would enable the department to develop realistic, detailed, and informed transition plans and time frames.

Conclusions

While DOD's current IPv6 transition effort is showing progress, the department has not completed most of OMB's planning requirements. Notable signs of progress include the appointment of an official to lead the initiative and the development of an overarching strategy document that outlines the transition's scope and goals. Nevertheless, DOD had not completed an inventory of IP-compliant technologies, a cost estimate, or a risk analysis before moving ahead with developing its February 2019 guidance and working against the guidance's list of transition activities. The lack of an inventory is problematic due to the role that it should play in developing transition requirements. In addition, without a cost estimate to guide decision-makers, DOD's current IPv6 transition plans could be based on unrealistic assumptions about costs and resource demands. Further, by moving forward without a risk analysis, DOD increases the probability that it is not proactively managing potential threats that could either disrupt the transition or introduce new IT security vulnerabilities. Completing these longstanding planning requirements would enable DOD to develop realistic plans with accurate transition requirements and proactive risk mitigation strategies, among other things.

Recommendations for Executive Action

We are making three recommendations to DOD.

The Secretary of Defense should direct the DOD CIO to complete a department-wide inventory of existing IP-compliant devices and technologies to help with planning efforts and requirements development for the transition to IPv6. (Recommendation 1)

The Secretary of Defense should direct the DOD CIO to develop a cost estimate as described in OMB memorandum M-05-22 for the department's transition to IPv6. (Recommendation 2)

The Secretary of Defense should direct the DOD CIO to develop a risk analysis as described in OMB memorandum M-05-22 for the department's transition to IPv6. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD and OMB for review and comment. In response, DOD agreed with two recommendations and disagreed with one recommendation that we made to the department. OMB did not state whether it agreed or disagreed with the report's findings.

In written comments, DOD stated that it agreed with our recommendations to develop a cost estimate and risk analysis for the department's transition to IPv6 (Recommendations 2 and 3). The department said that it plans to complete both the cost estimate and the risk analysis by the end of May 2020.

However, DOD stated that it did not agree with our recommendation to complete a department-wide inventory of existing IP-compliant devices and technologies (Recommendation 1). Specifically, the department referred to the draft IPv6 guidance that OMB developed in March 2020, stating that the draft guidance will rescind OMB's fiscal year 2005 IPv6 guidance, which includes the inventory requirement. DOD also said that creating such an inventory would be impractical given the department's size. It added that it has been mitigating the risk of not having an inventory by only acquiring IPv6-capable devices since December 2009.

We acknowledge that OMB's March 2020 draft IPv6 guidance, once finalized, would rescind its fiscal year 2005 IPv6 guidance. However, the draft guidance focuses on completing the operational deployments of IPv6, not on the initial key transition step of completing an inventory, as required in the 2005 guidance.

The draft guidance also requests information on agencies' completion of certain milestones using the percentage of IP-enabled devices that are IPv6-only as the metric. DOD's completed inventory would be essential to accurately responding to OMB's draft requirement. In addition, NIST's current IPv6 transition guidance cites an inventory of IP devices as a key step in transitioning to IPv6 since such information would help identify requirements for transitioning, including which assets would transition and what security controls would be needed. As DOD has acknowledged, however, it has not yet completed an inventory. Accordingly, we believe that our recommendation that DOD complete a department-wide inventory of its existing IP-compliant devices and technologies is warranted.

In addition, DOD provided a technical comment, which we incorporated as appropriate. DOD's comments are reprinted in appendix II.

In comments provided via email on May 8, 2020, an Associate General Counsel in OMB's Office of General Counsel expressed OMB's appreciation for the opportunity to review and comment on our draft report. The official did not state whether OMB agreed or disagreed with the report's findings. OMB also provided a technical comment, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of DOD, and the Acting Director of OMB. In addition, the report is available at no change on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-6240 or dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Vijay A. D'Souza

Vijay A. D'Souza
Director, Information Technology
and Cybersecurity

List of Committees

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard C. Shelby
Chairman
The Honorable Dick Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Pete Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: DOD's IPv6 Implementation and Planning Activities

In February 2019, the Department of Defense's (DOD) Chief Information Officer (CIO) released "Internet Protocol Version 6 Implementation Direction and Guidance," a memorandum containing guidance and a list of required implementation and planning activities for the department's transition to Internet Protocol version 6 (IPv6). For each activity, the memorandum included information such as the component or office responsible for completing the work and a description of the work to be completed. Out of 35 total activities, seven were completed and 12 were past due as of March 2020.[1] One key contributing factor behind the activities' unrealistic deadlines was that the department developed this list of required activities without having completed key planning efforts, such as an inventory of IP-compliant devices and technologies, a cost estimate, or a risk analysis. Table 4 shows the status of the completion of the required transition activities as called for in the department's guidance.

[1] Of the 12 required activities that were past due as of March 2020, one was due in May 2019, one was due in June 2019, three were due in September 2019, six were due in December 2019, and one did not have a specific due date in the February 2019 memorandum, but was due during fiscal year 2019. Of the 16 remaining activities that were neither completed or past due, seven were not due before March 2020, seven did not have specific due dates, and two were canceled.

Table 4: The Department of Defense's (DOD) Status In Completing Its Internet Protocol version 6 (IPv6) Transition Activities as Listed in DOD's February 2019 IPv6 Implementation Direction and Guidance Memorandum, as of March 2020

Activity number[a]	Activity description	Component or office responsible	Completed	Not completed and past due	Not completed and not yet due	Not completed and no due date[b]	Canceled
1	Lead development of a DOD IPv6 Strategy for Joint Information Environment Executive Committee endorsement and DOD CIO signature.	DOD Chief Information Officer (CIO)	X	—	—	—	—
2	Determine DOD cybersecurity architecture and posture impacts using the DOD Cybersecurity Analysis and Review process.	DOD CIO	—	X	—	—	—
3	Integrate IPv6 considerations into the DOD Cyber Security Reference Architecture.	DOD CIO	—	—	X	—	—
4	Integrate IPv6 considerations into the DOD Core and Component Enterprise Data Center Reference Architectures.	DOD CIO	—	X	—	—	—
5	Determine U.S. interagency collaboration and cybersecurity information sharing (e.g., best practices, product assessments, and roadmaps) opportunities.	DOD CIO	X	—	—	—	—
6	Establish supplemental guidance for acquisition of IPv6-capable products in the Defense Acquisition Guidebook and DOD Information Network Capabilities Requirements document.	DOD CIO	—	X	—	—	—
7	Propose Defense Federal Acquisition Regulation Supplement guidance for the acquisition of IPv6-capable products.	DOD CIO	—	—	—	—	X
8	Designate a DISA IPv6 lead and establish a virtual program management office.	Defense Information Systems Agency (DISA)	X	—	—	—	—

Activity number[a]	Activity description	Component or office responsible	Completed	Not completed and past due	Not completed and not yet due	Not completed and no due date[b]	Canceled
9	Develop a Defense Information Systems Network (DISN) IPv6 Implementation Plan for fiscal years 2019-2023 within 90 days of the memo. Include required actions with proposed schedule, costs, milestones, and critical dependencies to deliver reliable and secure IPv6 services within the DISN, and in support of internet-based capabilities.	DISA	—	X	—	—	—
10	Provide an electronic means for DOD components to submit, manage, and de-conflict IPv6 priorities, plans, and requirements.	DISA	X	—	—	—	—
11	Provide on demand IPv6 familiarization training and assess commercial advanced training resources for network engineers and cybersecurity personnel.	DISA	X	—	—	—	—
12	Provide on demand advanced IPv6 training resources for network engineers and cybersecurity personnel.	DISA	X	—	—	—	—
13	Update and maintain IPv6 standards and implementation profiles in the Defense Information Technology Standards Registry.	DISA	—	X	—	—	—
14	Verify the Internet Access Point systems provide equivalent IPv4/IPv6 capabilities and resolve gaps. Provide plans of action and milestones for any unresolved gaps.	DISA	—	X	—	—	—
15	Verify the Secure Cloud Computing Architecture provides equivalent IPv4/IPv6 capabilities and resolve gaps. Provide plans of action and milestones for any unresolved gaps.	DISA	—	X	—	—	—
16	Verify that DOD Public Key Infrastructure provides essential IPv6 functionality (e.g., Online Certificate Status Protocol responder) for external facing services and resolve gaps.	DISA	—	—	X	—	—

Activity number[a]	Activity description	Component or office responsible	Completed	Not completed and past due	Not completed and not yet due	Not completed and no due date[b]	Canceled
17	Develop test processes and methodologies to assess compliance with DOD Information Network Capabilities Requirements-related IPv6 requirements for Approved Products List testing.	DISA	—	—	X	—	—
18	Verify current Security Technical Implementation Guides/Security Requirements Guides are consistent with IPv6-related cybersecurity requirements.	DISA	—	X	—	—	—
19	Verify milCloud 2.0 provides equivalent IPv4/IPv6 capabilities and resolve gaps. Provide plans of action and milestones for any unresolved gaps.	DISA	—	—	X	—	—
20	Provide IPv6-enabled Cyber Security Range services.	DISA	X	—	—	—	—
21	Provide Domain Name System services to IPv6-only users/networks for the .mil generic top-level domain.	DISA	—	—	X	—	—
22	Provide IPv6-enabled unclassified milCloud 2.0 services.	DISA	—	—	X	—	—
23	Assist DISA in verifying that Internet Access Point systems provide equivalent IPv4/IPv6 capabilities.	National Security Agency	—	—	—	X	—
24	Provide cybersecurity guidance in support of DOD IPv6 deployments as needed.	National Security Agency	—	—	—	X	—
25	Provide technical input to updates and maintenance of IPv6 standards registries as needed.	National Security Agency	—	—	—	X	—
26	Assist DISA with IPv6 training identification, assessment, and development.	National Security Agency	—	—	—	X	—
27	Provide IPv4/IPv6 Attack Sensing and Warning, and Cyber Threat Intelligence.	National Security Agency	—	—	X	—	—
28	Establish requirements for IPv6 training and tools for Cyber Mission Force personnel.	United States Cyber Command	—	—	—	—	X

Activity number[a]	Activity description	Component or office responsible	Completed	Not completed and past due	Not completed and not yet due	Not completed and no due date[b]	Canceled
29	IPv6-enable all commercially hosted public facing unrestricted services. Monthly reporting will be accomplished with instructions to follow.	DOD components and the United States Coast Guard	—	X	—	—	—
30	Identify DOD hosted public facing unrestricted services. Include planned disposition (e.g., retain in place, transition to cloud by date, retire by date, etc.) and dependencies to enable IPv6.	DOD components and the United States Coast Guard	—	X	—	—	—
31	Ensure new cybersecurity products provide equivalent IPv4/IPv6 capabilities.	DOD components and the United States Coast Guard	—	—	—	X	—
32	Verify existing cybersecurity systems provide equivalent IPv4/IPv6 capabilities and resolve gaps. Provide plans of action and milestones for any unresolved gaps.	DOD components and the United States Coast Guard	—	X	—	—	—
33	Ensure all applications and systems migrated to commercially hosted cloud services are IPv6-only capable. If provider limitations exist, obtain a resolution roadmap.	DOD components and the United States Coast Guard	—	—	—	X	—
34	Monitor and report mission partner IPv6 plans and status on a semi-annual basis, or earlier as needed. Use existing engagement forums where possible (e.g., Combined Communications-Electronics Board).	DOD components and the United States Coast Guard	—	—	—	X	—
35	Identify any additional resources required to support actions directed in this guidance and incorporate into Program Objective Memorandum fiscal year 2021 submissions.	DOD components and the United States Coast Guard	—	X	—	—	—
Totals	**—**	**—**	**7**	**12**	**7**	**7**	**2**

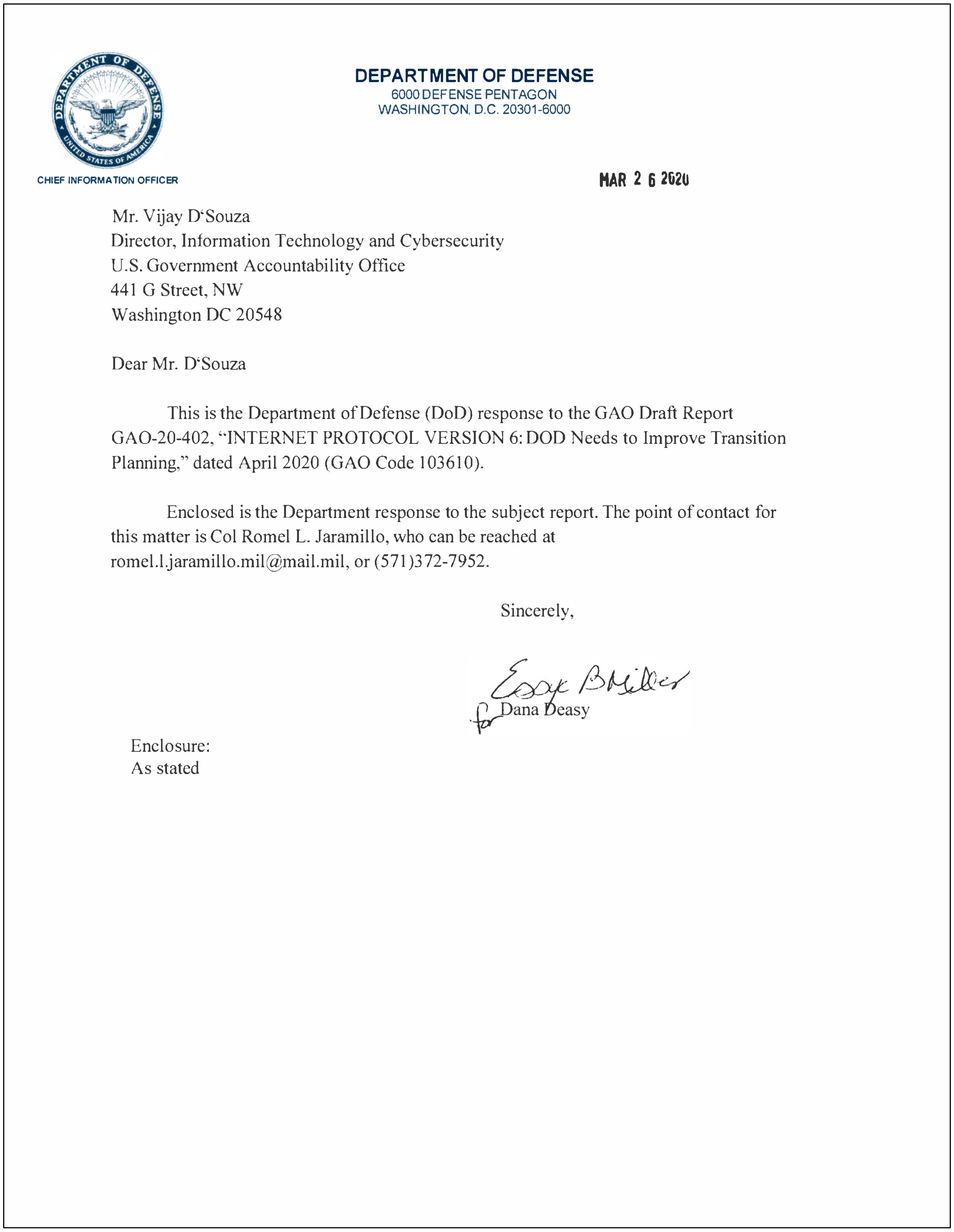
Legend: X = the activity's status as of March 2020; — = not applicable

Source: GAO analysis of DOD documentation. | GAO-20-402

[a] We assigned the values in the "Activity number" column by numbering each activity sequentially.

[b] According to officials leading the IPv6 transition, the activities without due dates are considered to be ongoing tasks.

Appendix II: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MAR 2 6 2020

Mr. Vijay D'Souza
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. D'Souza

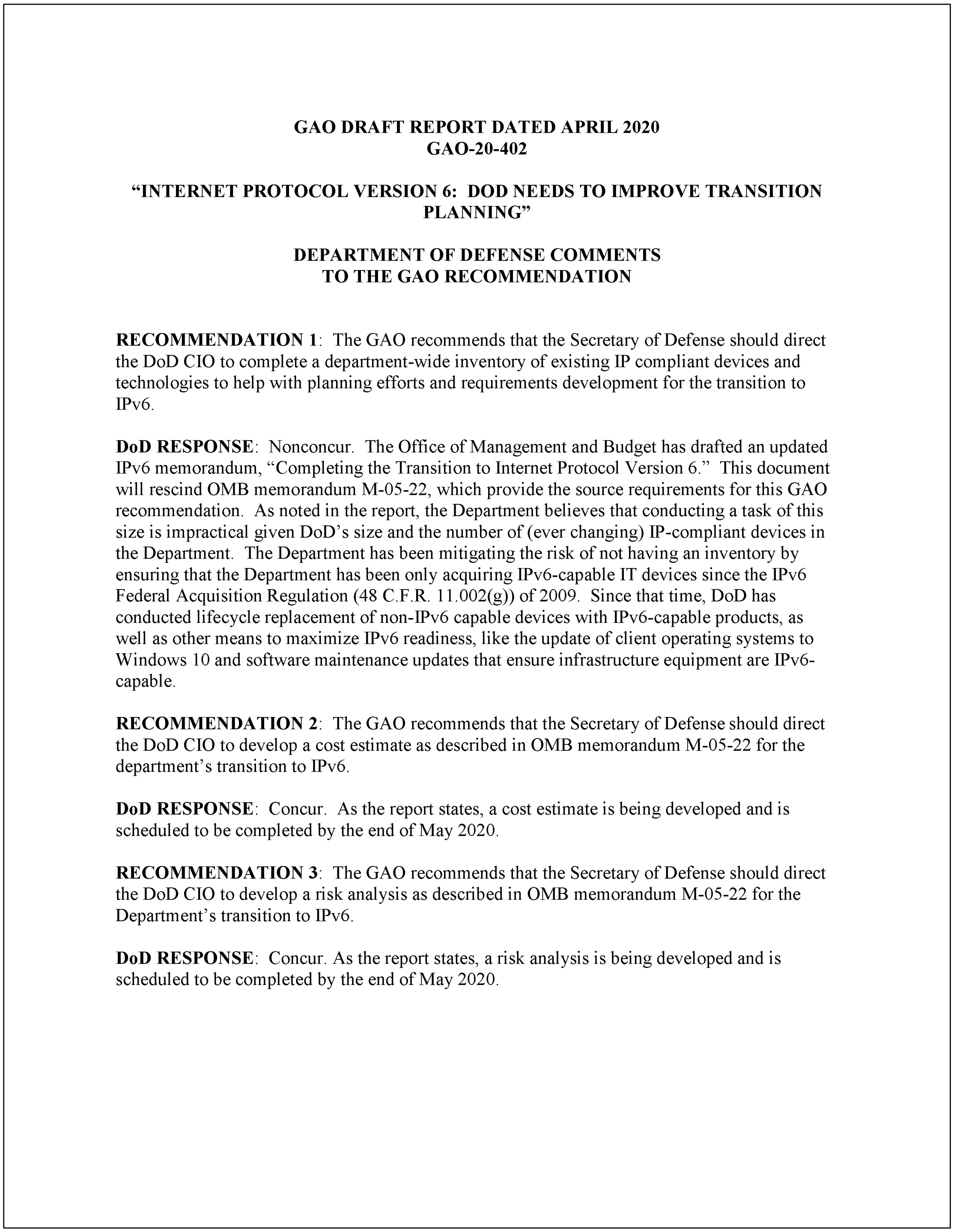
This is the Department of Defense (DoD) response to the GAO Draft Report GAO-20-402, "INTERNET PROTOCOL VERSION 6: DOD Needs to Improve Transition Planning," dated April 2020 (GAO Code 103610).

Enclosed is the Department response to the subject report. The point of contact for this matter is Col Romel L. Jaramillo, who can be reached at romel.l.jaramillo.mil@mail.mil, or (571)372-7952.

Sincerely,

Essye B Miller
for Dana Deasy

Enclosure:
As stated



GAO DRAFT REPORT DATED APRIL 2020
GAO-20-402

"INTERNET PROTOCOL VERSION 6: DOD NEEDS TO IMPROVE TRANSITION PLANNING"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should direct the DoD CIO to complete a department-wide inventory of existing IP compliant devices and technologies to help with planning efforts and requirements development for the transition to IPv6.

DoD RESPONSE: Nonconcur. The Office of Management and Budget has drafted an updated IPv6 memorandum, "Completing the Transition to Internet Protocol Version 6." This document will rescind OMB memorandum M-05-22, which provide the source requirements for this GAO recommendation. As noted in the report, the Department believes that conducting a task of this size is impractical given DoD's size and the number of (ever changing) IP-compliant devices in the Department. The Department has been mitigating the risk of not having an inventory by ensuring that the Department has been only acquiring IPv6-capable IT devices since the IPv6 Federal Acquisition Regulation (48 C.F.R. 11.002(g)) of 2009. Since that time, DoD has conducted lifecycle replacement of non-IPv6 capable devices with IPv6-capable products, as well as other means to maximize IPv6 readiness, like the update of client operating systems to Windows 10 and software maintenance updates that ensure infrastructure equipment are IPv6-capable.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should direct the DoD CIO to develop a cost estimate as described in OMB memorandum M-05-22 for the department's transition to IPv6.

DoD RESPONSE: Concur. As the report states, a cost estimate is being developed and is scheduled to be completed by the end of May 2020.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should direct the DoD CIO to develop a risk analysis as described in OMB memorandum M-05-22 for the Department's transition to IPv6.

DoD RESPONSE: Concur. As the report states, a risk analysis is being developed and is scheduled to be completed by the end of May 2020.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov

Staff Acknowledgments

In addition to the contact named above, Larry Crosland (Assistant Director), Meredith Raymond (Analyst in Charge), Amy Apostol, Chris Businsky, West Coile, Kristi Dorsey, Vernetta Marquis, and Evan Rapson made key contributions to this report.

(103610)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548