RED HAT

The world's leading provider of open source, enterprise IT products and services

Response of
Red Hat, Inc. ("Red Hat")

to the Request for Comments regarding
Draft Report to the President on Federal IT Modernization
(the "Report")

Published at: ***https://itmodernization.cio.gov/***

September 20, 2017

Red Hat appreciates the opportunity to provide comments on the above-referenced matter. We commend the development and release for comment of this draft Report to modernize the security and functionality of Federal IT, allow the Federal Government to improve service delivery and focus effort and resources on what is most important to customers of Government services.

Red Hat is a leading provider of open source software solutions, using a community-powered approach to deliver resilient and high-performing cloud, Linux, middleware, storage and virtualization technologies. An S&P 500 index member, Red Hat provides high-quality, trusted and affordable technology solutions that are found throughout mission-critical systems in the financial, transportation, telecommunication and government (civilian and defense) sectors in the United States and around the world. Red Hat is recognized as one of the world's most innovative companies.[1]

As a leader in catalyzing IT modernization, we are especially pleased to see the Administration focused on a forward-looking policy. We offer the following major attributes that we believe are missing from the targeted vision in the draft Report:

- Open source technology drives IT modernization and should continue to be considered alongside proprietary solutions and the default for use in U.S. government modernization efforts.

- IT modernization efforts must preserve future ability to shift cloud workloads, when necessary.

- Open standards should be encouraged to enable interoperability, prevent vendor lock-in and mitigate security risk or functionality limits when software is orphaned by developers.

- IT solutions deployed by the U.S. government should be commercially-supported in order to ensure effective and efficient evolution of functionality and security.

---

[1] *See* Forbes, "The World's Most Innovative Companies", 2017, found at: https://www.forbes.com/companies/red-hat/.

The Report correctly focuses on IT modernization through agile, commoditized, modular approaches -- to enable faster deployment of innovative solutions.

IT modernization or 'digital transformation' should enable new types of innovation and creativity in a particular domain, rather than simply incrementally enhancing and supporting the traditional methods.

According to Gartner[2], digital transformation is about the use of technologies to change a business model to provide new revenue and value-producing opportunities. In the government, it is fundamentally about enabling government to operate like an innovative and efficient digital 'business' for delivering citizen services.

To accelerate deployment of innovative and, more importantly, transformational solutions, we support that the Report highlights the need for: agile, commoditized, modular approaches to enterprise and end-user Federal IT. The Report's outline of an agile process for updating policies and reference architectures should guide agencies to more rapidly leverage American innovation.

Open Source drives IT modernization.

The Report's vision does not adequately recognize the essential role of open source software, which has become central to IT modernization efforts in the *commercial* sector:

"Enterprise-grade open source software has become ubiquitous across enterprise IT architectures ... used by most, if not all, enterprises to support a broad range of mission-critical applications and business services. … [open source] often provide the basis of critical new technologies … open source is more likely to lead the charge toward innovation"[3]

IDC research finds that the vast majority of enterprises currently utilize open source software in a variety of ways, including for mission-critical enterprise initiatives. Specifically, many common components of enterprise IT systems, including network infrastructure, big data storage, cloud platforms and management tools, firewalls, mobile devices and desk phones (just to name a few) are open source software in commercial products and services.

Also, enterprises rely on open source software embedded in commercial UNIX, Linux and Windows servers. Much of modern application development is taking place on open source tools and frameworks such as PHP, Perl, Ruby, or Node.js. Even Windows developers rely on the open source .NET Core Framework.[4]

Federal IT policy, for over a decade, has recognized this important role of open source.[5] We strongly

---

[2] Gartner IT Glossary, found at: https://research.gartner.com/definition-whatis-digitalization.
[3] IDC report, *Enterprise-Grade Open Source: An Imperative for Modern IT,* April 2016.
[4] IDC report, April 2016.
[5] *See, e.g.,* "U.S. report highlights positive elements of government open source adoption", October 9, 2015, found at: https://opensource.com/government/15/10/us-dhs-issue%C2%Ads-Report. "The Office of Management and Budget (OMB) has released a federal government-wide memo that acquisition rules apply to all software, whether it is proprietary or Open Source Software [citing the July 2004 OMB Software Acquisition memo] placing OSS on an equal footing. The Department of Defense (DoD) has a more detailed OSS policy that makes it clear that OSS is acceptable and must be considered, as well as supporting frequently asked questions (FAQs) and best practices documents."

urge that the updated Report include references to these policies[6] and also support incentives for consideration of open source solutions for modernization. Specifically, a 'default to open' approach[7] should be enumerated to harness the community-powered innovation of open source software.

We share the Report's view that Federal agencies have been stymied in IT modernization attempts because of a variety of factors, including resource prioritization, vendor lock-in, the ability to procure services quickly and technical issues. Open source solutions can help mitigate each of these.

Preventing 'Cloud Lock-In' is also critical for IT modernization strategies.

There has been significant guidance about the adoption of cloud (cloud first) for government use,[8] [9] [10] and the Report rightly identifies the use of trusted commercial cloud platforms where appropriate. However, little has been said about the need to have an appropriate *exit plan* for shifting use of cloud services, when necessary - whether it be to bring workloads back into government data centers or to realize the financial value of moving workloads to more cost-effective cloud offerings.

The Report should advise agencies making forays into cloud computing that a "cloud exit strategy" must be a key component of IT modernization. Avoiding the pitfalls of cloud lock-in will ensure that efforts to enable the next generation of government IT do not ultimately lead to a future problem of lock-in to 'legacy clouds' that prove more expensive or less effective than available alternatives.

Moreover, the Report should recognize the various use cases that drive cloud adoption. Private clouds offer control, predictability, and a clear migration path that can be attractive to government departments. Public clouds offer economies of scale, availability, and potential ease of use. "Hybrid clouds" promise the best of both public and private cloud computing, coupling the power and elasticity of public clouds with the security and control of private. These solutions require a new level of transparency, coordination, and flexibility that can be very difficult to muster. When developing a cloud strategy, this difficulty makes it tempting to focus solely on either public or private providers. In truth, the vast majority of agencies, reflecting trends in the commercial sector, will opt for a hybrid model, and government policies, procedures, and recommendations should anticipate this.

Open source software is at the heart of cloud computing. Public clouds are built on mountains of open source software, and the most innovative applications of cloud computing are on open source platforms. This means that lessons learned, best practices and hard-earned experience of cloud customers and providers are often embedded in open source projects. From foundational technology like the Linux operating system to high-order cloud tools like OpenStack private cloud platform and OpenShift platform-as-a-service tool, open source enables cloud innovation and flexibility.

---

[6] *See, e.g.,* OMB, "M-04-16, Software Acquisition", July 1, 2004, found at: https://www.whitehouse.gov/omb/memoranda_fy04_m04-16; U.S. Department of Defense, Office of the Chief Information Officer, "Memorandum Clarifying Guidance Regarding Open Source Software (OSS)", October 16, 2009, found at: http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf; OMB, "Memorandum Technology Neutrality", January 7, 2011, found at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf.

[7] *See* "U.S. Digital Services and Playbook: "Default to Open"", August 20, 2014, found at: https://opensource.com/government/14/8/us-digital-services-and-playbook-default-open.

[8] *See* "FEDRamp Tips" https://www.fedramp.gov/resources/fedramp-tips-cues/

[9] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_19_1.pdf

[10] See "Federal Cloud Computing Strategy" https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

Open Standards are essential.

The Report is notably silent on the essential role of open standards in IT modernization. Use of open standards in software interoperability promotes a level playing field between software vendors. In data, it affords greater portability among vendors and applications. In both cases, it creates an environment where innovation can progress without future technology lock-in.

Open standards and *fully disclosed application interfaces* -- central to interoperability and portability of software and data -- are both very important to realize the full value of cloud computing. The Internet itself would never have been possible without the TCP/IP networking standards, which allow any and all computers to connect to each other, much like any telephone in the world is capable of connecting to any other telephone. With the multitude of vendors offering cloud platforms, open standards and fully disclosed interfaces will continue to grow in importance as agencies turn to cloud services.

Differences between vendors and their cloud platforms in any of these areas can have significant effects on the overall interoperability and portability of *all* the cloud solutions on that platform. By having common, well-defined standards across multiple cloud platforms enterprises will have better options and more choices in meeting their needs as technology and markets evolve.

IT systems should be commercially supported in order to ensure effective and efficient support, functionality and security.

Current Federal policies have a long-standing policy to avoid government-off-the-shelf solutions (GOTS) and custom approaches. Yet, many of the legacy systems that are most at risk today either have no existing vendor to support and update them, or for all practical purposes are solely government-purposed IT systems.

Well developed existing USG policy (*e.g.*, Shared Services Strategy) emphasizes the key role of *commercial* organizations in providing IT shared service to agencies, with growing use of commodity IT, modularity and "open solutions," while reducing duplicative support.

Similarly, the long-standing approach of Circular A-130 directs agencies to give priority as a first step "to use of available and suitable existing Federal information systems, software, technologies, and shared services and/or information processing facilities." The policy emphasizes in its latest version that "all IT systems and services operate only vendor-supported solutions." That key principle should be reflected in the updated Report.

One of the benefits of road-tested, commercially-supported open source is that it is commercial-off-the-shelf (COTS). It can be supported by a variety of vendors and offers an agile, reusable, modular approach to agencies.[11]

---

[11] *See, e.g.,* "U.S. report highlights positive elements of government open source adoption", 09 October 2015, found at: https://opensource.com/government/15/10/us-dhs-issue%C2%Ads-report. *See, also,* U.S. Department of Homeland Security, *Open Source Software in Government: Challenges and Opportunities*, 2013, found at: https://www.dhs.gov/sites/default/files/publications/Open%20Source%20Software%20in%20Government%20%E2%80%93%20Challenges%20and%20Opportunities_Final.pdf

A recent Report by the U.S. Department of Homeland Security brings this point home. It found that "a [community open source] project fork is typically far more expensive for the government to maintain in the long term because the government must pay for every change (instead of sharing sustainment costs with others), and the fork is also cut off from the future innovations in the main open source project." This finding by DHS in its Report is also a key theme of the tenets of open source development literature which "strongly recommends avoiding creating a project fork wherever possible". Yet agencies and its contractors often unnecessarily encourage creating project forks. Addressing this issue clearly in the draft policy would be an important step forward.

The U.S. government has long recognized that open source software is, in fact, commercial software. An essential corollary is that, regardless of whether the software is proprietary, agencies must have a support and maintenance plan. As the US Department of Defense succinctly put it:

"The use of any software without appropriate maintenance and support presents an information assurance risk. Before approving the use of software (including open source software), system/program managers, and ultimately Designated Approving Authorities (DAAs), must ensure that the plan for software support (e.g., commercial or Government program office support) is adequate for mission need."[12]

Conclusion

The Report is, in many ways, forward-looking, and will improve with additional points shared in this paper. Today, the focus is not on 'whether' open source should be used (which has been articulated in U.S. government policy for years), but rather the 'how' of doing it. Effective utilization of commercially-supported open source software and open standards, both in government and the commercial sector, is essential to meaningful IT modernization. The revised Report should recognize this fact, build on existing policies and point to its key role in private sector digital transformation.

It is important that IT modernization efforts do not create 'cloud lock-in' problems in the future, promote GOTS over COTS, create 'forks' in open source projects, or rely on 'go it alone' support.

Once, again, we appreciate this opportunity to provide our comments on this draft Report. Please do not hesitate to contact us if we can provide further information or answer questions.

Contact:

Mark Bohannon
Vice President, Global Public Policy
and Government Affairs
Red Hat
markb@redhat.com

Adam Clater
Chief Architect, North American Public Sector
Red Hat
adam@redhat.com

[12] U.S. Department of Defense, "Clarifying Guidance Regarding Open Source Software (OSS)", Oct. 16, 2009, found at: http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf.