CHAPTER

A case for open source

3

INFORMATION IN THIS CHAPTER:

- Introduction
- Open Source Software and the Federal Government
- Open Source Software Adoption Challenges: Acquisition and Security
- Open Source Software and Federal Cloud Computing

INTRODUCTION

Open source software (OSS)[1] and cloud computing are distinctly different concepts that have independently grown in use, both in the public and private sectors, but have each faced adoption challenges by federal agencies. Both OSS[2] and cloud computing individually offer potential benefits for federal agencies to improve their efficiency, agility, and innovation, by enabling them to be more responsive to new or changing requirements in their missions and business operations. OSS improves the way the federal government develops and also distributes software[3] and provides an opportunity to reduce costs through the

[1]From Wennergren, D. Clarifying Guidance Regarding Open Source Software (OSS). Washington: US Department of Defense; 2009. "*Open software is software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software*."

[2]Some examples include operating systems (*Linux, Solaris*), web/middlewares (*Apache, JBoss Glassfish*), databases (*MySQLP, PostgreSQL*), applications (*Firefox, Thunderbird*), and programming languages (*Perl, Python, PHP*).

[3]From the Office of Management and Budget (OMB). OMB Memorandum 16−21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. Washington, DC: Executive Office of the President, Office of Management and Budget; 2016. "*Accessible, buildable, version-controlled repositories for the storage, discussion, and modification of custom-developed code are critical to both the Government-wide reuse*."

Federal Cloud Computing. DOI: http://dx.doi.org/10.1016/B978-0-12-809710-6.00003-2

reuse of existing source code,[4] whereas cloud computing improves the utilization of resources and enables a faster service delivery.

In this chapter, issues faced by OSS in the federal government will be discussed, in addition to the relationship of the federal government's adoption of cloud computing technologies.[5] However, this chapter does not present a differentiation of OSS from proprietary software,[6] rather focuses on highlighting the importance of the federal government's experience with OSS in the adoption of cloud computing.

Over the years, the private sector[7] has encouraged the federal government to consider OSS by making a case that it offers an acceptable alternative to proprietary commercial off-the-shelf (COTS) software. Regardless of the potential cost-saving benefits of OSS, federal agencies have historically approached it with cautious interest. Although, there are other potential issues in transitioning from an existing proprietary software, beyond cost. These issues include, a limited in-house skillset for OSS developers within the federal workforce, a lack of knowledge regarding procurement or licensing, and the misinterpretation of acquisition and security policies and guidance. Although some of the challenges and concerns have limited or slowed a broader-scale adoption of OSS, federal agencies have become more familiar with OSS and the marketplace expansion of available products and services, having made considerations for OSS as a viable alternative to enterprise-wide COTS software. This renewed shift to move toward OSS is also being driven by initiatives such as the 18F[8] and the US Digital Service,[9] and the publication of the guidance such as the Digital Services Playbook, which urges federal agencies to "consider using open source, cloud based, and commodity solutions across the technology stack" [1].

---

[4]From the Office of Management and Budget (OMB). OMB Memorandum 16−21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. Washington, DC: Executive Office of the President, Office of Management and Budget; 2016. "*Enhanced reuse of custom-developed code across the Federal Government can have significant benefits for American taxpayers, including decreasing duplicative costs for the same code and reducing Federal vendor lock-in.*"

[5]*NASA Nebula Cloud Computing Platform*. Available from: https://open.nasa.gov/blog/nebula-nasa-and-openstack/.

[6]From the Office of Management and Budget (OMB). OMB Memorandum 16−21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. Washington, DC: Executive Office of the President, Office of Management and Budget; 2016. "*Software with intellectual property rights that are retained exclusively by a rights holder (e.g., an individual or a company).*"

[7]For example, the Open Source for America (OSfA) is an effort to raise awareness in the federal government about the benefits of open source software. Available from: http://opensourceforamerica.org/.

[8]18F is a digital services delivery team within the General Services Administration that develops in-house digital solutions to help agencies meet the needs of the citizens and businesses it serves. Available from: https://github.com/18F/open-source-policy/blob/master/policy.md.

[9]*The US Digital Service*. Available from: https://www.whitehouse.gov/digital/united-states-digital-service.

NOTE

Example cases where OSS was identified as a viable option to support federal government programs:

- In May 2011, the US Department of Veterans Affair (VA) CIO stated to avoid costs, and to find a way to involve the private sector in modernizing Veterans Integrated System Technology Architecture (VistA; *electronic medical records system*), the VA turned to open source [2]. In response, the VA launched the Open Source Electronic Health Record Alliance (OSEHRA) in August 2012 "as a central governing body of a new open source Electronic Health Record (EHR) community" [3].
- In January 2012, the National Aeronautics and Space Administration (NASA) launched a new website, the NASA Open Government Initiative,[10] to expand the agency's OSS development. The NASA Open Government co-lead stated: "We believe tomorrow's space and science systems will be built in the open, and that code.nasa.gov will play a big part in getting us there" [4].

Interoperability, portability, and security standards[11] have already been identified[12] as critical barriers for cloud adoption within the federal government. OSS facilitates overcoming standards obstacles through the development and implementation of open standards.[13] OSS communities support standards development through the "shared" development and industry implementation of open standards.[14] In some instances, the federal government's experience with standards development has enabled the acceptance and use of open standards-based, open source technologies and platforms.

[10]*NASA Open Government Initiative. Available from*: http://www.nasa.gov/open/.

[11]Standards were discussed in detail in Chapter 2, Cloud Computing Standards.

[12]From Kundra, V. Federal Cloud Computing Strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *Standards will be critical for the successful adoption and delivery of cloud computing, both within the public sector and more broadly. Standards are also critical to ensure clouds have an interoperable platform so that services provided by different providers can work together, regardless of whether they are provided using public, private, community, or a hybrid delivery model.*

[13]From the Office of Management and Budget (OMB). OMB Memorandum 16−21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. Washington, DC: Executive Office of the President, Office of Management and Budget; 2016. "*Regardless of the specific solution selected, all software procurements and Government software development projects should consider utilizing open standards whenever practicable in order to increase the interoperability of all Government software solutions. Open standards enable software to be used by anyone at any time, and can spur innovation and growth regardless of the technology used for implementation—be it proprietary, mixed source, or OSS in nature*."

[14]Open standards, in general terms, is a technical specification that is developed openly (participation and publication) and is vendor neutral with limited cost (or free availability) to implementers.

TIP

OSS also enables agile software development[15] where the federal agencies can more rapidly deploy technologies and capabilities; however, for agile software development to be viable across the government, supporting government-wide agile acquisition guidance needs to be established. The *TechFAR Handbook*,[16] consistent with the Federal Acquisition Regulation (FAR),[17] was published to guide federal agencies by explicitly encouraging the use of agile software development and procure development services of modern software development techniques used in the private sector through modular contracting practices.[18]

Many modernization projects have identified the use of OSS as a more economical value for the federal government. Through the use of smaller, agile procurements, federal agencies are achieving a higher yield and greater return on investment (ROI) compared to slower, inefficient long-term investments that use traditional procurement methods that tend to be outpaced by private sector innovations due to lengthy development cycles. Additionally, federal agencies are required to consider multiple factors when defining the overall business case[19] for an Information Technology (IT) investment.[20] Some factors that must be considered as part of the IT investment decision-making process[21] includes the total cost of ownership (TCO) and lifecycle maintenance costs, the costs associated with mitigating security risks, and the security and privacy of data [5]. OSS also requires transitioning to a subscription-based model, thereby reducing the burden for federal agencies to invest in upfront costs, which lock them into capital expenses that may be unrecoverable if the requirements change or a program is canceled or rescoped.

[15]From TechFAR Handbook for Procuring Digital Services for Using Agile Processes [Internet]. Washington, DC: The White House [cited January 26, 2016]. Available from: https://playbook.cio.gov/assets/TechFAR%20Handbook_2014-08-07.pdf. "*Agile software development is a method of software development that is based on iterative and incremental processes and collaboration among a team.*"

[16]From TechFAR Handbook for Procuring Digital Services for Using Agile Processes [Internet]. Washington, DC: The White House [cited January 26, 2016]. <https://playbook.cio.gov/assets/TechFAR%20Handbook_2014-08-07.pdf>. TechFAR Handbook "*highlights the flexibilities in the Federal Acquisition Regulation (FAR) that can help agencies implement 'plays' from the Digital Services Playbook that would be accomplished with acquisition support—with a particular focus on how to use contractors to support an iterative, customer-driven software development process, as is routinely done in the private sector.*"

[17]From TechFAR Handbook for Procuring Digital Services for Using Agile Processes [Internet]. Washington, DC: The White House [cited January 26, 2016]. <https://playbook.cio.gov/assets/TechFAR%20Handbook_2014-08-07.pdf>. "*The FAR and each agency's supplement to the FAR, set forth Government-wide overarching Federal procurement principles, policies, processes and procedures on procuring goods and services, including IT and digital services.*"

[18]*Contracting Guidance to Support Modular Development*. Available from: https://www.whitehouse.gov/sites/default/files/omb/procurement/guidance/modular-approaches-for-information-technology.pdf.

[19]Guidance on exhibit 300A (business cases). Available from: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy13_guidance_for_exhibit_300_a-b_20110715.pdf.

[20]From the Office of Management and Budget (OMB). OMB Circular A-11, Planning, Budgeting, and Acquisition of Capital Assets. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. "*Agencies should make security's role explicit in information technology investments and capital programming*."

[21]The Capital Planning and Investment Control Process (CPIC) includes a requirement to integrate IT security into the IT investment evaluation criteria. Available from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-65.pdf.

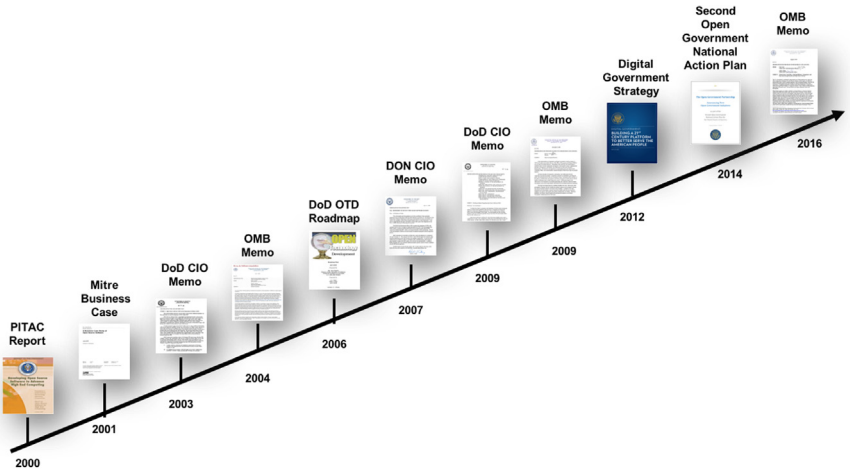

FIGURE 3.1

US Government OSS Policy Framework.

OPEN SOURCE SOFTWARE AND THE FEDERAL GOVERNMENT

The federal government's use of OSS has its beginning in the 1990s.[22] During this period, OSS was used primarily within the research and scientific community where collaboration and information sharing was a cultural norm. However, it was not until 2000 that federal agencies began to seriously consider the use of OSS as a model for accelerating innovation within the federal government. As illustrated in Fig. 3.1, the federal government has developed a list of OSS-related studies, policies, and guidelines that have formed the basis for the policy framework that has guided the adoption of OSS. This framework tackles critical issues that have inhibited the federal government from attaining the full benefits offered by OSS. Although gaps[23] still exist in specific guidelines relating to the evaluation, contribution, and sharing of OSS, the policy framework serves as a foundation for guiding federal agencies in the use of OSS. In this section, we will explore the policy framework with the objective of describing how the current policy framework has led to the broader use of OSS across the federal government, and more importantly how this framework has enabled the federal government's adoption of cloud computing by overcoming the challenges with acquisition and security that will be discussed in detail in the next section.

[22]*Timeline: A History of Open Source in Government.* Available from: http://gov-oss.org/.
[23]Lessons Learned: Roadblocks and Opportunities for Open Source Software (OSS) in US Government.

Table 3.1 Advantages and Challenges Highlighted in the PITAC Report [6]

Advantages	• Potentially improved security because programmers have developed access to source code that allows them to examine it for potential embedded trap doors and/or Trojan horses. • Increase in the number of programmers searching for software bugs and developing fixes.
Challenges	• Limitation in the project management and funding models to support "fiscal flexibility" for open source development. • Lack of policies or guidance governing export control and national security considerations. • Potentially incompatible licensing agreements used within the open source community may cause delays due to the lack of education of how to use them. • Poorly defined procurement[a] rules do not explicitly authorize competition between open source alternatives and proprietary software. • Lack of clear guidance regarding the decision-making authority and/or responsibility of the federal agency to use OSS. • Lack of a single repository for warehousing open source projects.

[a]From US Department of Homeland Security, Science and Technology. Open Source Software in Government: Challenges and Opportunities. Washington, DC: US Department of Homeland Security; 2013. "*Incentivize government program offices and contractors to build collaborative communities and to share code. Request for proposal developers should not presume that respondents have a particular business model and should not impose unnecessary paperwork burdens. The government should require sharing software and release software as OSS by default if it was developed with public funds; this may require changes to contracting strategies.*"

The President's Information Technology Advisory Committee (PITAC),[24] which examined OSS, was given the goal [6] of:

- Charting a vision of how the federal government can support developing OSS;
- Defining a policy framework;
- Identifying policy, legal, and administrative barriers to the widespread adoption of OSS; and
- Identifying potential roles for public institutions in OSS economics model.

The PITAC published a report[25] concluding that the use of the open source development model (also known as the Bazaar model[26]) was a viable strategy for producing high-quality software through a mixture of public, private, and academic partnerships [7]. In addition, as presented in Table 3.1, the report also

[24]Co-Chaired by Raj Reddy of Carnegie Mellon University (http://www.rr.cs.cmu.edu/) and Irving Wladawsky-Berger of MIT (https://esd.mit.edu/people/scholars/wladawsky-berger/wladawsky-berger.htm).
[25]*Developing Open Source Software to Advance High End Computing*. Available from: http://www.nitrd.gov/pitac/report/index.html.
[26]*The Cathedral and the Bazaar*. Available from: http://www.catb.org/esr/writings/cathedral-bazaar/.

highlighted several advantages and challenges. Some of these key issues have been at the forefront of the federal government's adoption of OSS.

Over the years since the PITAC report, the federal government has gained significant experience in both sponsoring and contributing to OSS projects. For example, one of the most widely recognized contributions by the federal government specifically related to security is the Security Enhanced Linux (SELinux) project.[27] The SELinux project focused on improving the Linux kernel through the development of a reference implementation of the Flask security architecture[28] for flexible mandatory access control (MAC). In 2000, the National Security Agency (NSA)[29] made the SELinux available to the Linux community under the terms of the GNU's Not Unix (GNU) General Public License (GPL).[30]

NOTE

The Open Source Definition (OSD)[31] had its beginning as free software[32] in the early 1980s during the free software movement[33] starting with the GNU[34] project[35] that implemented the GPL. Although the early uses of the terms "open source" and "free software" had been used interchangeably during that period, it was not until 1998 that Netscape Communications Corporation released[36] their Netscape Navigator Web browser source code as Mozilla. At this time, the distinction of the "open source"[37] concept became more mainstream within the broader commercial software industry. The Free Software Foundation[38] and Open Source Initiative (OSI)[39] have similar goals, but there was a notable difference in respect to their philosophies[40] and approved licenses.[41]

[27]SELinux Frequently Asked Questions (FAQ). Available from: https://www.nsa.gov/what-we-do/research/selinux/faqs.shtml.
[28]*Flask security architecture*. Available from: http://www.cs.utah.edu/flux/fluke/html/flask.html.
[29]Raising the Bar in Operating System Security: SELinux and OpenSolaris FMAC. Available from: https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-18-2.pdf.
[30]*GNU General Public License*. Available from: http://www.gnu.org/copyleft/gpl.html.
[31]Based loosely on the *Debian Software Guidelines (DFSG)*. Available from: http://www.debian.org/social_contract#guidelines.
[32]*The Free Software Definition*. Available from: http://www.gnu.org/philosophy/free-sw.html.
[33]*Why Software Should Not Have Owners*. Available from: http://www.gnu.org/philosophy/why-free.html.
[34]*GNU Not For Unix*. Available from: http://www.gnu.org/gnu/manifesto.html.
[35]The Free Software Foundation was a sponsoring organization of GNU.
[36]*The Beginning of Mozilla*. Available from: http://blog.lizardwrangler.com/2008/01/22/january-22-1998-the-beginning-of-mozilla/.
[37]*The Cathedral and the Bazaar*. Available from: http://www.catb.org/esr/writings/cathedral-bazaar/.
[38]*Free Software Foundation (FSF)*. Available from: http://www.fsf.org/.
[39]*Open Source Initiative (OSI)*. Available from: http://www.opensource.org/.
[40]*Why Open Source missed the point of Free Software*. Available from: http://www.gnu.org/philosophy/open-source-misses-the-point.html.
[41]*OSI Approved Licenses*. Available from: http://www.opensource.org/licenses/alphabetical and *Free Software Foundation Licenses*. Available from: http://en.wikipedia.org/wiki/List_of_FSF_approved_software_licenses.

Starting in 2001, the MITRE Corporation, for the US Department of Defense (DoD), published a report[42] that built a business case for the DoD's use of OSS. The business case discussed both the benefits and risks for considering OSS. In MITRE's conclusion, OSS offered significant benefits to the federal government, such as improved interoperability, increased support for open standards and quality, lower costs, and agility through reduced development time. In addition, MITRE highlighted issues and risks, recommending any consideration of OSS should be carefully reviewed.

Shortly after the MITRE report, the federal government began to establish specific policies and guidance to help clarify issues around OSS. The DoD Chief Information Officer (CIO) published the Department's first official DoD-wide memorandum to reiterate existing policy and to provide clarifying guidance on the acquisition, development, and the use of OSS within the DoD community [8]. Soon after the DoD policy, the Office of Management and Budget (OMB) established a memorandum to provide government-wide policy[43] regarding acquisition[44] and licensing issues.

Since 2003, there were multiple misconceptions, specifically within the DoD, regarding the use of OSS. Therefore, in 2007, the US Department of the Navy (DON) CIO released a memorandum[45] that clarified the classification of OSS and directed the Department to identify areas where OSS can be used within the DON's IT portfolio. This was followed by another DoD-wide memorandum in 2009, which provided DoD-wide guidance and clarified the use and development of OSS, including explaining the potential advantages of the DoD reducing the development time for new software, anticipating threats, and response to continual changes in requirements [9].

In 2009, OMB released the Open Government Directive,[46] which required federal agencies to develop and publish an Open Government Plan on their websites.

---

[42] *A Business Case Study of Open Source Software*. Available from: http://www.mitre.org/sites/default/files/pdf/kenwood_software.pdf.

[43] Office of Management and Budget (OMB) Memorandum 04–16, Software Acquisition. Available from: http://www.whitehouse.gov/omb/memoranda_fy04_m04-16.

[44] From Evans, K., Burton, R. Office of Management and Budget (OMB) Memorandum 04–16, Software Acquisition. Washington, DC: Executive Office of the President, Office of Management and Budget; 2004. *The Office of Management and Budget (OMB) Circulars A-11 and A-130 and the Federal Acquisition Regulation (FAR), guide agency information technology (IT) investment decisions and are intentionally technology and vendor neutral.*

[45] *Department of the Navy Open Source Software Guidance*. Available from: http://www.doncio.navy.mil/ContentView.aspx?ID = 312.

[46] From Transparency and Open Government [Internet]. Washington, DC: The White House [cited June 2, 2012]. <http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government>. *In 2009, a Presidential Memoranda was issued titled "Transparency and Open Government," which directed the OMB Director to issue an Open Government Directive to instruct federal agencies to take specific action in implementing the Open Government Initiative.*

The Open Government Plan[47] provided a description on how federal agencies would improve transparency and integrate public participation and collaboration [10]. As an example response to the directive support for openness, the National Aeronautics and Space Administration (NASA), in furtherance of its Open Government Plan, released the "open. NASA"[48] site that was built completely using OSS, such as the LAMP stack[49] and the Wordpress content management system (CMS).

On May 23, 2012, the White House released the *Digital Government Strategy* that complements[50] other initiatives and established principles for transforming the federal government. More specifically, the strategy outlined the need for a "Shared Platform" approach. In this approach, the federal government would need to leverage "sharing" of resources such as the "use of open source technologies that enable more sharing of data and make content more accessible" [11].

The Second Open Government Action Plan established an action to develop an OSS policy to improve access by federal agencies to custom software to "fuel innovation, lower costs, and benefit the public" [12]. In August 2016, the White House published the Federal Source Code Policy, which is consistent with the "Shared Platform" approach in the Digital Government's Strategy, by requiring federal agencies make available custom code as OSS.[51] Further, the policy also made "custom-developed code available for Government-wide reuse and make their code inventories discoverable at https://www.code.gov ('Code.gov')" [12].

In this section, we discussed key milestones that have impacted the federal government's cultural acceptance of OSS. It also discussed the current policy framework that has been developed through a series of policies and guidelines to support federal agencies in the adoption of OSS and the establishment of processes and policies to encourage and support the development of OSS. The remainder of this chapter will examine the key issues that have impacted OSS adoption and briefly examine the role of OSS in the adoption of cloud computing within the federal government.

---

[47]NASA released its original Open Government Plan 1.0 in April 2010 and in accordance with the requirement to review/update every two years under the Open Government Directive, NASA's current Open Government Plan was released in April 2012. Available from: http://www.nasa.gov/open/plan/.

[48]*open.NASA*. Available from: http://open.nasa.gov.

[49]Linux, Apache, MySQL, and Perl/PHP (LAMP).

[50]From the White House. Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*The Digital Government Strategy complements several initiatives aimed at building a 21st century government that works better for the American people. These include Executive Order 13571 (Streamlining Service Delivery and Improving Customer Service), Executive Order 13576 (Delivering an Efficient, Effective, and Accountable Government), the President's Memorandum on Transparency and Open Government, OMB Memorandum M-10-06 (Open Government Directive), the National Strategy for Trusted Identities in Cyberspace (NSTIC), and the 25-Point Implementation Plan to Reform Federal Information Technology Management (IT Reform).*"

[51]From the Office of Management and Budget (OMB). OMB Memorandum 16–21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. Washington, DC: Executive Office of the President, Office of Management and Budget; 2016. "*Contracts for the custom development of software shall—at a minimum—acquire and enforce rights sufficient to enable Government-wide reuse of custom-developed code*."

OPEN SOURCE SOFTWARE ADOPTION CHALLENGES: ACQUISITION AND SECURITY

The adoption of OSS as previously mentioned, has faced a number of roadblocks within the federal government. In this section, we will focus our examination specifically on the acquisition and security challenges that have been key inhibitors in the broad adoption of OSS. In addition, through our review we will obtain a better understanding of how the federal government's relationship with OSS has changed over time and gain some insight into how this experience has eased the path to cloud computing.

NOTE

In a blog post titled "Streaming at 1:00: In the Cloud" [13], former US CIO Vivek Kundra noted three critical challenges facing the federal government in deploying new IT services and products:

- Procurement processes can be confusing and time-consuming.
- Security procedures are complex, costly, lengthy, and duplicative across agencies.
- Our (federal government) policies lag behind new trends, causing unnecessary restrictions on the use of new technology.

ACQUISITION CHALLENGES

In the past, federal agencies have relied upon limited acquisition policy guidance[52] when considering the procurement and the use of OSS. In the PITAC report [14] discussed previously, two specific acquisition-related findings were highlighted:

- *Licensing agreements*—numerous licensing agreements, incompatible licensing requirements, and educating federal managers on open source licenses[53] and conditions.[54]
- *Federal procurement rules*—no explicit authorization of competition between open source alternatives and proprietary software, and lack of guidance on applicability and usage of OSS.

[52]From Federal Acquisition Regulation (FAR). Washington, DC: US General Services Administration; 2011. The Federal Acquisition Regulation (FAR) classifies open source software as commercial computer software (or "commercial item means")—"*(1) customarily used by the general public or by non-governmental entities and (1)(i) sold, leased, or licensed to the general public; or (1)(ii) offered for sale, lease, or license to the general public*".

[53]From Office of Management and Budget (OMB). OMB Memorandum 16-21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. Washington, DC: Executive Office of the President, Office of Management and Budget; 2016. "*Licensing is a critical component of OSS and can affect how the source code can be used and modified*."

[54]MITRE study conducted in 2003, "Use of Free and Open Source Software (FOSS) in the US Department of Defense." Available from: http://dodcio.defense.gov/Portals/0/Documents/FOSS/dodfoss_pdf.pdf.

Table 3.2 Federal Laws and Regulations

Federal Laws	• 41 U.S.C. § 430[a]—Definitions (defines "*commercial item*") • 41 U.S.C. § 431[b]—Commercially available off-the-shelf item acquisitions: lists of inapplicable laws in FAR (defines "*Commercially available off-the-shelf (COTS) item*") • 41 U.S.C. § 264B[c] and 10 USC § 2377[d]—Preference for acquisition of commercial items
Regulations	• FAR 2.101(b)[e], 12.000, 12.101(c)[f]—Acquisition of Commercial Items • FAR 10.001[g]—Market Research

[a]Available from: *http://www.gpo.gov/fdsys/pkg/USCODE-2009-title41/html/USCODE-2009-title41-chap7-sec403.htm*.
[b]Available from: *http://www.gpo.gov/fdsys/pkg/USCODE-2009-title41/html/USCODE-2009-title41-chap7-sec431.htm*.
[c]Available from: *http://www.gpo.gov/fdsys/pkg/USCODE-2009-title41/html/USCODE-2009-title41-chap4-subchapIV-sec264b.htm*.
[d]Available from: *http://www.gpo.gov/fdsys/pkg/USCODE-2006-title10/html/USCODE-2006-title10-subtitleA-partIV-chap140-sec2377.htm*.
[e]Available from: *https://www.acquisition.gov/far/html/Subpart%202_1.html*.
[f]Available from: *https://www.acquisition.gov/far/html/Subpart%2012_1.html*.
[g]Available from: *https://www.acquisition.gov/far/html/Subpart%202_1.html*.

Even with the limited policies guidance, federal agencies were required to understand how federal laws and regulations applied to the acquisition of OSS. Table 3.2 provides several references within federal laws and regulations that must be considered by federal agencies when procuring OSS (and other proprietary) COTS products.

In addition, federal agencies are also required to understand how to select and apply the various types of software licenses, specifically "where future modifications by the US government may be necessary" [15]. Guidelines in developing license criteria [16] used in determining which OSS license to use could include:

- Using an existing OSS license; not creating a new OSS license.
- Making sure it is actually OSS.
- Using a GPL-compatible license.
- Choosing a license that meets the expected uses of the OSS.
- Using a common OSS license.

In order to dispel concerns over these license issues, several policy documents were issued to govern acquisition and provide guidance on the use of OSS within the federal government. The OSS acquisition policy framework, outlined in Table 3.3, consists primarily of the existing OMB and DoD policies; however, some federal agencies have issued additional guidance[55] to provide specific direction on how OSS could be used to support their specific mission and business

[55]For example, Internal Revenue Service (http://www.irs.gov/pub/irs-utl/fti-in-opensourcesoftware.doc), the Consumer Financial Protection Bureau (http://www.consumerfinance.gov/developers/sourcecodepolicy/), and NASA (http://nodis3.gsfc.nasa.gov/displayDir.cfm?t = NPR&c = 2210&s = 1C).

Table 3.3 OSS Acquisition Policy Framework

OMB Memorandum 04–16, Software Acquisition (2004)[a]	• Clarified the equal treatment of OSS and proprietary software in acquisition decision • Recommended caution when using OSS to understand the type of OSS license associated with software and obligations to make original source available • Employee education of licensing restrictions
Clarifying Guidance Regarding Open Source Software (2009)[b]	• Clarified the applicability of OSS in meeting the definition of "commercial software" in accordance with 10 U.S.C 2377 • Requirement for conducting market research when preparing for procurement of property or services, including OSS • Clarified DoD Instruction 8500.2,[c]Information Assurance (IA) Implementation—DCPD-1 Public Domain Software Controls, does not forbid usage of OSS • All software, including OSS, should include maintenance and support • Clarified misconceptions of requirements to distribute modified OSS to public and emphasized importance of understanding which licenses allow users to modify *for internal use only* • Required the usage of a DoD-wide collaborative software development environment to distribute software source code and design documents[d] • Distribution of OSS, including code fixes and enhancement, to the public when it is determined it is in the government's interest; the government has rights to reproduce and release, and public release of item is not restricted by other law or regulations (e.g., Export Administration Regulations (EAR)[e] or International Traffic in Arms Regulation (ITAR)[f])
Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software (2016)	• Provided a policy to agencies on considerations that must be made prior to acquiring any custom-developed code • Required agencies to obtain appropriate Government data rights to custom-developed code, including at a minimum, rights to Government-wide reuse and rights to modify the code • Required agencies to consider the value of publishing custom code as OSS • Established requirements for releasing custom-developed source code, including securing the rights necessary to make some custom-developed code releasable to the public as OSS under this policy's new pilot program

[a]From Evans, K., Burton, A. Office of Management and Budget (OMB) Memorandum 0416, Software Acquisition. Washington, DC: Executive Office of the President, Office of Management and Budget; 2004. "The Office of Management and Budget (OMB) Circulars A-11 and A-130 and the Federal Acquisition Regulation (FAR), guide agency information technology (IT) investment decisions."
[b]*DoD Instruction 8510.01.* Available from: *http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf.*
[c]From Stenbit, J. DoD Instruction 8500.2 Information Assurance (IA) Implementation. Washington: US Department of Defense; 2003. *The DoD memo also dispelled the misconceptions that OSS is classified as "freeware or shareware," which is prohibited from being* "used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available."
[d]From DISA. Forg.mil [Internet]. Maryland: Defense Information Systems Agency [cited March 18, 2016]. "*Forge.mil is a DISA-led activity designed to improve the ability of the U.S. Department of Defense to rapidly deliver dependable software, services and systems in support of net-centric operations and warfare.*"
[e]DoD Instruction 8510.01. Available from: *http://www.bis.doc.gov/policiesandregulations/index.htm.*
[f]International Traffic in Arms Regulation (ITAR). Available from: *http://pmddtc.state.gov/regulations_laws/itar.html.*

Table 3.4 Federal Government OSS FAQs

Frequently asked questions regarding OSS and the US DoD (2009)	"An educational resource for government employees and government contractors to understand the policies and legal issues relating to the use of OSS in the DoD" [15]
Frequently asked questions about copyright and computer software: issues affecting the US Government with Special Emphasis on OSS (2010)	"Provides general guidance on a special category of copyright works—computer software—and includes a details discussion of open source software" [17]

requirements. In addition to the policy documents, several frequently asked questions (FAQs) have been developed to facilitate understanding key acquisition-related issues (see Table 3.4).

SECURITY CHALLENGES

OSS has previously been characterized as offering a number of potential security advantages. The security advantages[56] include the ability for developers to access the source code, allowing for a more thorough examination and identification of security vulnerabilities, and an increased number of availability of programmers searching for bugs and subsequently developing fixes [14]. However, some of the same advantages have also been overshadowed by hindrances such as uncertainty of the trustworthiness of code repositories and the availability of source code to allow malicious attackers the ability to identify security vulnerabilities.

Challenges associated with security in OSS have also existed because there has been a lack of clarification and education of the processes and certifications required to ensure that software is validated for use within the federal government. Some of the commonly used processes[57] and certification methodologies that are required for verifying that software and applications meet federal security requirements include, but are not limited to:

- NIST Risk Management Framework (RMF).[58]
- DoD Information Assurance Security Certification and Accreditation Process (DIACAP).[59]

[56]From Wennergren, D. Clarifying guidance regarding OSS. Washington, DC: Department of Defense; 2009. "*The continuous and broad peer-review enabled by publicly available source code supports software reliability and security efforts through the identification and elimination of defects that might otherwise go unrecognized by a more limited core development team.*"

[57]Certification and accreditation processes are discussed in detail in Chapter 7, Comparison of Federal and International Security Certification Standards.

[58]*NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems.* Available from:<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.

[59]*DoD Instruction 8510.01, RMF for DoD Information Technology.* <http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf>.

- Risk Management Framework (RMF) for DoD Information Technology *(previously known as the DoD Assurance Certification and Accreditation Process (DIACAP))*.[60]
- National Information Assurance Partnership (NIAP), Common Criteria (CC).[61]

In addressing the challenges with OSS security, the federal government initiated a number of programs "to investigate open security methods, models and technologies and identify viable and sustainable approaches that support national cyber security objectives" [18]. For example, the US Department of Homeland Security (DHS), Science and Technology (S&T), and Directorate Cyber Security Research and Development Center (CSRDC) manages the Homeland Open Security Technology (HOST)[62] program, which is an information portal for open-source security tools and applications. In addition, the DHS also initiated the Open Source Hardening Project to maintain a database of analyzed OSS using the coverity scan.[63] The scan website offers qualified project developers of OSS with a portal where they can retrieve defects identified by Coverity[64] analyses [19].

OPEN SOURCE SOFTWARE AND FEDERAL CLOUD COMPUTING

Open source technologies have played a significant role in the federal government's adoption of cloud computing. From the inception of the *25-Point Implementation Plan to Reform Federal Information Technology Management*, which introduced the key components of the federal government's adoption of "light technologies" and "shared solutions," the federal government has initiated the shift toward more openness and shared platforms. Openness and shared platforms support the ability of the federal government to deliver agility and innovation. OSS has served as the enabler, spawning incubations[65] in technologies across the industry and public sector that have formed the foundation of many of the cloud computing platforms.

[60]NSTISSI-1000, National Information Assurance Certification and Accreditation Process (NIACAP).

[61]*National Informational Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS)*. Available from: http://www.niap-ccevs.org/.

[62]*Homeland Open Security Technology (HOST).* Available from: / http://www.dhs.gov/science-and-technology/csd-host.

[63]List of open source software scanned by the Coverity Scan. Available from: https://scan.coverity.com/projects.

[64]Coverity provides the results of its static-analysis code inspection tool for free to open source community.

[65]Examples include python (http://www.python.org/), Java (http://www.java.com), Springsource (http://spring.io/), Apache Software Foundation (https://projects.apache.org/projects.html), and Linux (http://kernel.org/).

NOTE

In 2003, NASA began "assessing the formal barriers to distributing software they developed as open source and began reviewing the state of open source licenses"[66] [20]. Open source[67] directly addressed NASA's needs of the rapid and wide dissemination of software with minimal overhead and cost, supporting its functions under the National Aeronautics and Space Act.[68] However, it was not until September 15, 2009, when the former US CIO Vivek Kundra announced the launch of Apps.gov[69] at the NASA Ames Research Center (ARC),[70] did it set the stage for the next phase in the federal government's adoption of public cloud computing services. During this time, NASA ARC had already begun an effort in the development of a cloud environment through the Nebula project.[71] NASA Nebula, "which started out as a Web consolidation exercise" [21], succeeded primarily because of the experience obtained through NASA's involvement in OSS.[72] Following experimentation with both commercial and open source cloud computing solutions, the Nebula project initiated an effort to begin building the first open source Infrastructure as a Service (IaaS) cloud software platform.[73] Nebula provided a case study for demonstrating the value OSS brought to the federal government.

The Federal Data Center Consolidation Initiative (FDCCI) is a federal consolidation effort focused on reducing physical space by shifting IT investments to more efficient computing platforms and technologies [22]. These computing platforms and technologies leverage virtualization to support the ability to consolidate and improve government-wide IT utilization through shared infrastructures. The Cloud First and Shared First policies were established to increase the return on investment (ROI) associated with the federal government's use of its IT investment. The optimization of IT investment requires the use of the economies of scale offered by cloud

[66]NASA Open Source Agreement (NOSA), which became the only government agency to receive OSI Certification. Available from: http://www.opensource.org/licenses/nasa1.3.

[67]Instead of using an existing licensing model, NASA chose to produce the NOSA, which became an OSI-approved software license.

[68]From NASA, The National Aeronautics Space Act [Internet]. Washington, DC: NASA [cited May 21, 2012]. <http://www.nasa.gov/offices/ogc/about/space_act1.html>. "*Provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof.*"

[69]A storefront portal hosted by GSA for federal agencies to find cloud computing applications to include business applications, productivity applications, cloud IT services, and social media apps.

[70]NASA Ames Research Center (ARC). Available from: http://www.nasa.gov/centers/ames/.

[71]From NASA, Nebula Cloud Computing Platform [Internet]. California: NASA Ames Research Center [cited November 11, 2011]. <http://www.nasa.gov/open/nebula.html>. "*Nebula is an open-source cloud computing project and service developed to provide an alternative to the costly construction of additional data centers.*"

[72]From Cureton, L., Braun, B. NPR 22101C, Requirement Waiver in Support of Open Source Software Development. Washington, DC: NASA; 2010. "*For example, in November 2010, the NASA Chief Information Officer (CIO) issued a request for a waiver to support the release of the Nebula software for development in a publicly accessible repository to accelerate development and leverage community expertise to produce higher quality software.*"

[73]The NASA Nebula cloud fabric became the Nova fabric controller as the Compute component of the OpenStack cloud software. Available from: http://www.openstack.org.

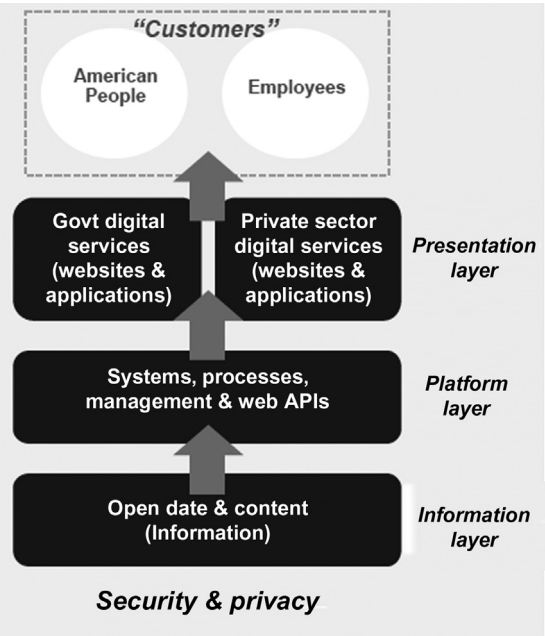

FIGURE 3.2

Conceptual layers of digital services [23].

commuting and other shared service[74] platforms. By leveraging reuse offered by OSS and the consolidation of redundant missions, through cross-organizational cloud services, efficiency can be delivered through more "economical" and "shared" delivery service models. The Digital Government Strategy, as illustrated in Fig. 3.2, reiterated the need to deliver more efficient customer-centric services at a lower cost point through technologies that support the *information*,[75] *platform*,[76] and *presentations*[77] layers. In addition, cloud computing and related technologies offer a shared

[74]From VanRoekel, V. Federal Information Technology Shared Services Strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*An information technology function that is provided for consumption by multiple organizations within or between Federal Agencies*."

[75]From the Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*The information layer contains digital information*."

[76]From the Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. The platform layer includes all the systems and process to manage digital information.

[77]From the Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*The presentation layer defines the manager in which information is organized and provided to customers*."

platform to support the federal government's ability to manage information[78] in an organized manner and deliver the information using multiple accessibility modes (e.g., websites and mobile applications). A shared platform approach also provides an efficient and low-cost mechanism to develop and deliver services and information that support the strategy through three strategic objectives:

- Securely architect for interoperability and openness.
- Develop governance structure for digital services[79] (e.g., procurement and security policies and processes).
- Spur innovation by providing the federal government's data in open and machine-readable formats.

OSS, as an enabler for cloud computing and other shared platforms, has accelerated the shift in technology delivery models, both in the public and private sectors. OSS has also produced many of the key technology innovations that are built into the foundation of this technology shift, such as different virtualization[80] technologies and cloud computing[81] platforms. These technologies and platforms can be leveraged to support the federal government's digital strategy through an open, standards-based approach that provides a more efficient use of rapidly evolving technologies. In addition, many OSS projects utilize a shared development methodology. This methodology promotes agility by bringing together a community of developers that can deliver innovative solutions faster and with fewer dedicated resources.

SUMMARY

In this chapter, a case for open source was presented with a focus on understanding how the accelerated pathway to the cloud was, in part, contributed to by the broader government-wide acceptance of OSS. Challenges faced by the federal government in addressing acquisition were examined, which included licensing

[78]From the Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*Information, as defined in OMB Circular A-130, is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms*."

[79]From the Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "Digital services include the delivery of digital information (i.e., data or content) and transactional services (e.g., online forms, benefits applications) across a variety of platforms, devices and delivery mechanisms (e.g., websites, mobile applications, and social media)."

[80]Examples include Kernel-based Virtual Machine (http://www.linux-kvm.org/page/Main_Page) and Xen Hypervisor (http://www.xenproject.org/developers/teams/hypervisor.html).

[81]Examples include OpenStack cloud software (http://www.openstack.org), CloudStack (http://cloudstack.apache.org/), and Cloud Foundry (https://www.cloudfoundry.org/).

and federal procurement policies. Security was also discussed with specific focus on the processes and certification methods that provide risk-based approaches to verify OSS as part of the system development life cycle (SDLC). Finally, the chapter concluded with a brief discussion on how OSS is an enabler that supports the federal government's objectives of embracing technologies to promote efficiency and improved service delivery in a secure, standards-based approach.

REFERENCES

[1] The U.S. Digital Service. Digital Services Playbook [Internet]. Washington, DC: Executive Office of the President [cited January 28, 2016]. <https://playbook.cio.gov/>.

[2] US House of Representatives. Subcommittee on oversight and investigation of the committee on Veteran's affairs [Internet]. Washington, DC: US Government Printing Office [cited May 22, 2012]. <http://veterans.house.gov/sites/republicans.veterans.house.gov/files/documents/112-12transcripto-i5-11-11.html>.

[3] US Department of Veterans Affairs. VA launches open source custodian: open source electronics health record agent begins operations [Internet]. Washington, DC: US Department of Veterans Affairs [cited May 22, 2012]. <http://www.va.gov/opa/pressrel/pressrelease.cfm?id=2153>.

[4] NASA. NASA clears the runway for open source software [Internet]. Washington, DC: National Aeronautics and Space Administration [cited May 24, 2012]. <http://www.nasa.gov/home/hqnews/2012/jan/HQ_12-021_Open_Source_Software.html>.

[5] Evans K, Burton A. Office of Management and Budget (OMB) memorandum 04-16, software acquisition. Washington, DC: Executive Office of the President, Office of Management and Budget; 2004.

[6] President's Information Technology Advisory Committee. Developing open source software to advance high end computing. Washington, DC: National Coordination Office for Networking and Information Technology Research and Development; 2000.

[7] President's Information Technology Advisory Committee Letter [Internet]. Washington, DC: National Coordination Office for Networking and Information Technology Research and Development [cited October 20, 2011]. <http://www.nitrd.gov/Pitac/letters/pitac_ltr_sep11.html>.

[8] Stenbit DJ. Open source software (OSS) in the Department of Defense (DoD). Washington, DC: Department of Defense; 2003.

[9] Wennergren D. Clarifying guidance regarding open source software (OSS). Washington, DC: Department of Defense; 2009.

[10] Orszag P. Office of Management and Budget (OMB) Memorandum 10-06, Open Government Directive. Washington, DC: Executive Office of the President, Office of Management and Budget; 2009.

[11] The White House. Digital government: building a 21st century platform to better serve the American people. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012.

[12] Office of Management and Budget (OMB). The Open Government Partnership, Announcing New Open Government Initiatives, Second Open Government National Action Plan. Washington, DC: Executive Office of the President, Office of Management and Budget; 2014.

[13] Streaming at 1:00 in the cloud [Internet]. Washington, DC: Office of Social Innovation and Civic Participation [cited November 2, 2011]. <http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud>.
[14] President's Information Technology Advisory Committee. Developing open source software to advance high end computing. Washington, DC: National Coordination Office for Networking and Information Technology Research and Development; 2000.
[15] US Department of Defense (DoD), Chief Information Officer (CIO). DoD open source software (OSS) FAQ. [Internet]. Washington, DC: US Department of Defense [cited October 31, 2011]. <http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx>.
[16] US Department of Defense (DoD), Chief Information Officer (CIO). What license should the government or contractor choose/select when releasing open source software? [Internet]. Washington: US Department of Defense [cited June 2012]. <http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx#Q:_What_license_should_the_government_or_contractor_choose.2Fselect_when_releasing_open_source_software.3F>.
[17] CENDI Copyright Working Group. Frequently asked questions about copyright and computer software: issues affecting the US government with special emphasis on open source software. Tennessee: CENDI Secretariat; 2010.
[18] DHS Homeland Open Security Technology (HOST) [Internet]. Washington, DC: US Department of Homeland Security [cited November 5, 2011]. <http://www.dhs.gov/science-and-technology/csd-host>.
[19] Stanford University. AFRL-RI-RS-TR-2009-192, Final technical report: the open source hardening project. New York: Air Force Research Laboratory; 2009.
[20] Moran P. Developing an open source option for NASA software. California: NASA Ames Research Center; 2003.
[21] Williams J. NASA Nebula in action: cloud computing case examples. California: NASA Ames Research Center; 2009.
[22] Kundra V. Federal cloud computing strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.
[23] Office of Management and Budget (OMB). Digital government: building a 21st century platform to better serve the american people. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012.