



**Hewlett Packard  
Enterprise**

# **Emerging Federal Policy on OSS and Code Reuse**

**4 October 2016**

**John M. Farrell**

---

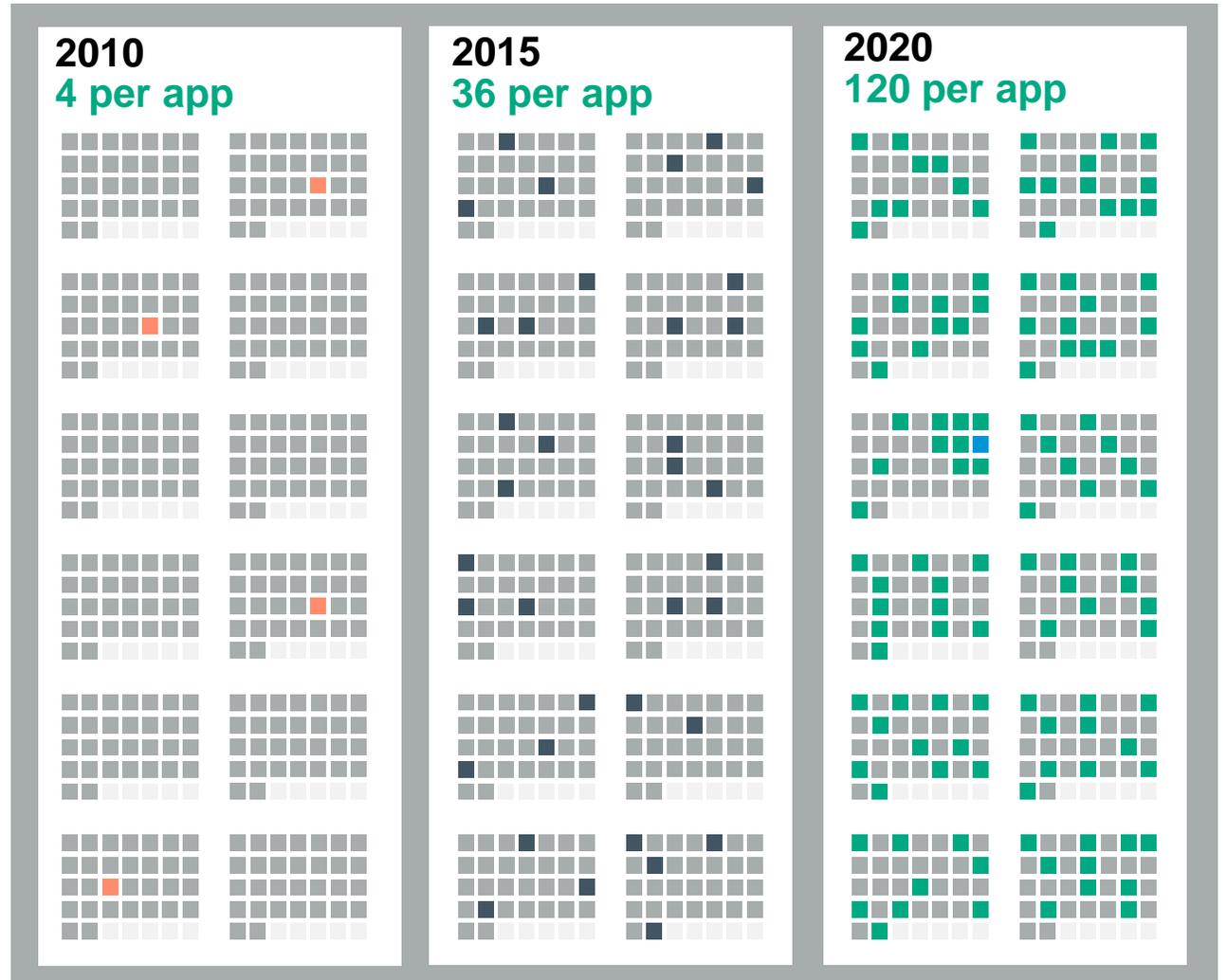
# Measuring the Benefits of Software Reuse

Does software reuse really pay off in the long run? How can you tell?

- **Software reuse has long been on the radar of many companies because of its potential to deliver quantum leaps in production efficiencies.** In fact, basic, or ad hoc software reuse already exists within most organizations. This reuse of documents, coding styles, components, models, patterns, knowledge items, and source code is rarely discussed because it usually starts and ends as an informal grass roots effort, with management having little understanding of how it started, why it persists, and how they might proactively extract larger benefits from it.
- With an understanding that some form of reuse very likely already exists within most, if not all, software development organizations, the questions emerge, "**how can we measure the level of reuse that already exists?**", "**what can be done to increase reuse benefits?**", and "**how can we track our progress along the way?**".
- Lior Amar and Jan Coffey, June 01, 2005 - Dr. Dobb's The World of Software Development

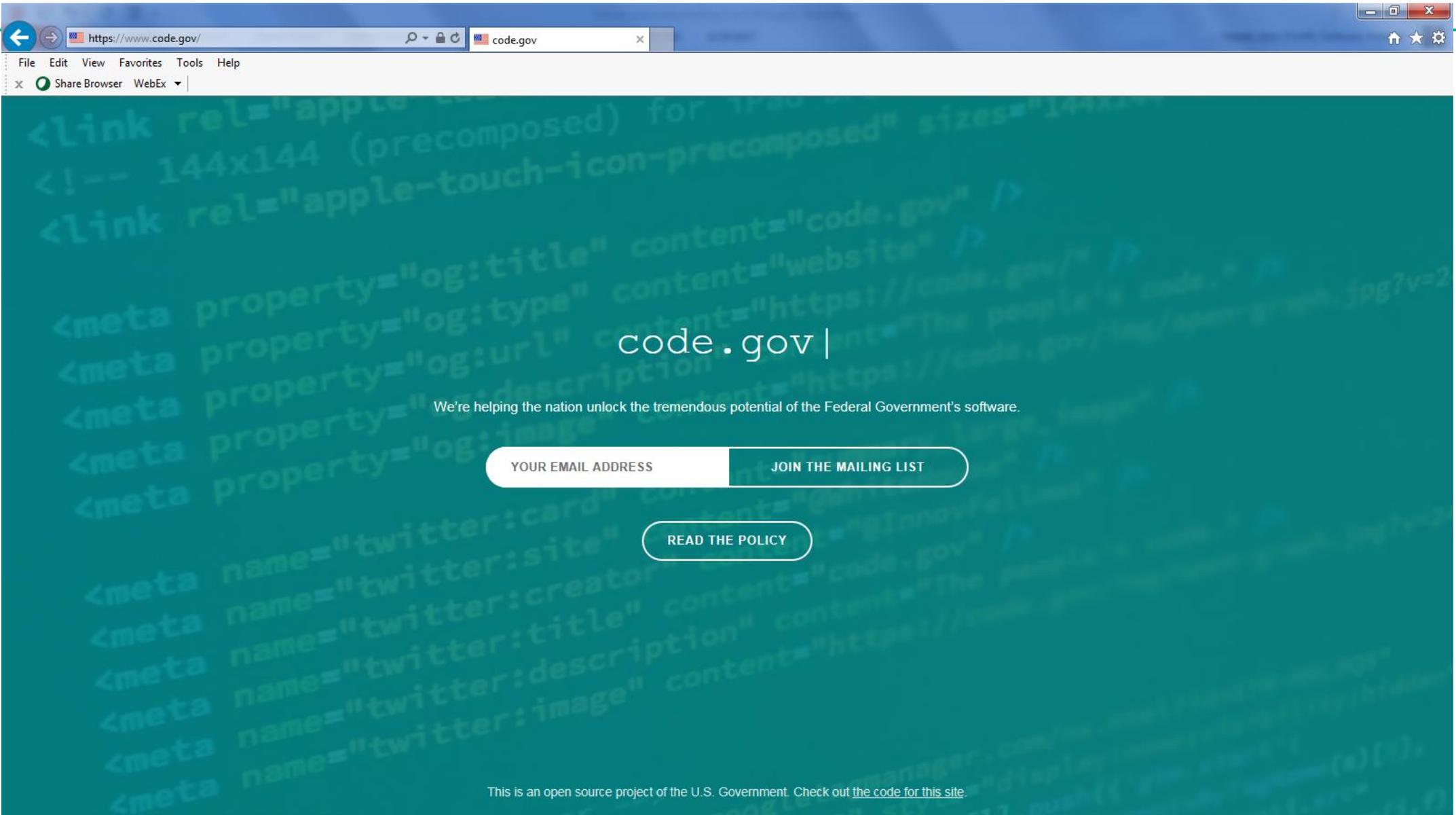


# Developers need to move at the speed of business innovation



## Number of Releases per year

Thanks to consumerization, users now expect continuous improvements to apps rather than the traditional annual mega-updates



---

# Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software

- The U.S. Government is committed to improving the way Federal agencies buy, build, and deliver information technology (IT) and software solutions to better support cost efficiency, mission effectiveness, and the consumer experience with Government programs.
- Each year, the Federal Government spends more than \$6 billion on software through more than 42,000 transactions.<sup>1</sup> A significant proportion of software used by the Government is comprised of either preexisting Federal solutions or commercial solutions.
- These solutions include proprietary, open source, and mixed source<sup>2</sup> code and often do not require additional custom code development.

**M-16-21**

**MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES**

**FROM:**

**Tony Scott**

**United States Chief Information Officer**

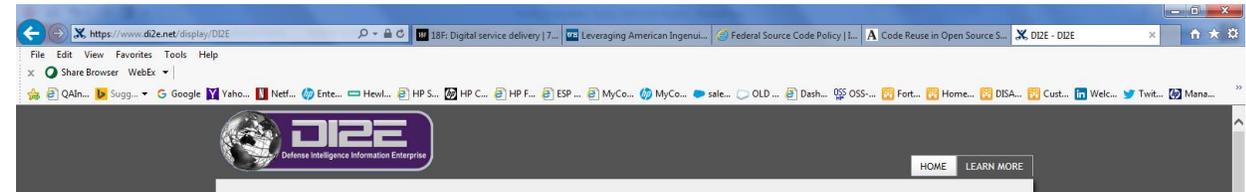
**Anne E. Rung**

**United States Chief Acquisition Officer**

<https://sourcecode.cio.gov/Reuse/>

# Government Open Source and Code Reuse Programs

- Civilian Agencies
- Defense Department
- Intelligence Community



## GitHub Privacy Policy and Notice

security (DHS or Department) will use GitHub for collaborative development using GitHub is open source software (OSS), which is openly modified and redistributed. In a collaborate on data and policy. The DHS National Information Exchange M Hub site and controls who at the Dep.

ing site for software development projects that are and its privacy policy can be found at <https://www.github.com/privacy> and Privacy Impact Assessment (PIA) govern the policy can be found at [www.dhs.gov/privacy-policy](http://www.dhs.gov/privacy-policy) can be found at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

ons while interacting with the Department. DHS "like" public users proactively without a waiver and tribal government agencies.) To the extent necessary to accomplish a purpose authorize

Task	Due Date	Checklist	Description
Find Email Address	3/1/2016 (-2 days)	Buddy of New Hire	Find your new buddy's email address.

**7 projects that state and local governments can reuse**  
By Melody Kramer  
April 13, 2016  
[tools you can use](#) [open source](#)

**DISA** The IT Center Supporting the DoD

Enterprise Services > Applications > Forge.mil

**FORGE.MIL**

Forge.mil is a family of enterprise services, consisting of SoftwareForge and ProjectForge, provided to support the DOD's technology community. The service provides for collaborative development and IT project management through the full application lifecycle. Forge.mil also enables the reuse of open source and DOD community source software. Forge.mil continues to add new capabilities to support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users. It is available as an open community service supporting anyone affiliated with the DOD, or as a private service, and is maintained on both the unclassified and classified networks.

**FORGE**

---

# Objectives

This policy will accomplish the following objectives:

- Provide a policy to agencies<sup>19</sup> on considerations that must be made prior to acquiring any custom-developed code;
- Require 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. Agencies shall make such custom-developed code broadly available across the Federal Government, subject to limited exceptions;<sup>20</sup>
- Require agencies to consider the value of publishing custom code as OSS;
- Establish 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; and
- Provide instructions and resources to facilitate implementation of this policy.

---

# Scope and Applicability

- The requirements outlined in this policy apply to source code that is custom-developed for the Federal Government, subject to the limited exceptions outlined in Section 6 of this document. Source code developed for National Security Systems (NSS), as defined in 40 U.S.C. § 11103, is exempt from the requirements of this policy. For NSS, agencies shall follow applicable statutes, Executive Orders, directives, and internal agency policies.
- The policies in this document do not apply retroactively (*i.e.*, they do not require that existing custom-developed code be retroactively made available for Government-wide reuse or as OSS). However, making such code available for Government-wide reuse or as OSS, to the extent practicable, is strongly encouraged.
- The agencies' Chief Information Officers (CIO), Chief Acquisition Officers (CAO), and other key stakeholders should promptly begin working together to implement this policy. Agencies are expected to issue internal policies, as necessary, to support these efforts and should expect their progress to be evaluated in accordance with accountability mechanisms described in Section 7.

---

# Three-Step Software Solutions Analysis

- Agencies must obtain sufficient rights to custom-developed code to fulfill both the Government-wide reuse objectives and the open source release objectives outlined in this policy's pilot program.
- In meeting their software needs, agencies must conduct the three-step analysis outlined below. This analysis is intended to leverage existing solutions—consistent with principles of category management<sup>21</sup> and shared services<sup>22</sup>—and suitable commercial solutions, while mitigating duplicative spending on custom-developed software solutions.
- These steps are consistent with the Office of Management and Budget's (OMB) long-standing policy on investments in major information systems.<sup>23</sup> Moreover, consistent with OMB's memorandum on Technology Neutrality,<sup>24</sup> agencies must consider open source, mixed source, and proprietary software solutions equally and on a level playing field, and free of preconceived preferences based on how the technology is developed, licensed, or distributed.

---

## 3 Steps

- **Step 1 (Conduct Strategic Analysis and Analyze Alternatives):** Each agency must conduct research and analysis prior to initiating any technology acquisition or custom code development. The strategic analysis should consider not only agency mission and operational needs, but also external public initiatives and interagency initiatives such as Cross-Agency Priority Goals. Having conducted the strategic analysis, agencies shall then conduct an alternatives analysis, evaluating whether to use an existing Federal software solution or to acquire or develop a new software solution. The alternatives analysis shall give preference to the use of an existing Federal software solution.<sup>25</sup>
- **Step 2 (Consider Existing Commercial Solutions):** If an agency's alternatives analysis concludes that existing Federal software solutions cannot efficiently and effectively meet the needs of the agency, the agency must explore whether its requirements can be satisfied with an appropriate commercially-available solution.<sup>26</sup>
- **Step 3 (Consider Custom Development):** If an agency's alternatives analysis concludes that an existing Federal software solution or commercial solution cannot adequately satisfy its needs, the agency may consider procuring custom-developed code in whole or in conjunction with existing Federal or commercial code. When commissioning new custom-developed software, agencies must consider the value of publishing custom code as OSS and negotiate data rights reflective of its value-consideration. Agencies must also obtain sufficient rights to fulfill this policy's objectives related to Government-wide code reuse and the open source pilot program.

---

# Three-Step Software Solutions Analysis

Agencies must also consider several factors throughout each stage of the three-step analysis:

- Hybrid Solutions: Solutions containing a mixture of existing Federal, commercial, and/or custom-developed solutions should be considered throughout each step of the analysis.
- Modular Architecture: Agencies should consider modular approaches to solution architecture. As discussed in the *Digital Government Strategy*, modularity can reduce overall risk and cost while increasing interoperability and technical flexibility.
- Cloud Computing: Consistent with OMB strategy, agencies are encouraged to evaluate safe and secure cloud computing options throughout each step of the analysis.<sup>27</sup>
- Open Standards: 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.
- Targeted Considerations: Agencies must select a software solution that best meets the operational and mission needs of the agency, taking into consideration factors such as performance, total life-cycle cost of ownership, security and privacy protections, interoperability, ability to share or reuse, resources required to later switch vendors, and availability of quality support. These considerations should be taken into account during all three steps of the analysis.

---

# Government Wide Code Reuse

Ensuring Government-wide reuse rights for custom code that is developed using Federal funds has numerous benefits for American taxpayers. To realize these benefits, agencies must comply with the following requirements:

## A. Secure Rights for Government Reuse and Ensure Delivery of Source Code

- Agencies that enter into 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. Agencies must ensure appropriate contract administration and use of best practices to secure the full scope of the Government’s rights, including—but not limited to—sharing and using the code with other Federal agencies.
- Additionally, in order to ensure the ability to exercise these rights, agencies must use best practices to ensure delivery of the custom-developed code, documentation, and other associated materials from the developer throughout the development process.

## B. Inventory All Custom-Developed Code and Make It Available Government-Wide

- Securing adequate rights to enable Government-wide reuse of custom-developed code is a critical first step in gaining efficiencies in Federal software purchasing; however, without broad and consistent dissemination of the code across the Federal Government, these efficiencies cannot be fully realized. Therefore, in addition to securing the rights discussed above, agencies shall do the following:
- Maintain a Code Inventory: As part of their broader responsibility to maintain an up-to-date inventory of agency information resources, agencies shall make custom-developed code and related information available to all other Federal agencies<sup>28</sup> by creating and maintaining an enterprise code inventory that lists all new code that is custom-developed for the Federal Government; and
- Make Custom-Developed Code Available: Agencies shall make custom-developed code available for Government-wide reuse and make their code inventories discoverable at <https://www.code.gov> (“Code.gov”), pursuant to the limited exceptions outlined in Section 6 of this policy.

---

# Open Source Software

## – Pilot Program: Publication of Custom-Developed Code as OSS

- Each agency shall release as OSS at least 20 percent of its new custom-developed code<sup>29</sup> each year for the term of the pilot program. As discussed above, agencies must obtain sufficient rights to custom-developed code to fulfill the open source release objectives of this policy’s pilot program.
- When deciding which custom-developed code projects to release, each agency should prioritize the release of custom-developed code that it considers potentially useful to the broader community. Agencies should calculate the percentage of source code released using a consistent measure—such as real or estimated lines of code, number of self-contained modules, or cost—that meets the intended objectives of this requirement. Additional information regarding how best to measure source code will be provided on Code.gov.
- Although the minimum requirement for OSS release is 20 percent of custom-developed code, agencies are strongly encouraged to release as much custom-developed code as possible to further the Federal Government’s commitment to transparency, participation, and collaboration.

---

# Open Source Software

## – Pilot Program: Publication of Custom-Developed Code as OSS

- OMB expects all agencies to satisfy the requirements of this pilot program without exception. Agencies should—as part of their selection of custom-developed code to be released as OSS—refrain from selecting code that would fall under the exceptions outlined in Section 6 of this policy. In the event that an agency’s CIO believes that the agency cannot satisfy the 20 percent requirement of the OSS pilot program (e.g., because releasing code as OSS would create an identifiable risk to the detriment of national security), the CIO should consult with OMB.
- Unless extended or supplanted by OMB through the issuance of further policy, the pilot program under this sub-section will expire three years (36 months) after the publication date of this policy; however, the rest of the Federal Source Code Policy will remain in effect. No later than two years after the publication date of this policy, OMB shall evaluate pilot results and consider whether to allow the pilot program to expire or to issue a subsequent policy to continue, modify, or increase the minimum requirements of the pilot program.
- Within 120 days of the publication date of this policy, OMB shall develop metrics to assess the impact of the pilot program. Additional information on these topics will be available on Code.gov.

---

# Open Source Software

## 5.2 Participation in the Open Source Community

- When agencies release custom-developed source code as OSS to the public, they should develop and release the code in a manner that (1) fosters communities around shared challenges, (2) improves the ability of the OSS community to provide feedback on, and make contributions to, the source code, and (3) encourages Federal employees and contractors to contribute back to the broader OSS community by making contributions to existing OSS projects. In furtherance of this strategy, agencies should comply with the following principles:
- Leverage Existing Communities: Whenever possible, teams releasing custom-developed code to the public as OSS should appropriately engage and coordinate with existing communities relevant to the project. Government agencies should only develop their own communities when existing communities do not satisfy their needs.
- Engage in Open Development: Software that is custom-developed for or by agencies should, to the extent possible and appropriate, be developed using open development practices. These practices provide an environment in which OSS can flourish and be repurposed. This principle, as well as the one below for releasing source code, include distributing a minimum viable product as OSS; engaging the public before official release;<sup>30</sup> and drawing upon the public's knowledge to make improvements to the project.
- Adopt a Regular Release Schedule: In instances where software cannot be developed using open development practices, but is otherwise appropriate for release to the public, agencies should establish an incremental release schedule to make the source code and associated documentation available for public use.
- Engage with the Community: Similar to the requirement in the Administration's Open Data Policy, agencies should create a process to engage in two-way communication with users and contributors to solicit help in prioritizing the release of source code and feedback on the agencies' engagement with the community.
- Consider Code Contributions: One of the potential benefits of OSS lies within the communities that grow around OSS projects, whereby any party can contribute new code, modify existing code, or make other suggestions to improve the software throughout the software development lifecycle. Communities help monitor changes to code, track potential errors and flaws in code, and other related activities. These kinds of contributions should be anticipated and, where appropriate, considered for integration into custom-developed Government software or associated materials.
- Documentation: It is important to provide OSS users and contributors with adequate documentation of source code in an effort to facilitate use and adoption. Agencies must ensure that their repositories include enough information to allow reuse and participation by third parties. In participating in community-maintained repositories, agencies should follow community documentation standards. At a minimum, OSS repositories maintained by agencies must include the following information:
  - Status of software (e.g., prototype, alpha, beta, release, etc.); Intended purpose of software; Expected engagement level (i.e., how frequently the community can expect agency activity); License details; and any other relevant technical details on how to build, make, install, or use the software, including dependencies (if applicable).

---

# Exceptions to Government Code Reuse

The exceptions provided below may be applied, in specific instances, to exempt an agency from sharing custom-developed code with other Government agencies. These exceptions do not apply to the OSS pilot program.<sup>31</sup> Any exceptions used must be approved and documented by the agency's CIO for the purposes of ensuring effective oversight and management of information technology resources.

Applicable exceptions are as follows:

- The sharing of the source code is restricted by law or regulation, including—but not limited to—patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulation, and the Federal laws and regulations governing classified information;
- The sharing of the source code would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy;
- The sharing of the source code would create an identifiable risk to the stability, security, or integrity of the agency's systems or personnel;
- The sharing of the source code would create an identifiable risk to agency mission, programs, or operations; or
- The CIO believes it is in the national interest to exempt sharing the source code.

---

# Implementation

## – Roles and Responsibilities

- The Federal Information Technology Acquisition Reform Act (FITARA)<sup>32</sup> creates clear responsibilities for agency CIOs related to IT investments and planning, as well as requiring that agency CIOs be involved in the IT acquisition process. OMB’s FITARA implementation guidance<sup>33</sup> established a “common baseline” for roles, responsibilities, and authorities of the agency CIO and the roles of other applicable Senior Agency Officials in managing IT as a strategic resource. Accordingly, agency heads must ensure that CIOs and Senior Agency Officials,<sup>34</sup> including CAOs, are positioned with the responsibility and authority necessary to implement the requirements of this policy. As appropriate, Senior Agency Officials should also work with the agency’s public affairs staff, open government staff, web manager or digital strategist, program owners, and other leadership to properly identify, publish, and collaborate with communities on their OSS projects.
- Moreover, in support of the objectives and requirements of this policy, agencies should strengthen internal capacity to efficiently and securely deliver OSS as part of regular operations. Additional information on this topic will be provided on Code.gov.

---

# Implementation

## Code Inventories and Discovery

- Inventories are a means of discovering information such as the functionality and location of potentially reusable or releasable custom-developed code. Within 120 days of the publication date of this policy, each agency must update—and thereafter keep up to date—its inventory of agency information resources to include an enterprise code inventory that lists custom-developed code for or by the agency after the publication of this policy. **Each agency's inventory will be reflected on Code.gov**. The inventory will indicate whether the code is available for Federal reuse, is available publicly as OSS, or cannot be made available due to a specific exception listed in this policy. Agencies shall fill out this information based on a metadata schema that OMB will provide on Code.gov.

---

# Implementation

## Code Repositories

- Accessible, buildable, version-controlled repositories for the storage, discussion, and modification of custom-developed code are critical to both the Government-wide reuse and OSS pilot program sections of this policy. Agencies should **utilize existing code repositories and common third-party repository platforms as necessary in order to satisfy the requirements of this policy.**<sup>36</sup> Code.gov will contain additional information on this topic.

## Licensing

- Licensing is a critical component of OSS and can affect how the source code can be used and modified. Accordingly, when agencies release custom-developed code as OSS, they **shall append appropriate OSS licenses to the source code.** Additional information on licensing will be available on Code.gov.

---

# Implementation

## Agency Policy

- Within 90 days of the publication date of this policy, each agency’s CIO—in consultation with the agency’s CAO—shall develop an agency-wide policy that addresses the requirements of this document. For example, the policy should address how the agency will ensure that an appropriate alternatives analysis has been conducted before considering the acquisition of an existing commercial solution or a custom-developed solution. In accordance with OMB guidance,<sup>37</sup> these policies will be posted publicly. Moreover, within 90 days of the publication date of this policy, each agency’s CIO office must correct or amend any policies that are inconsistent with the requirements of this document, including the correction of policies that automatically treat OSS as noncommercial software.

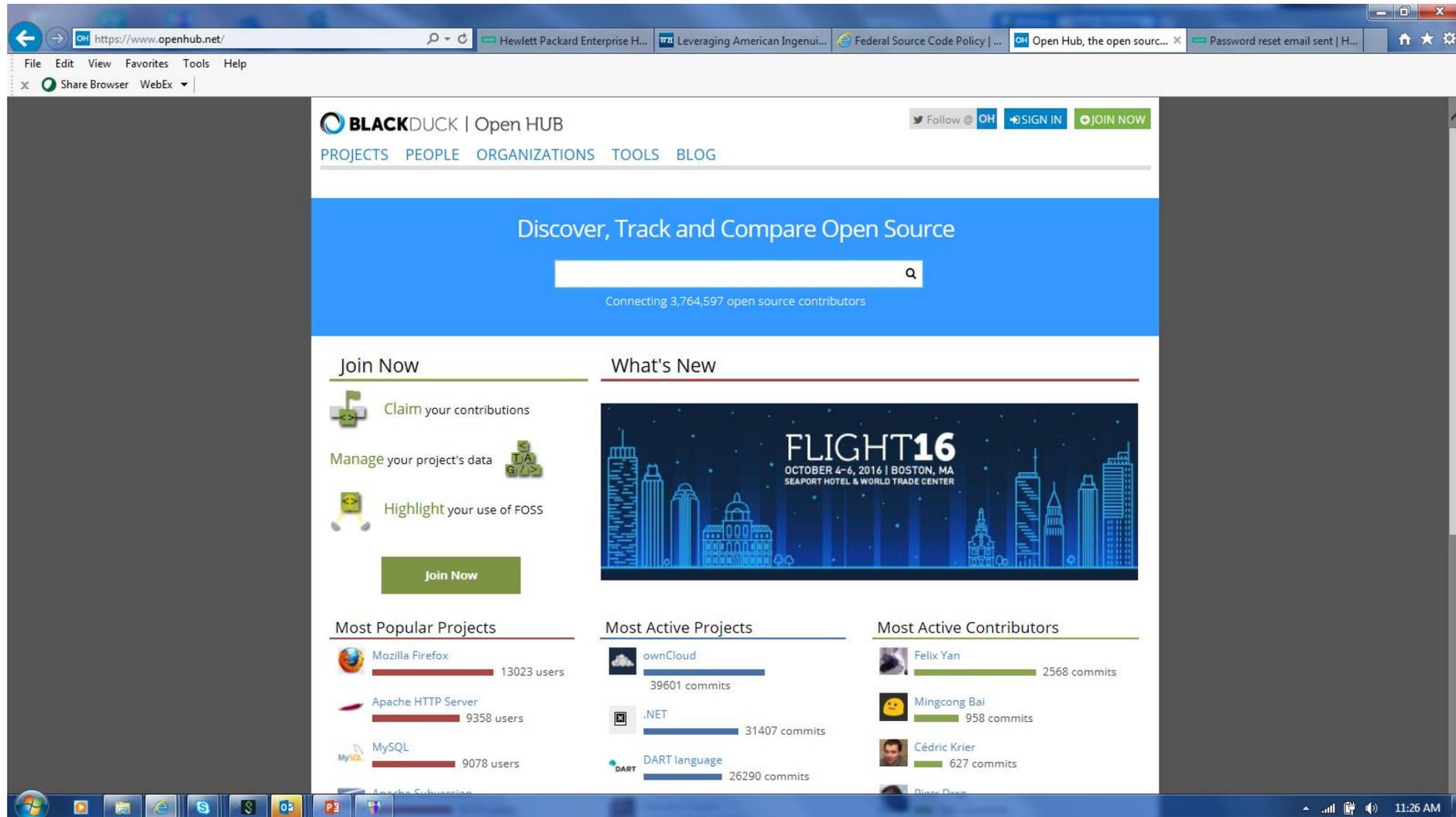
## Accountability Mechanisms

- Progress on agency implementation of this policy will be primarily assessed by OMB through an analysis of each agency’s internal Government repositories, public OSS repositories, and code inventories on Code.gov, as well as data obtained through the quarterly Integrated Data Collection (IDC), quarterly PortfolioStat sessions, the IT Dashboard, and additional mechanisms to be provided via Code.gov.

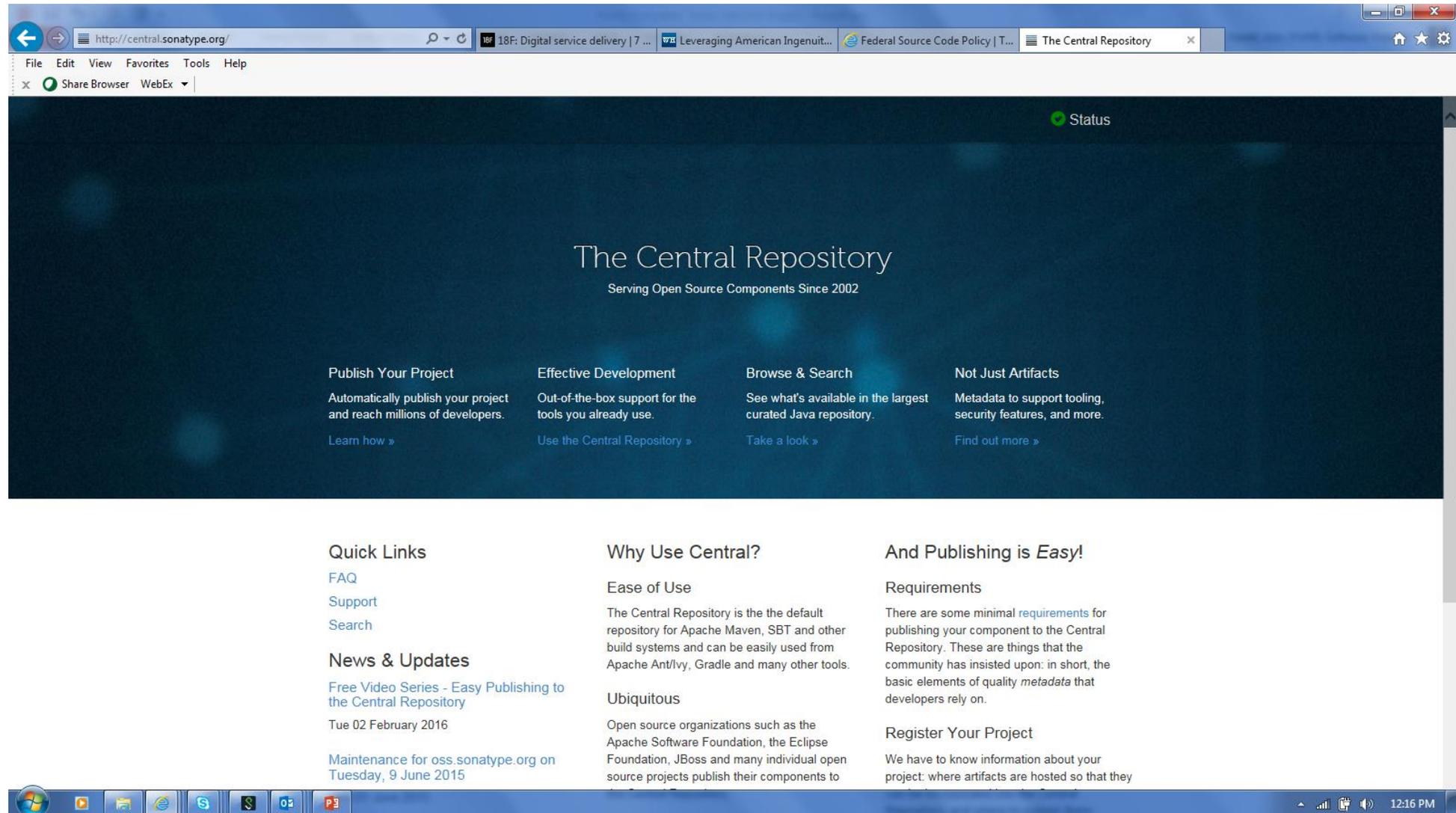
---

# What are the vendors doing to support these objectives?

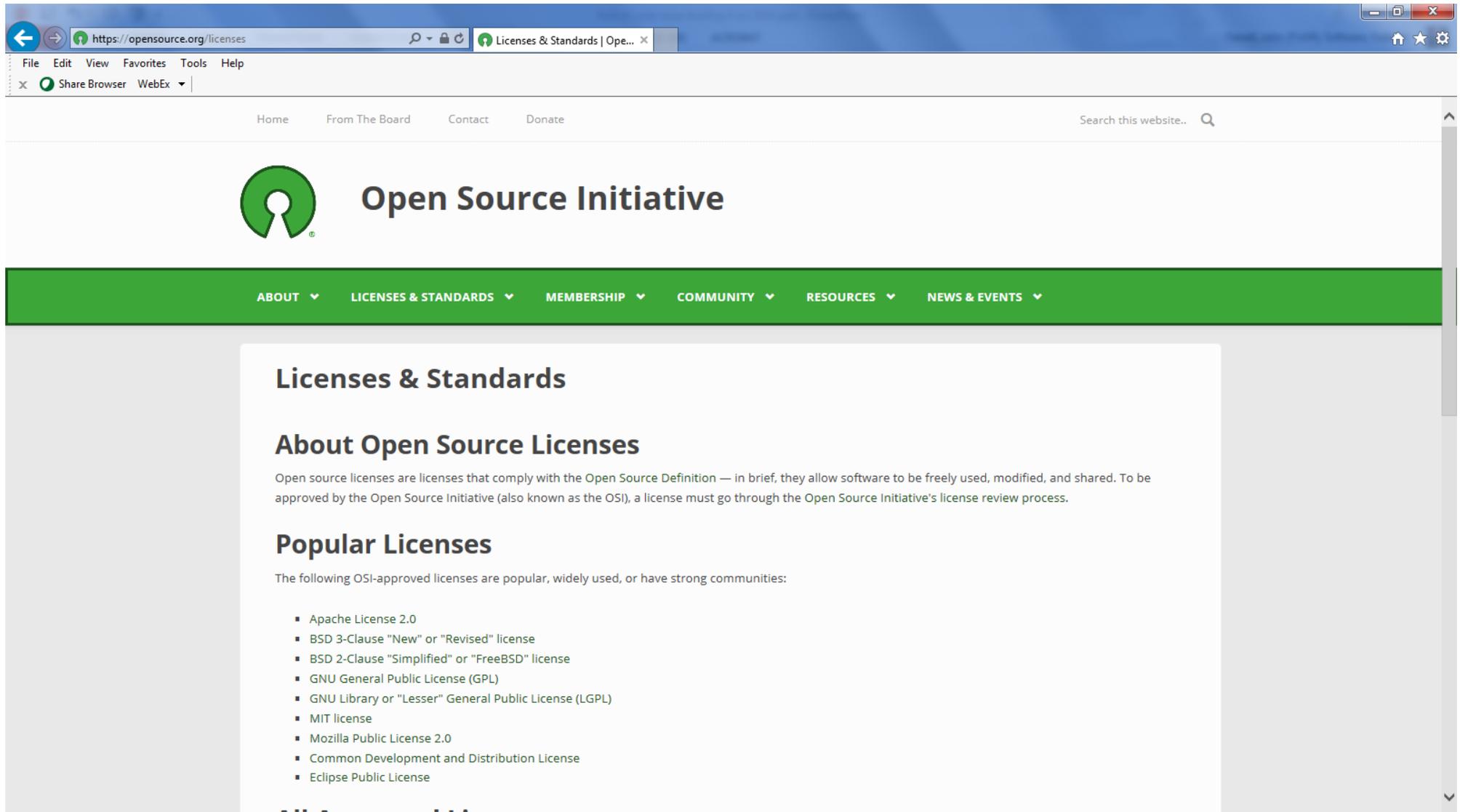
# Offering Directories of Open Source Code



# Supporting Open Source Code Development



# Communicating Licensing Information



The screenshot shows a web browser window displaying the Open Source Initiative (OSI) website. The browser's address bar shows the URL <https://opensource.org/licenses>. The website's navigation menu includes links for Home, From The Board, Contact, and Donate, along with a search bar. The main content area features the OSI logo and the title "Open Source Initiative". A green navigation bar contains dropdown menus for ABOUT, LICENSES & STANDARDS, MEMBERSHIP, COMMUNITY, RESOURCES, and NEWS & EVENTS. The current page is titled "Licenses & Standards" and includes a sub-section "About Open Source Licenses" with a paragraph explaining the OSI's license review process. Below this is a "Popular Licenses" section listing several OSI-approved licenses.

## Licenses & Standards

### About Open Source Licenses

Open source licenses are licenses that comply with the Open Source Definition — in brief, they allow software to be freely used, modified, and shared. To be approved by the Open Source Initiative (also known as the OSI), a license must go through the Open Source Initiative's license review process.

### Popular Licenses

The following OSI-approved licenses are popular, widely used, or have strong communities:

- Apache License 2.0
- BSD 3-Clause "New" or "Revised" license
- BSD 2-Clause "Simplified" or "FreeBSD" license
- GNU General Public License (GPL)
- GNU Library or "Lesser" General Public License (LGPL)
- MIT license
- Mozilla Public License 2.0
- Common Development and Distribution License
- Eclipse Public License

# Facilitating Collaboration on GOTS Code

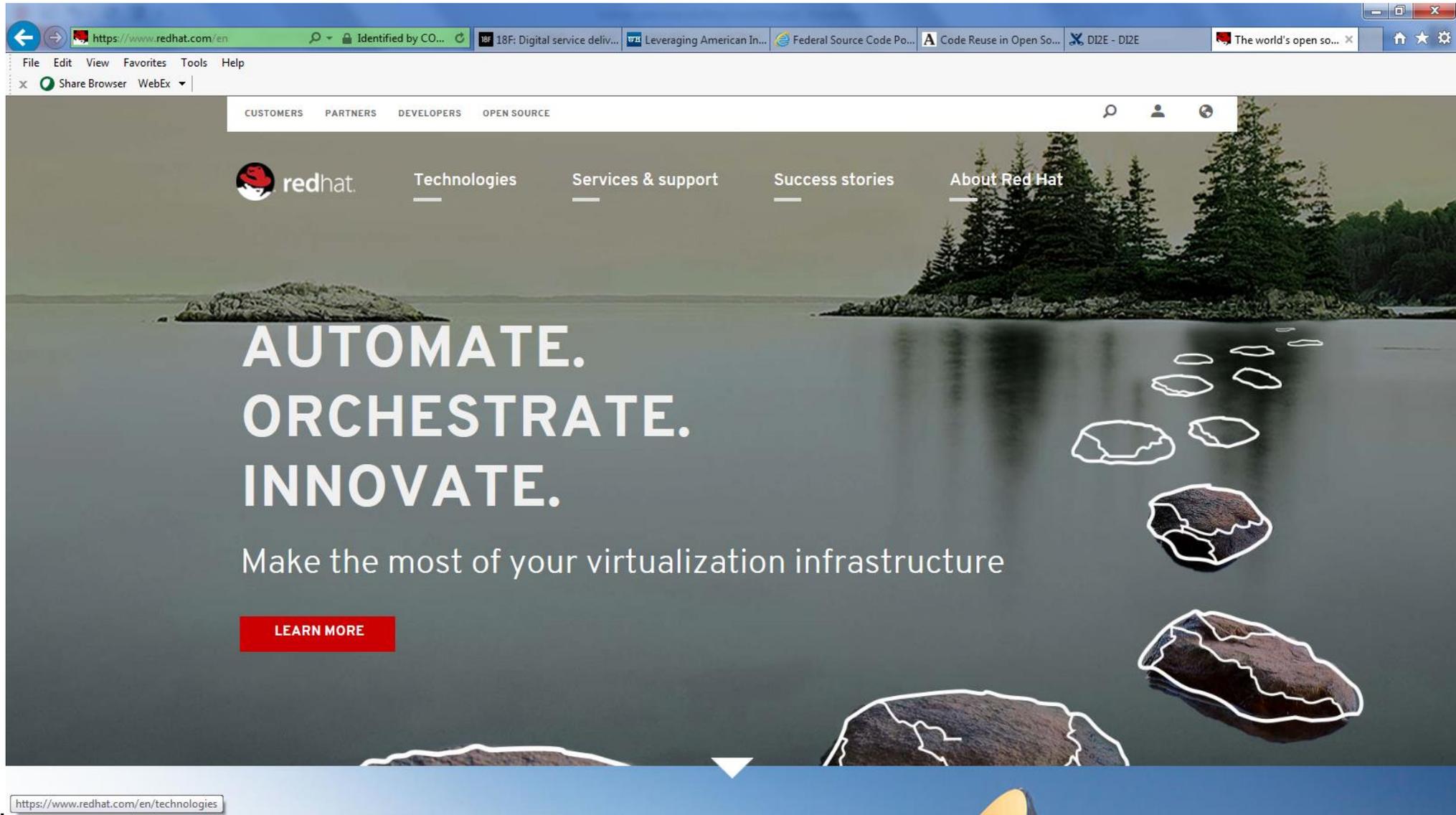
The screenshot shows a web browser window displaying the GitHub organization page for the National Geospatial-Intelligence Agency (NGA). The browser's address bar shows the URL <https://github.com/ngageoint>. The page header includes navigation links for Personal, Open source, Business, and Explore, along with a search bar and buttons for Sign in and Sign up.

The main content area features the NGA profile, which includes the organization's logo, name, and description: "Official organizational account for the NGA". Below the profile, there are tabs for Repositories and People. The Repositories tab is active, showing a list of repositories with their names, languages, star counts, and fork counts. Each repository entry also includes a brief description and the time it was last updated.

Repository Name	Language	Stars	Forks	Description	Updated
scale	JavaScript	44	18	Containerized processing framework for algorithms focused on remote sensing	Updated 6 minutes ago
hootenanny	C++	86	29	high-performance conflation software	Updated 29 minutes ago
hootenanny-ui	JavaScript	10	5	Hootenanny UI is a submodule of the Hootennanny vector conflation project.	Updated 4 hours ago
disconnected-content-explorer-iOS	Objective-C	11	9	Disconnected-Intelligence Content Explorer (DICE) is a new iOS, Android and...	

The 'People' section shows four team members, each with a profile picture and a green four-leaf clover icon.

# Innovating Open Source Products



# Leveraging Open Source Data

http://www.cloudera.com/why-cloudera.html

File Edit View Favorites Tools Help

Share Browser WebEx

Downloads Training Support Portal Partners Developers Community

Search Sign In Language

**cloudera**

[Why Cloudera](#) [Products](#) [Services & Support](#) [Solutions](#) [Get Started](#)

## No one knows Apache Hadoop like Cloudera

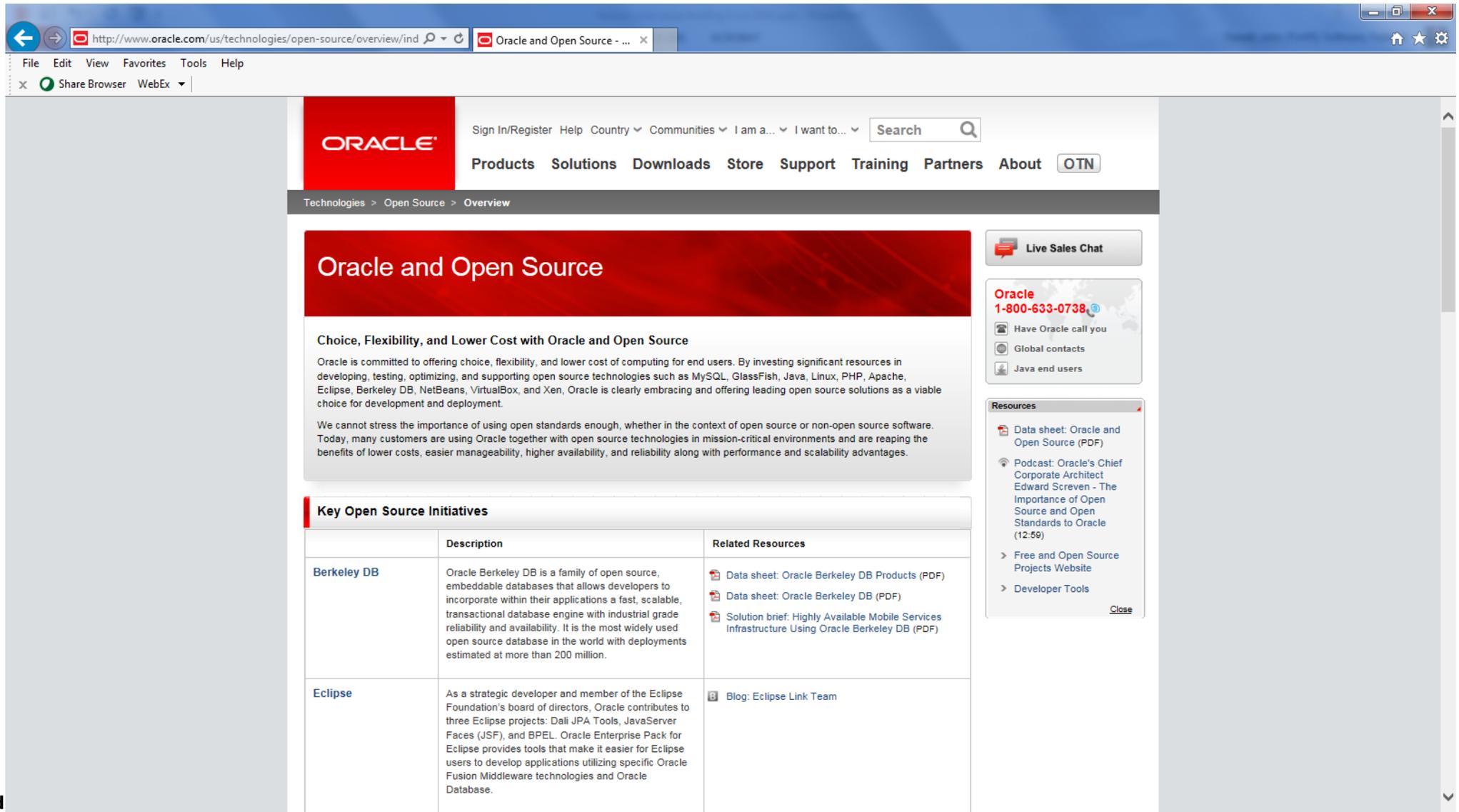
We provide the world's fastest, easiest, and most secure data platform built on Hadoop. We help solve your most demanding business challenges with data.

[CLOUDERA SOLUTIONS](#) [THE CLOUDERA STORY](#)

Why Cloudera

Build your business from the data up

# Investing in Open Source Code Development



The screenshot shows the Oracle Open Source Overview page. The page features a red header with the Oracle logo and navigation links. The main content area is titled "Oracle and Open Source" and includes a sub-header "Choice, Flexibility, and Lower Cost with Oracle and Open Source". Below this, there is a paragraph of text and a section titled "Key Open Source Initiatives" which contains a table with two rows: Berkeley DB and Eclipse. The table columns are Description and Related Resources. On the right side of the page, there are several widgets: "Live Sales Chat", "Oracle 1-800-633-0738" with contact options, and a "Resources" section with links to PDFs and a podcast.

ORACLE

Sign In/Register Help Country Communities I am a... I want to... Search

Products Solutions Downloads Store Support Training Partners About OTN

Technologies > Open Source > Overview

## Oracle and Open Source

### Choice, Flexibility, and Lower Cost with Oracle and Open Source

Oracle is committed to offering choice, flexibility, and lower cost of computing for end users. By investing significant resources in developing, testing, optimizing, and supporting open source technologies such as MySQL, GlassFish, Java, Linux, PHP, Apache, Eclipse, Berkeley DB, NetBeans, VirtualBox, and Xen, Oracle is clearly embracing and offering leading open source solutions as a viable choice for development and deployment.

We cannot stress the importance of using open standards enough, whether in the context of open source or non-open source software. Today, many customers are using Oracle together with open source technologies in mission-critical environments and are reaping the benefits of lower costs, easier manageability, higher availability, and reliability along with performance and scalability advantages.

#### Key Open Source Initiatives

	Description	Related Resources
<a href="#">Berkeley DB</a>	Oracle Berkeley DB is a family of open source, embeddable databases that allows developers to incorporate within their applications a fast, scalable, transactional database engine with industrial grade reliability and availability. It is the most widely used open source database in the world with deployments estimated at more than 200 million.	<ul style="list-style-type: none"><li>Data sheet: Oracle Berkeley DB Products (PDF)</li><li>Data sheet: Oracle Berkeley DB (PDF)</li><li>Solution brief: Highly Available Mobile Services Infrastructure Using Oracle Berkeley DB (PDF)</li></ul>
<a href="#">Eclipse</a>	As a strategic developer and member of the Eclipse Foundation's board of directors, Oracle contributes to three Eclipse projects: Dali JPA Tools, JavaServer Faces (JSF), and BPEL. Oracle Enterprise Pack for Eclipse provides tools that make it easier for Eclipse users to develop applications utilizing specific Oracle Fusion Middleware technologies and Oracle Database.	<ul style="list-style-type: none"><li>Blog: Eclipse Link Team</li></ul>

Live Sales Chat

Oracle  
1-800-633-0738

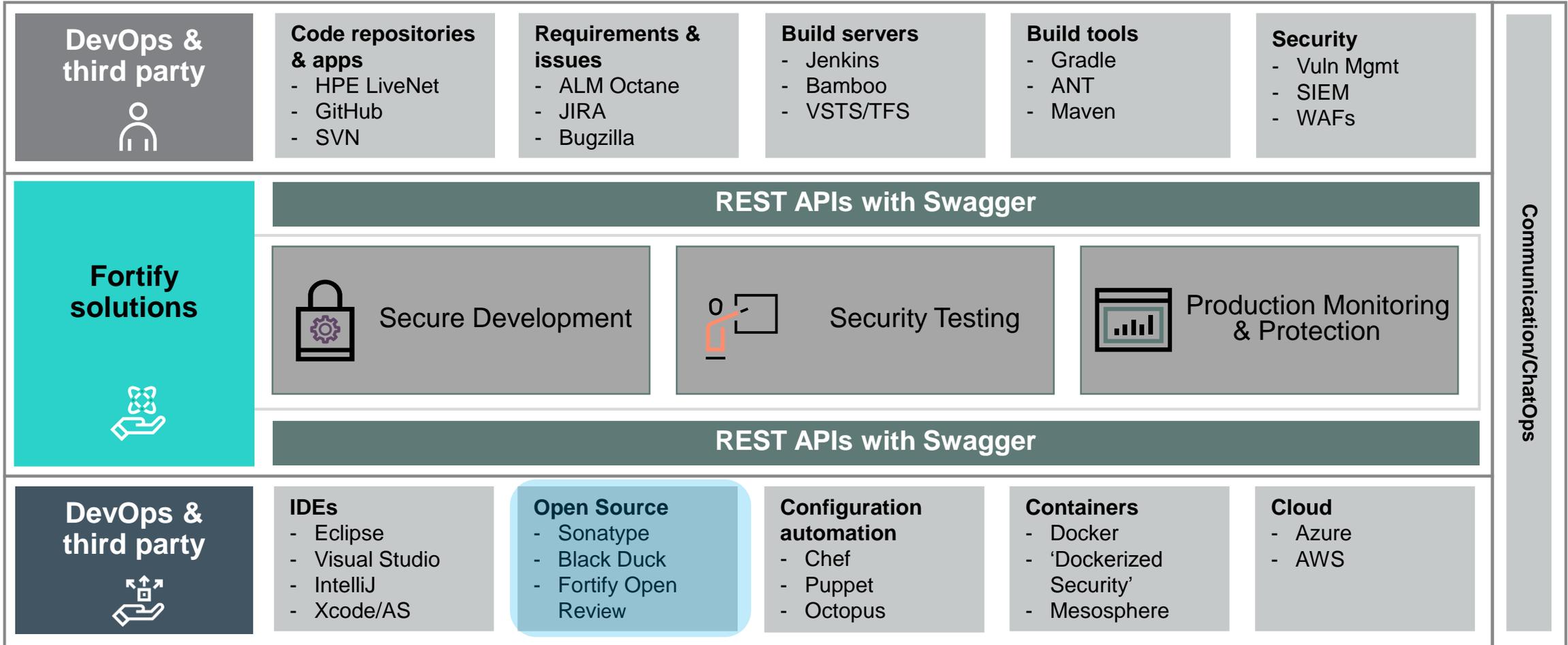
- Have Oracle call you
- Global contacts
- Java end users

Resources

- Data sheet: Oracle and Open Source (PDF)
- Podcast: Oracle's Chief Corporate Architect Edward Screven - The Importance of Open Source and Open Standards to Oracle (12:59)
- > Free and Open Source Projects Website
- > Developer Tools

Close

# Securing Custom Built and Open Source Applications



# Integrating Offerings

**FORTIFY ON DEMAND** Dashboard Applications Reports Administration

**WebGoat Java > v6.0.1**

Rating: ★★★★★ Status: **Fail** [edit](#)

Show Fixed Send to WAF/IPS Re-Im

Total	Static	Dynamic	Network
<b>1092</b>	Status: <b>Completed</b> 889 Last Scan: 05/27/2015 (Scan ID: 742)	Status: <b>Not Scanned</b> 0 Last Scan: none	Status: <b>Completed</b> Last Scan: 11/24/2015 (Scan ID: 4715)

32 Components Identified 91% of all components are open source

47 Security Issues Affecting 6 components

3 License Alerts [View Interactive Report](#)

Component	Version	Known Public Vulnerabilities	License
org.apache.struts: struts2-core	2.0.11	12 Critical, 10 High, 0 Medium, 0 Low	Apache-2.0 No Sources
com.opensymphony: xwork	2.0.4	8 Critical, 7 High, 1 Medium, 1 Low	Apache-1.1 Apache-2.0, BSD-3
struts: struts	1.1	3 Critical, 1 High, 0 Medium, 0 Low	Not Declared Non-Standard
freemarker: freemarker	2.3.8	1 Critical, 1 High, 0 Medium, 0 Low	BSD Non-Standard

**Hewlett Packard Enterprise** Dashboard Search

Applications Reports Administration Help

**Bill Payment Processor | 1.1 | Overview**

Version 1.1 Overview Artifacts Audit Trend Filter Set PCI Auditor View Profile New Version

Top Risk Makers Group by Analysis Ty... Filter by Select attributes Advanced...

**Reviewed** **Pending Review**

BLACK DUCK SOFTWARE (13%)

**Todo List**

**Alerts**  
No pending unread alerts  
[Show all alert notifications](#)

**Version Progress**

Last measured on 07/06/2016 3:22:22 PM

Total Issues	854
Total Issues Audited %	96.5%
Critical Priority Issues	105
Critical Priority Issues Audited %	88.6%
Fortify Security Rating	1

**FORTIFY ON DEMAND** Dashboard Applications Reports Administration

**WebGoat Java > v6.0.1**

Open Source Components by Sonatype [Download Sonatype Report](#)

Summary Security Issues License Analysis

This report provides security and license assessments for open source components found within an application.

**Scope of Analysis**

32 COMPONENTS IDENTIFIED 91% OF ALL COMPONENTS ARE OPEN SOURCE

11 POLICY ALERTS AFFECTING 23 COMPONENTS

77 SECURITY ALERTS AFFECTING 6 COMPONENTS

5 LICENSE ALERTS

**Security Issues**

How bad are the vulnerabilities and how many are there?

Threat Level	Count
Critical (7-10)	36
Severe (4-6)	33
Moderate (1-3)	8

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application. The dependency depth highlights quantity and severity and distribution within the application's dependencies.

**License Analysis**

What type of licenses and how many of each?

Threat Level	Count	Percentage
Critical (8-10)	0	15%
Severe (4-7)	4	4%
Moderate (1-3)	1	

The summary of license analysis demonstrates the number of licenses detected in each category. The dependency depth compares quantity by category and the distribution within your application's dependencies.

---

# References

– **M-16-21 MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES**

<https://sourcecode.cio.gov/>

– **Leveraging American Ingenuity through Reusable and Open Source Software**

March 10, 2016 at 9:00 AM ET by Tony Scott

<https://www.whitehouse.gov/blog/2016/03/09/leveraging-american-ingenuity-through-reusable-and-open-source-software>

– **Code Reuse in Open Source Software Development: Quantitative Evidence, Drivers, and Impediments**

**Manuel Sojer** , Technische Universität München (TUM) - TUM School of Management

**Joachim Henkel** , TUM School of Management - Technische Universität München (TUM); Centre for Economic Policy Research (CEPR)

March 9, 2010, *Journal of the Association for Information Systems*, Vol. 11, No. 12, pp. 868-901, 2010

---

**Thank You**

**[jmfarrell@hpe.com](mailto:jmfarrell@hpe.com)**