Coalition for Enterprise Open Source Software for Government

The main goal of CEOSSG is to ensure that EOSS vendors have a fair opportunity to compete against OSS acquisitions.

Open Source Software as an Innovation Agent

Open Source Software (OSS) is widely available, and fundamentally changing the way agencies develop and deploy technology solutions. Forward-thinking federal agencies are using the collaborative nature of OSS to fuel innovation. They are leveraging the knowledge of a widespread community to build and improve application functionality. As more federal IT organizations adopt OSS, they are accelerating at a pivot point away from the closed-source, proprietary software that once defined it.

The Coalition for Enterprise Open Source Software in Government (CEOSSG) was established to advocate for more effective OSS acquisitions. CEOSSG seeks to educate federal stakeholders on the differences between Free Open Source Software (FOSS) and Enterprise Open Source Software (EOSS). While officials in the General Service Administration (GSA) and the Office of Management and Budget (OMB) are promoting the adoption and utilization of OSS on a government-wide basis, Federal Agency end users often choose FOSS over EOSS. This is due to the perception that downloading “free” software is easier. Agency Contracting Officers and Program Managers often overlook the add-on costs associated with modifying the “free” OSS life-cycle costs against the cost of fully supported EOSS software.

The main goal of CEOSSG is to ensure that EOSS vendors have a fair opportunity to compete against OSS acquisitions. These acquisitions must comprehensively consider the actual cost of modifying “free” community-based OS solutions. These costs include the labor costs associated with “productizing” FOSS and making FOSS application selection based on all projected costs ensures compliance with Federal Acquisition Regulations (FAR). It also provides a level playing field for EOSS vendors, who price their solutions based on the cost they have already incurred to ensure scalability and compliance with federal information security requirements.

Free Open Source Software (FOSS) vs. Enterprise Open Source Software (EOSS)

The name FOSS is deceiving, as there is no “free” software. While the code is free to use, it requires an investment of man-hours to make it operational. The agency can download, view, and work on

The cyber and performance advantages of EOSS, include:

- Using EOSS removes any uncertainty about security or stability, as it is subjected to rigorous testing, evaluation, and certification prior to release.
- EOSS vendors provide on-demand customer support by trained software engineers, providing users an immediate and reliable source of assistance, which includes software patches.
- EOSS solutions deliver plug and play functionality, whereas FOSS requires labor hours to fix bugs, employ security patches, and to understand the software's full functionality.

the underlying code for free. Support is not included. The agency largely relies on community discussion boards where users can post questions or problems, with no guarantee of a response or solution.

EOSS combines the flexibility of FOSS with the support and stability of traditional IT software. With EOSS, the vendor provides the underlying source code along with support and certifications that guarantee security, reliability, and consistency.

In a 2011 IDC study, EOSS was proven more cost-effective than FOSS. This study compared organizations using Red Hat Enterprise Linux against organizations using free community-supported Linux. The study found that using EOSS can result in substantial cost savings.

Federal agencies that use FOSS in critical applications are taking significant cyber risk. A recent Center for Strategic and International Studies (CSIS) report found that FOSS components include "code that is not owned by anyone responsible vendor or party — and thus often goes unmaintained." This leads to hidden vulnerabilities that are often left unprotected for years. According to From Awareness to Action — A Cybersecurity Agenda for the 45th President, federal agencies need to address these cyber risks when using FOSS to support critical agency applications. With EOSS, the vendor has already addressed these risks consistent with federal cybersecurity standards and requirements.

Helping the Government Adopt Open Source, Responsibly

CEOSSG seeks to educate federal cybersecurity stakeholders in the Executive Office of the President and Congress on the cyber vulnerabilities associated with mission-critical applications built on FOSS. Agency CIOs should be encouraged to examine whether the FOSS applications they are running have up-to-date security patches. This review is critical to mitigating software vulnerabilities.

CEOSSG is committed to educating federal IT stakeholders in executive branch agencies and in Congress on the importance of ensuring fair and open OSS acquisitions.

1860 Michael Faraday Drive, Suite 100 | Reston, VA 20190 | Phone: 703.871.8629 | Fax: 703.871.8505 | www.ceossg.org