The U.S. Army and Red Hat – Taking Ownership of IT through Choice, Control and Innovation

With the current budget cuts and the looming certainty of more to come, this is a critical time for Defense. While infrastructure costs continue to increase, if current trends continue, the costs to maintain the enterprise will exceed even the most liberal resource projections. It's clear today that senior leadership knows that a significant comprehensive change is urgently required.

Open Source Software (OSS) has, for years, brought together the best and brightest developers to produce software products that rival commercial solutions on every level. Department of Defense (DoD) agencies of all sizes are continuing to realize the power and savings that open source solutions provide to mission critical operations. An example of this is Mil-OSS.org, which exists to improve technology development and innovation across the DoD.

In 2009 the DoD issued a memo providing clarification and guidance to establish the definitive interpretation of Open Source Software (OSS) as being "commercial" and therefore given preferential treatment in the acquisition process and extended that interpretation to all military services. The memo expresses confidence in the OSS security model: "*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*."

With over 200,000+ instances deployed Army wide, Red Hat's OSS has had a tremendous impact on reducing costs and increasing agility within the enterprise in U.S. Army programs like, but not limited to, DCGS-A, AESIP, LMP, PM AcqBusiness, PD ALTESS, LMP, GCSS-A, AESIP Hub, GFEBS, DLS, PM WIN-T, NETCOM, ARCYBER, JLCCTC, WARSIM, AVCATT, CCTT, VCOTS, iPERMS, GoArmy, BEP, IPPS-A and PM JBC-P.

The Army's own **Common Operating Environment** prescribes an open standards approach, which makes it easier for the Army to entertain a number alternatives for critical infrastructure tools. Similarly, the Federal Shared Services Implementation Guide makes it clear that procurements for cloud infrastructure should include a clear "exit strategy" to encourage more choice and more control over the Army's computing platform. In the private sector, we have seen an explosion of innovation using these principles – leading cloud providers like Facebook, Google, and Amazon are built around open source software. Red Hat believes the Army should focus on driving innovation with the utilization of more open source and open standards-based tools.

About Red Hat

Red Hat is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux, and middleware technologies.

Red Hat also offers award-winning support, training, and consulting services. Red Hat is an S&P company with more than 70 offices spanning the globe, empowering its customers' operations.

The Army is at a critical juncture – it's time for a fresh approach.

Here's why:

Red Hat and the U.S. Army – The Future Has Never Been More Open

Red Hat's partnership with the U.S. Army spans 10 years starting with the deployment of Red Hat Enterprise Linux in 2002 and, to this day, the U.S. Army remains one of Red Hat's largest customers by volume.

During this period, and through the use of its key open source subscription, the Army and the DoD at large has reduced its lower total cost of ownership (TCO) of IT systems by millions of dollars, while significantly reducing aspects of proprietary vendor lock-in and integration complexity, all while maintaining the highest security posture and mission-emphasis.

Taking ownership of IT infrastructure through open source technology is nothing new in the DoD. Deep budget cuts are driving radical change in the way government agencies procure, develop, and deploy technology solutions. Several government agencies (notable the NSA, Whitehouse.gov, and the Veteran's Administration) are just a few examples of agencies who are encouraging the use of open source software in critical mission areas. In late 2011, the **National Geospatial-Intelligence Agency (NGA)** issued a public release[1] outlining its intent to shift its IT infrastructure away from a heavy reliance on commercial proprietary software to no-cost/low-cost open source applications and software solutions.

Red Hat Enterprise Linux and JBoss Enterprise Middleware are key components of many strategic, tactical, enterprise and simulation systems and programs including:

- U.S. Army Appendix C Future State Common Operating Environment (COE)
- PEO EIS
- PEO C3T
- PEO STRI
- Human Resources Command
- Army G1
- CIO/G6
- ASALT
- RDE-COM

Citing the "*overwhelming burden*" of rising IT costs and shrinking budgets, coupled with a need for greater technological agility, NGA management was resolute in the shift in its approach: "*It is clear today to the senior leadership that significant comprehensive change is urgently required*".

For NGA the shift towards open source technology creates several advantages: "*…we can reduce our total cost to own and operate (our) vast technology infrastructure,…we will be able to respond more quickly, more effectively, and with greater agility to leverage and exploit mission successes…We will be able to take ownership of our software applications, tailor and customize them in response to unique operational needs."* Finally*: "…we will accelerate the pace of innovation, while reducing our dependence on commercial vendors and external system integrators and the risks associate with commercial software licenses*."

NGA isn't alone. The public and private sector alike no longer argue whether open source is secure or not or whether it's safe to use. The focus now is on how best to tie open source to long-term strategy while getting the best value for every tax dollar.

[1] "Taking Ownership of IT Infrastructure through Open Source Technology (OST)" National Geospatial-Intelligence Agency Innovision Directorate. Approved for Public Release 11-401

One example of the cost reduction benefits of open source can be seen with the DoD's **PM AcqBusiness** cloud initiative, which is anticipated to save $5.1 million through fiscal year 2015. PM AcqBusiness is the only Army system implementing a "cloud capable" infrastructure.

Using a complete open source solution integrated with Red Hat Enterprise Linux, Red Hat JBoss Middleware, and Red Hat Enterprise Virtualization, together with partners Nagios and Puppet, the DoD achieved substantial savings thanks to a reduced TCO, reduced licensing costs for legacy Oracle systems, and the deployment of a modern NIST-compliant infrastructure which eliminated problems in system performance during usage spikes.

> "*When we rolled into Baghdad, we did it using open source. It may come as a surprise to many of you, but the U.S. Army is the single largest install base for Red Hat Enterprise Linux*."
>
> Brigadier General Nick Justice, PEO C3T, Linux.com, 2007

The infrastructure deployment will enable one of the first implementations of a private cloud with automated elasticity within DoD and is positioned as a repeatable template for future Army and DoD requirements with larger infrastructures. All that's needed is additional storage and CPU power and the Army can build upon the economies of scale being realized by PM AcqBusiness.

Red Hat Open Source Solutions – A Foundation for "Doing More with Less"

In alignment with the DoD directive - "*Implementation Directive for Better Buying Power - Obtaining Greater Efficiency and Productivity in Defense Spending*" – we believe that scalable, trustworthy and secure Red Hat solutions can improve the effectiveness of the DoD enterprise. Together, we can achieve its directives to do more, without more, through: "*…affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition*."

In this section, we'll explore how Red Hat solutions can help the Army meet key directives, achieve mission goals, and "do more with less":

More than two decades ago, Red Hat had a spark of an idea – a vision for developing better software. Then and now, collaboration with an ecosystem of IT leaders, open source advocates, developers, and partners creates the perfect foundation for the future of IT– Red Hat Enterprise Linux. But that was just the beginning.

The Red Hat open source software development model has produced high-performance, cost-effective solutions. Our model mirrors the highly interconnected world we live in and takes advantage of the ability to share ideas and information worldwide, in seconds. It allows customers to enjoy the highest levels of technology innovation while remaining aligned with real-world business requirements.
Unlike traditional software licensing and maintenance agreements, all Red Hat software solutions are procured using a ***subscription model***. A subscription provides a cost advantage in situations where many copies of the software may be required and can mitigate the risk of cost growth – a risk factor in the licensing and maintenance model.

With subscription, agencies pay an annual cost that's easy to budget for since the cost only increases if you purchase additional subscriptions – there are no unbudgeted for updated costs, upgrades or hidden charges. Instead, your subscription gives you Red Hat enterprise open source solutions and everything you need to use them effectively. This includes, continuous access to all supported versions of the Red

Hat software in both binary and source form, including all security updates, bug fixes, unlimited access to technical support (whether you have a technical issue or a question), a knowledge base of information through our customer portal and most importantly software assurance that's required by the DoD.

With a Red Hat subscription, the Army not only gets a robust, scalable, and flexible IT application platform that meets its performance, security, and budgetary goals, you get access to world-class expertise and a culture of innovation and collaboration that will support the Army throughout the entire infrastructure life cycle.

Red Hat has five key areas of expertise that offer a specific way to stretch existing DoD IT budgets and meet the implementation DoD directive:

1. Enterprise Linux

Red Hat Enterprise Linux (RHEL) the world's most trusted IT platform. RHEL has been deployed in mission-critical applications and websites across the DoD and listed in the Army's Common Operating Environment Document as one of the two operating systems. Designed to help agencies make a seamless transition to emerging datacenter models that include virtualization and cloud computing, Red Hat Enterprise Linux includes support for major hardware architectures, hypervisors, and cloud providers, making deployments across physical and different virtual environments predictable and secure. Customers include, but aren't limited to, DCGS-A, PM AESIP, LMP, PM AcqBusiness, PD ALTESS, GCCS-J, GFEBS, PM WIN-T, NETCOM and PEO STRI.

2. Enterprise Virtualization

Red Hat offers virtualization products that meet both the needs for traditional datacenter virtualization as well as cloud computing. Red Hat Enterprise Virtualization (RHEV) is a comprehensive datacenter virtualization product for Linux and Windows workloads that enables users to build an agile, secure virtualization foundation with the features needed for traditional enterprise application workloads. For cloud computing, Red Hat Enterprise Linux OpenStack Platform is a fully supported OpenStack environment that allows customers to create secure, multi-tenant cloud computing enclaves in their own datacenters. Customers include, but aren't limited to, Human Resource Command, PM AcqBusiness.

3. Enterprise Middleware

JBoss Enterprise Middleware is the leading enterprise-class open source software used to build, deploy, integrate, orchestrate, and present web applications and services in a service-oriented architecture (SOA). These solutions offer federal agencies the best of both worlds: enterprise-class stability and open source innovation. It's the ideal middleware portfolio for open hybrid cloud environments across physical, virtual, mobile, and cloud environments. Customers include, but aren't limited to, Human Resource Command, PM AcqBusiness, DISA, DLA, DTRA, GCSS-A, GCSS-J, US Navy and WIN-T.

4. Storage

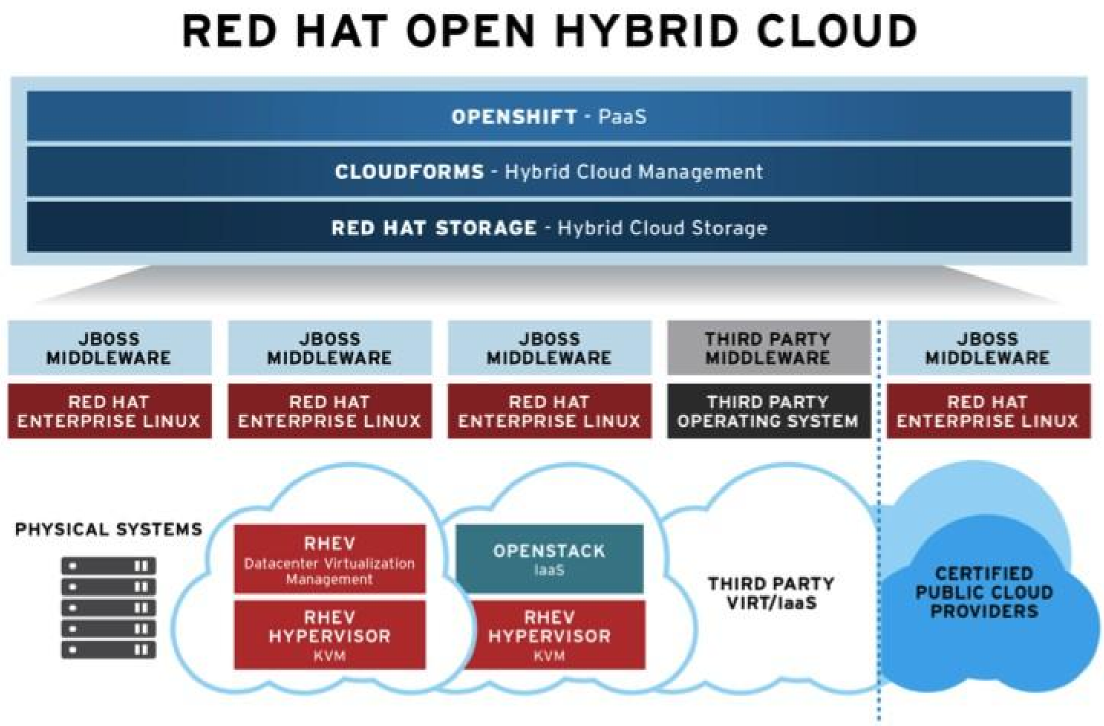
Red Hat Storage is an open, software-defined, scale-out storage platform that helps you manage the explosion of big, semi-structured, and unstructured data growth for physical, virtual, and cloud environments - while maintaining the storage performance, capacity, and availability needed to meet demanding enterprise storage requirements. Customers include, but aren't limited to, Pandora and NASA.

5. Open Hybrid Cloud

Cloud computing has evolved in recent years. The new world of the *hybrid cloud* is an environment that employs both private and public cloud services. The DoD is realizing that they need many different types of cloud services in order to meet a variety of customer needs. There are two primary deployment models of clouds: public and private. Most agencies will use a combination of private computing resources (data centers and private clouds) and public services, where some of the services existing in these environments touch each other — this is the open hybrid cloud environment. Customers include, but aren't limited to, PayPal, Dell and Autonomic Resources - a FedRAMP Certified Red Hat Partner.

By embracing Red Hat's open hybrid cloud portfolio, that includes CloudForms, OpenStack, Red Hat Enterprise Virtualization, Red Hat Enterprise Linux, Red Hat Storage, and OpenShift, you ensure the following benefits:

- ***Cloud Efficiencies Everywhere*** – An open hybrid cloud brings the benefits of cloud across all of your IT resources, not just a subset.
- ***You Avoid Cloud Silos*** – Building a cloud silo or turning an existing management silo into a cloud just increases overall IT management complexity
- ***Easy On-ramp Without Migration*** – An open hybrid cloud provides a straightforward path for enterprises, not an expensive migration process.
- ***You're in Control*** – An open hybrid cloud prevents one vendor from controlling your economic model and your access to innovation.
- ***Achieve the Ultimate in Portability and Interoperability*** – An open hybrid cloud allows you to manage applications and data across your choice of a diverse infrastructure.



The Red Hat Open Hybrid Cloud solves real business problems by providing interoperability, workload and data portability, open APIs, and freedom of choice across new and existing heterogeneous infrastructures.

In summary, by adopting Red Hat's supported low-cost OSS solutions at the enterprise program level, the Army can rapidly explore external technical advances, induct the best-in-class solutions, and then re-use all or parts of them to create unique new capabilities and lower TCO, without degrading the functionality, productivity, or mission effectiveness of current and future systems.

The Army can evolve processes, policies, and procedures in order to keep pace with emerging technologies, including advanced internet-based applications, cloud computing (more on this below) and storage alternatives, databases, virtualization, infrastructure outsourcing, distributed collaboration and development, an increasingly rich menu of social networking technologies, and other innovations that the Army currently can't exploit or absorb into the current IT environment without reallocating resources from other areas.

In the next section, we'll specifically discuss how Red Hat's open hybrid cloud infrastructure addresses the Federal Shared Services Implementation Guide call for cloud procurements to include a clear "exit strategy" and DoD control over its own computing environments.

Open Hybrid Cloud Computing with Red Hat – Future Proof Management Investment without Lock-In

In recent years, the private sector has seen an explosion of innovation using open source software principles – the leading cloud providers today, like Facebook, Google, and Amazon, are based on open source software. Red Hat believes the Army should focus on driving innovation with the utilization of more open source and open standards-based tools.

It's important to note that while open technologies help agencies virtualize faster, many proprietary and so-called "open" cloud solutions aren't compatible with existing DoD investments and present real challenges for enterprise IT processes and staff already faced with the increased complexity of managing virtualized infrastructures.

Red Hat, however, delivers the world's leading open source solutions for private clouds, hybrid clouds, and public clouds: Red Hat CloudForms for building and managing your own IaaS cloud plus the revolutionary OpenShift PaaS and the new Red Hat Enterprise Linux OpenStack Platform.

Red Hat's cloud solutions are unique. For example, the Red Hat open hybrid cloud uses resources the Army already has alongside a broad portfolio of open, interoperable virtualization and cloud-management products. It provides deep and useful analytics, streamlines management, and lowers IT costs – without vendor lock-in or limiting future innovation.

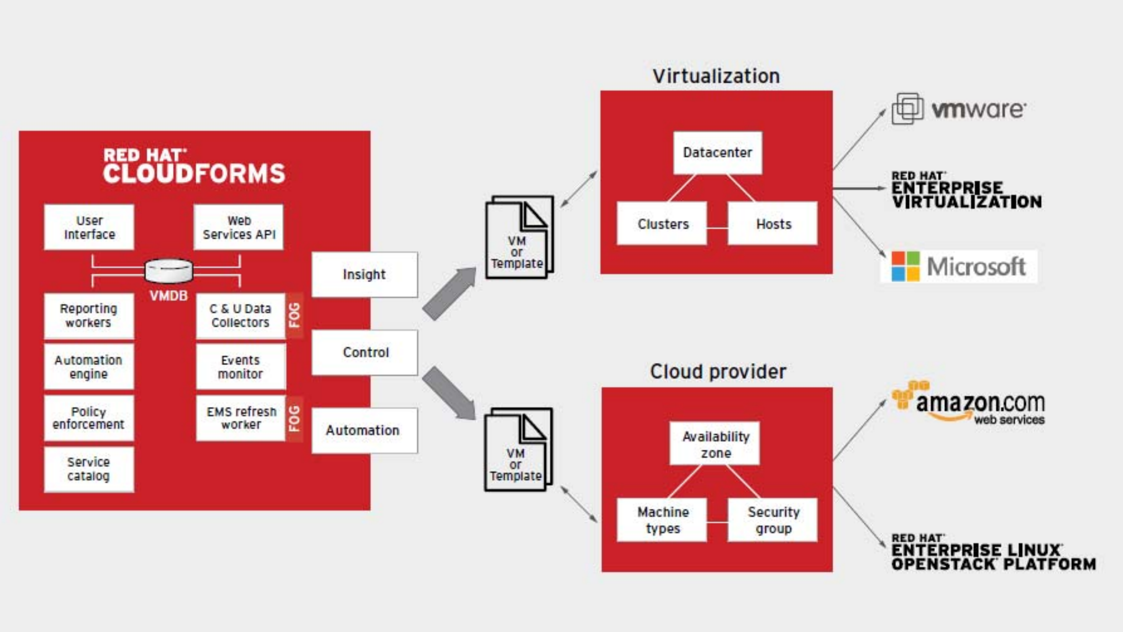
The following sub-sections address the features and benefits of CloudForms, Red Hat Enterprise Linux OpenStack platform, and OpenShift:

CloudForms: Manage Your Virtual, Private, and Hybrid Cloud Infrastructures

With CloudForms the Army can benefit from a unified management framework with advanced life cycle management capabilities across IaaS private and hybrid clouds, such as OpenStack, **VMware**, Red Hat, Microsoft and Amazon. Finding the right balance between a cloud user's control and autonomy is critical to the manageability, scalability, and, ultimately, the success of hybrid cloud environments, especially where public cloud resources are involved. CloudForms helps agencies achieve and maintain that balance through a flexible set of management and automation tools that enable a wide range of self-management activities. These tools provide policy-based visibility, control, and automation for workload instances in the public cloud, as well as the private (on-premise) cloud to effectively manage overall IT capacity and provide effective customer service.

With CloudForms users benefit from:

- ***Self-service provisioning and management*** – End users can request, provision, deploy, operate, manage, and decommission their own services configured with approval processes and enterprise standards enforced.
- ***Governing, tracking, and compliance*** – Deploy and manage clouds with policy-based control, mitigating risk associated with shared infrastructure. Secure role-based delegation, approval workflow, quota enforcement, and IT policies ensure service-level agreements.
- ***Cost allocation and charge-back*** – CloudForms enables cost transparency and accountability so that program managers and IT can understand the actual cost of the infrastructure required. Constantly monitor the actual consumption of server, storage, and network resources and organize by enterprise-specific classifications.
- ***Cloud brokering*** – Many agency CIOs and users are demanding an "Amazon-like cloud" that provides self-service provisioning, in reality, what they really require are self-managing systems that increase agility, while enforcing agency policies. These systems must meet fluctuations in demand, address variable workload demands, and continuously optimize resource allocation and resource demand. As the U.S. Army seeks to automate the provisioning process and provide self-service, cloud brokering becomes critical. By marrying infrastructure knowledge, with policies and business logic means customers have an adaptable management platform that can be relied on to allow a true self-service model and future-proof an organization's management investment. For example, if an Army IT department receives a request for a web application that will run in production, capacity exists in three Army clouds – VMware, RHEV and Amazon. However, since Army policy dictates that no production workloads can be run in the public cloud and that the lowest cost available resources must be used – RHEV and VMware clouds are left as the only option. RHEV, however, combined with OpenStack (more on this below) and CloudForms as a hybrid cloud management tool provides the lower licensing costs and the ideal automated environment to run traditional and cloud workloads such as this.



CloudForms: Manage existing investments in virtual, private, and hybrid cloud infrastructures – without vendor lock-in.

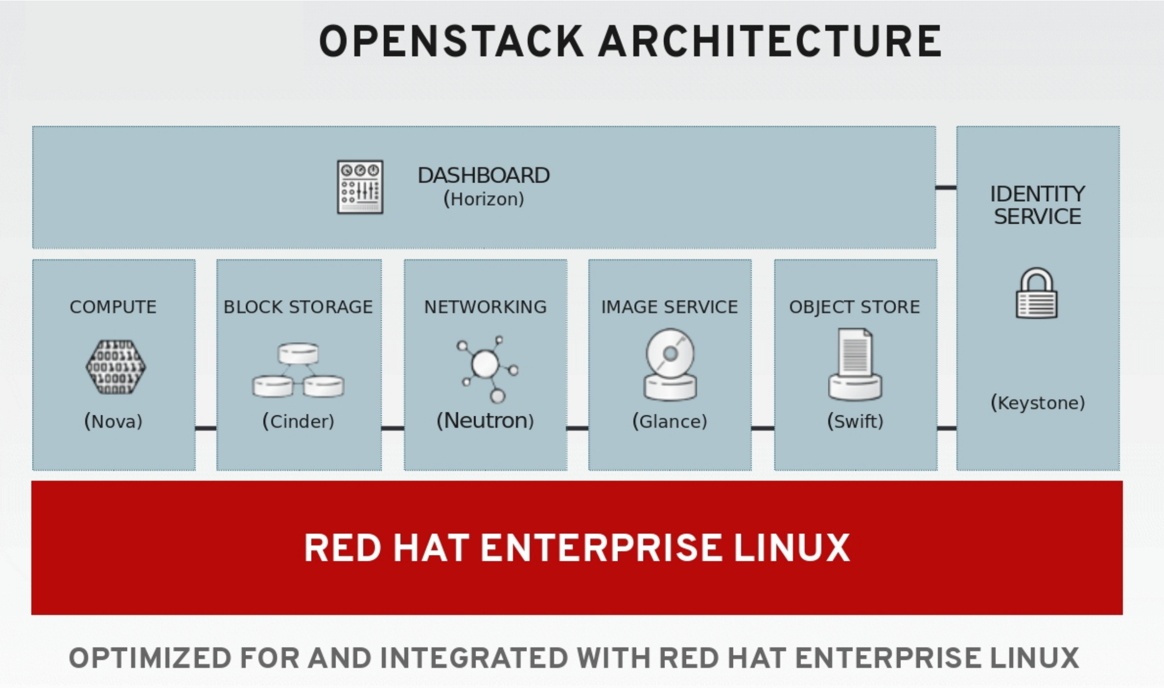
Red Hat Enterprise Linux OpenStack: Build an OpenStack-Powered Cloud

As part of Red Hat's open cloud portfolio, Army customers can also benefit from a commercially supported and tested version of OpenStack (an open source cloud system software project that has broad participation from the IT industry). The **Red Hat Enterprise Linux OpenStack Platform** serves as the foundation for advanced cloud users who are seeking to build an OpenStack-powered cloud. The solution is supported by a broad ecosystem of partners through the Red Hat OpenStack Cloud Infrastructure Partner Network, and designed to make it easier for enterprises to adopt OpenStack for building a private or public cloud.

Using Red Hat Enterprise Linux OpenStack Platform users can develop and deploy production OpenStack infrastructure while concentrating on adding value in the service layer, tooling and customizations they need on top of the Red Hat Enterprise Linux OpenStack Platform foundation, while trusting Red Hat to maintain the integrity of both the Red Hat Enterprise Linux Server and OpenStack code.
Users can also benefit from enterprise-grade features, including:

- Testing and certification for each OpenStack release running on Red Hat Enterprise Linux OpenStack Platform for broad hardware and software compatibility and performance.
- A predictable, stable lifecycle.
- SELinux military-grade security.
- A broad ecosystem of certified partners for compute, storage, networking, ISV software, and deployment and customization services.

In addition to the flexibility afforded by CloudForms and Red Hat Enterprise Linux OpenStack, Red Hat open cloud solutions also address the increasing pressure placed on federal IT to deliver services faster and with greater agility.



We've combined Red Hat Enterprise Linux with OpenStack, the fastest-growing and massively scalable cloud infrastructure platform. Together, they form the ideal platform for building private or public clouds.

Red Hat OpenShift: Deploy Warfighter Applications Faster with Open Source Platform-As-A-Service

Up-and-coming web startups are leapfrogging each other to market using Internet-hosted PaaS technologies. PaaS allows these startups to innovate rapidly by focusing more time on their mission and less time managing hardware and software. Can the warfighter benefit from PaaS too? Yes, if the warfighter controls the PaaS stack - and open source delivers that control.

Historically, warfighter applications are often monoliths from the power plug to the running application – they were often designed for a single purpose without reuse and interoperability in mind. The design variances of these monoliths have also prevented economies of scale in terms of technology and Certification and Accreditation (C&A) reuse. This lack of reuse can prevent applications from getting to the warfighter in a timely fashion and can also lead to cost and schedule overruns. By identifying areas of commonality that could be standardized, certifying those components once for reusability, and focusing more on the remaining differences, agencies can increase efficiency and save the time involved with regularly recertifying applications.

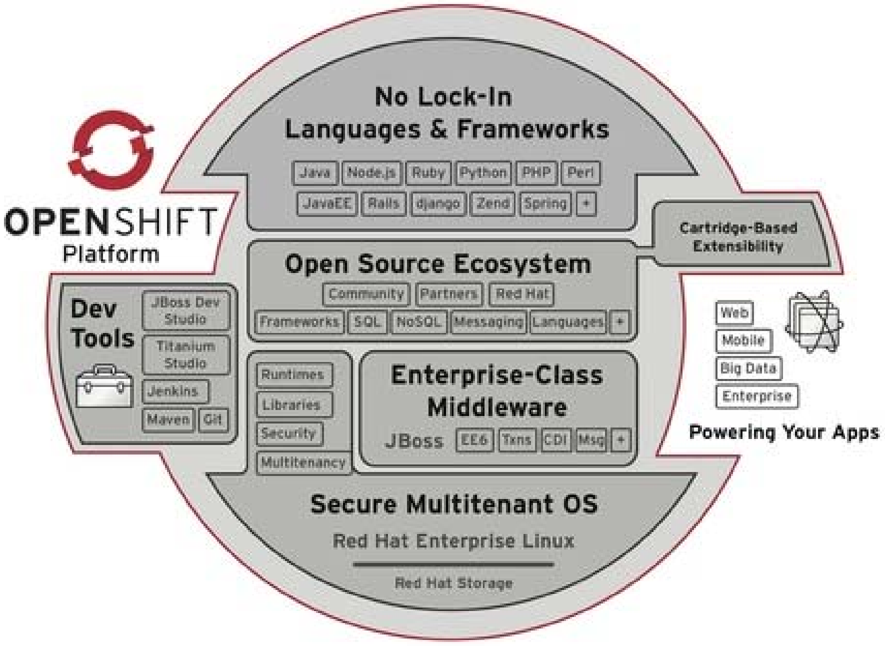
"Platform-as-a-Service (PaaS) will attain a 41% CAGR through 2016, generating 24% of total cloud revenues. 71% of PaaS revenues will be generated by vendors over $75M in sales."

According to a forecast by Market Monitor, a service of 451 Research

PaaS is one solution that can alleviate these challenges by shrinking timelines and eliminating vendor lock-in. PaaS utilizes IT stacks that are consistent across multiple applications, including everything from the power plug to hardware to virtualization to operating system to application server. The IT stack can be certified once and reused many times with a significantly smaller amount of re-certification work. As such, developers can focus more on their application and get it into production sooner since it's running on a stack of hardware and software that someone else has already rigorously certified.

One problem with PaaS, however, is that most Internet-hosted PaaS providers are proprietary. Many of these PaaS providers only support their proprietary languages and/or libraries, which only run on their back-end servers on the Internet. If a developer ever wants to move an application to another PaaS provider or move an application to on-premise servers, application porting is necessary. And in the case of embedded and/or classified systems, which may not have Internet connectivity, proprietary Internet-hosted PaaS is not an option. This is where open source PaaS can provide a solution. A PaaS stack that is open source from top to bottom can be run on a public cloud, a classified enclave, or a tactical vehicle and provide the same experience. The application written for one deployment model is also portable across all. Open source PaaS offers the deployment efficiencies of traditional PaaS with the platform deployment target choice of open source.

Red Hat OpenShift is an autoscaling, open source PaaS for applications and includes hosted, on-premise, and community offerings. It was first released in developer preview in May 2011 to address the need for vendor-agnostic PaaS using open source principles and serves as a good example of the aforementioned PaaS concepts. It runs on top of Red Hat Enterprise Linux and each user-developed application runs as a PaaS "gear" inside a Linux container. By using Linux containers and not giving each application its own virtual machine, applications can be thinly and rapidly provisioned, which is ideal for massive scale as well as for small form factor embedded tactical deployments. Even though the applications are multitenant and running on the same Linux operating system, the Linux containers are confined using Linux resource control groups called cgroups, as well as Common Criteria-certified and NSA-developed SELinux.



OpenShift components

By being built on top of open source, any application written for the PaaS can run without it, so vendor lock-in is eliminated. Further, an application can be developed on the PaaS and then deployed without it, such as in a lightweight tactical or embedded environment.

Agencies are being forced to do more with less. They need to identify areas of redundancy and consolidate efforts without compromising their missions. As proven in the private sector, PaaS provides the ability to rapidly deploy applications by focusing more on the mission and letting the PaaS provider economically provide a secure and stable platform upon which to build. For the warfighter, Internet-hosted PaaS is often a nonstarter. Applications need to run disconnected in either tactical and/or classified environments. Again, open source PaaS, such as Red Hat's OpenShift, for example, provides a way for the warfighter to take advantage of the economies of scale of PaaS with the control of open source.

Key benefits:

- ***Open source*** – OpenShift uses an open source platform and standards-based components to ensure application portability and *eliminate lock-in.*
- ***Speed*** – Reduce the time required to build and deploy your applications by letting you focus on your code and innovation rather than infrastructure provisioning and administration.
- ***Choice*** – Benefit from the widest choice of programming languages, frameworks and runtimes including Java EE6 with JBoss EAP
- ***Ease of use*** - Integrated development tools and intuitive interface enable you to get started quickly. No new programming models, no app changes, and *no cloud lock-in.*

Strategic Cloud Partners Ease Deployment of Hybrid Clouds

For customers seeking a trusted public cloud to deploy or build applications upon, Red Hat's rich partner community of Certified Cloud Providers gives our customers the advantage of using their existing datacenter-based technologies in public clouds. Staying true to our principles of choice and portability, whether you're implementing an open hybrid cloud or starting a new application entirely on a public cloud, by using a Red Hat Certified Cloud Provider, your custom-developed or third-party ISV applications certified to Red Hat Enterprise Linux are assured to function as anticipated in a trusted cloud.

Red Hat Certified Cloud Providers have to meet business, operational, and technical requirements to be able to offer Red Hat solutions under cloud-appropriate business models and are backed by Red Hat support relationships.

Of specific benefit to the DoD is Red Hat's partnership with Certified Cloud Provider – **Autonomic Resources**. Together, Red Hat and Autonomic Resources brings an open choice to our joint federal customers as we offer the ability to plan, build and manage clouds more easily and more securely. Autonomic Resources' security accreditations are significant:

Autonomic Resources has been issued a Provisional Authority to Operate (ATO) from the DISA ECSB (Enterprise Cloud Service Broker[2]) for its ARC-P (Government Community and Hosted Private Stacks) IaaS solutions at DoD Impact Levels 1 & 2.

The ARC-P IaaS offering was assessed using the DISA-developed DoD cloud security model, which was performed for an additional twenty-three controls and control enhancements from NIST SP 800-53 revision 3, above and beyond the FedRAMP Moderate baseline. A review of the standing ARC-P FedRAMP security authorization package was also performed. ARC-P is a FISMA Moderate system and is

[2] Created by the DoD CIO, Theresa Takai, ECSB is the central cloud brokerage for all of DoD and is accountable for evaluating and assessing federal cloud service providers post-FedRAMP authorization.

now authorized at DoD Impact Levels 1 & 2 for Unclassified Public Information and Unclassified Private Information.

This Provisional Authorization is an initial approval of the Cloud Service Provider (CSP) authorization package by the DISA Designated Accrediting Authority (DAA), which a DoD DAA can leverage to grant an Authority to Operate (ATO) for a specific DoD customer or mission owner.

Autonomic Resources' hosted private IaaS solution, **ARC-P** *Private*, is a *RHEV stack implementation*. **ARC-P** *Government Community* is planned to transition to RHEV next year, but is *currently a KV- based* solution utilizing RHEL for most of the underlying systems.

The DoD approval is timely for Autonomic Resources and the ARC-P platform, considering the launch of ARCWRX, the ARC-P implementation of OpenShift by Red Hat, now open for evaluation. ARCWRX is Autonomic's new PaaS offering and is an excellent match for rapid development and test environments. No IT staff intervention is required to provision or de-provision DevOp environments. Additionally, ARC-P is ready for authorization at Impact Levels 3 & 4 once finalized by DISA, and Level 5 by early 2014.
As you can see, Red Hat provides everything the Army needs to evolve its IT infrastructure and applications into the future. From individual technology components to complete solutions and services, we have led the industry into the world of the cloud. And with the richest ecosystem anywhere, from a range of Certified Public Cloud Providers, hardware vendors, ISVs, and PaaS middleware vendors, Red Hat is the cloud platform that delivers you the widest range of choices.

Unlike other approaches, we deliver choice to our customers…Choice of platform, choice of virtualization, choice of cloud provider.

Cloud Computing – The Red Hat Advantage

But how do Red Hat's cloud solutions compare to existing proprietary options? For cash- and resource-strapped agencies, surely it would be more opportune to purchase a "cloud-in-a-box". This monolithic piece of hardware holds your entire infrastructure inside: networking, compute, storage, operating systems, databases, and so on. They are expensive up front, but the gamble is that by removing or reducing the cost of tying all these pieces together yourself, it's less expensive in the long-run.

In fact, this couldn't be further from the truth. Cloud computing is about elasticity and flexibility. It's about moving away from encumbering capital investments and towards operating expenses, which are more agile. A big black box with all your hardware and software in it is the opposite of that. A single vendor in control of your entire virtualization layer is the opposite of that. Government agencies can get much more out of their infrastructure and staff by deploying an open cloud strategy that encourages standardization across their physical, virtual, and cloud-deployed systems, rather than consolidating their spend with a single vendor.

By bringing open choice and standardization to the cloud — both for deployment and development — Red Hat delivers some distinct cloud advantages:

- **An open, standardized, and agile operating system** –With Red Hat Enterprise Linux, APIs are open source and based on open standards that run across a broad swath of computer architectures. This brings in a large community of developers and users and eliminates the possibility of being locked into any single vendor's API.

- **The ideal platform for building Linux or Windows-based clouds** – Red Hat Enterprise Virtualization is a comprehensive datacenter virtualization product for Linux and Windows workloads that allow users to build an agile, secure virtualization foundation with the features needed for traditional enterprise application workloads, and is the ideal platform on which to build an internal or private cloud.

- **Industry-leading government cloud security standards** – Red Hat is committed to providing secure and stable software that can be easily used in security-sensitive cloud environments. Red Hat Enterprise Linux, for example, holds the Common Criteria Certification at Evaluation Assurance Level (EAL) 4+ – the highest level of assurance for an unmodified commercial operating system. In addition, Red Hat partner, Autonomic Resources, is the first cloud provider to achieve compliance under the Federal Risk and Authorization Management Program (FedRAMP) and was issued a provisional authorization by the DoD in November, 2013 for its IaaS offering, making it the only cloud provider offered for DoD-wide acceptance under the Defense Information Systems Agency (DISA) Enterprise Cloud Service Broker catalog.

- **Portability and an "exit-strategy" option** – Red Hat CloudForms (a comprehensive private and cloud management platform) integrate with existing products and technologies, including physical servers and virtualization platforms from other vendors. This provides the easiest on-ramp to an on-premise cloud. It also allows you migrate to multiple public or community cloud providers (in accordance with the "exit strategy" requirements of the Federal Shared Services Implementation Guide), including those running software stacks from a different vendor. In addition, CloudForms also allows you to manage the lifecycle of your applications across disparate virtual machines (Red Hat, VMware, and Microsoft) and cloud providers.

- **A consistent development and deployment platform for use across multiple clouds** - With OpenShift (Red Hat's hosted public PaaS that offers an application development, build, deployment, and hosting solution in the cloud), developers can take full advantage of clouds while continuing to use their preferred development tools and approaches. There is no need to adopt new development tools or be locked into the offerings of a single cloud provider. Users can use OpenShift to set up their own internal PaaS service or leverage the powerful capabilities of JBoss Enterprise Middleware on public clouds such as Amazon EC2.

- **Enterprise grade management for multiple environments** – Red Hat CloudForms offers you a unified management framework with advanced life cycle management capabilities across infrastructure platforms, such as OpenStack, VMware, Red Hat, and Amazon.

Open Source - A Future Based on the Power of Community

We've touched on the cost savings and reduced TCO that open source software can enable, but the development process is much more than a means of lowering acquisition costs. It is also the means by which agencies can become more innovative, more agile and more cost-effective by building on the collaborative efforts of open source communities.

It seems counterintuitive, but what used to be thought of as open source's greatest weakness – the community – is now viewed as its greatest strength. The quality of open source software is the result of contributions from the entire IT industry, including core open source developers, the government, commercial entities, chip manufacturers, and IHV and ISV partners. With almost every leading IT vendor funding open source development groups, the aggregate horsepower has become very formidable and promises stability for the continued growth of the open source model. As the community continues to expand, a halo effect encourages even more vendors to join and contribute. This is a positive for government agencies since it mitigates risk and offers choice. In addition, open source vendors have strong approaches to quality assurance — thanks to the breadth of testers that they have access to thanks to the power of the community.

As the government has become more comfortable with open source in general, and Red Hat specifically, agencies have increasingly begun to think about open source in a more strategic way; they want to contribute code back to the communities that were helping them, and Red Hat Enterprise Linux is a catalyst.

The U.S. Navy, for example, had a need for a deterministic computing platform for its shipboard command-and-control systems. Weary of paying for expensive "real-time" operating systems, the Navy and a coalition of vendors worked to develop patches to the open source Linux operating systems. For the Navy, these improvements meant that the hardware, operations, and maintenance would be identical for a real-time workload and a regular workload. It also meant they now shared the ongoing maintenance burden with the broader Linux community.

Some in that broader community are companies that trade securities and commodities - and this is where we see the power of those communities come together. These companies have a similar need for real-time systems but they shared the Navy's problem: reliance on expensive, proprietary software that locked them to a single vendor and required new training for their systems administrators. However, they were able to take the same software the Navy had developed and apply it to their trading systems. Now they spend less on hardware and training, and have a broad portfolio of IT systems that they can use. These same Wall Street developers then make improvements to the real-time software that the Navy can then use. This kind of unwitting collaboration would be untenable outside of the open source development process.

Now, it's worth noting that this collaboration occurred without making drastic changes to policy or the Defense Acquisition Regulations. Nor did it require a Cooperative Research and Development Agreement. The Navy awarded task orders to companies, and those companies worked with the open source software community. The opportunity and economies of scale for the Army is self-evident – the open source community can be efficiently leveraged to provide capabilities faster and with a more viable long-term maintenance strategy than a vendor of proprietary software and traditional procurement cycles could offer.

The adoption of Red Hat Enterprise Linux and open source in government is an evolution: the first furtive steps in the early 2000s, and leaders like the Army and the Census Bureau taking us to the close of the first decade of Red Hat Enterprise Linux where the government appears to be comfortable not just using open source, but creating its own open source communities (Mil-OSS.org and Forge.mil are two examples of DoD OSS communities).

Creating a community around software is, in fact, what makes open source work so well. An open source license will allow a community of developers to collect around a shared set of problems, and work together on the solution. In contrast to national or symbolic efforts to improve collaboration in a particular community, open source is effective because it is organized around useful work.

The **National Security Agency (NSA)**, for example, has used open source to reduce the cost of its high-security systems to drive better security. Similarly, the **Consumer Financial Protection Bureau**—a relatively new agency—has even gone as far as being 'open source by default', by releasing everything it does to the community. Why? Because they feel that citizens should benefit from the software they helped pay for while allowing them to participate in improving the software that they're using.

DoD Mandates Support Red Hat OSS

But not all communities are created equal, and DoD and Army policy has evolved to recognize this important distinction. In 2009, both DoD and the Army took specific steps to clarify misconceptions and misinterpretations of existing government laws, policies and regulations that pertain to OSS and that previously hampered effective use and development of OSS in defense agencies.

For example, with **AR25-2,** the Army permitted the use of "productized" open source software, citing Red Hat, as a specific example, while outlawing use of "shareware" or "freeware". The latter are both also driven by the open source community, but lack the support and government security accreditations offered by Red Hat.

In the same year, **DoD issued a memo** "Clarifying Guidance Regarding Open Source Software (OSS)" citing several distinct information assurance advantages offered by the open source community and supported-OSS solutions, such as those offered by Red Hat:

> *"2. b. (I), (i): 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."*

And:

> *"2. d: The use of any software without appropriate maintenance and support presents an information assurance risk. Before approving the use of software (including OSS), system/program managers, and ultimately Designated Approving Authorities (DAAs), must ensure that the plan for software support (e.g., commercial or Government program office support) is adequate for mission need.*

This leads us to our next point:

Through Community Comes Security

One of the most misunderstood aspects of the open source software development model is the security benefits it offers – and once again, community is a catalyst for security. OSS security relies on genuinely hardened code that is tested by a large number of reviewers in a wide variety of circumstances.

"…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."

DoD 2009 Memo: "Clarifying Guidance Regarding Open Source Software (OSS)"

Hiding code, as proprietary software vendors so, does not prevent attacks. Open Source development practices rely on actually hardening (or improving the security of) code by making it available for peers to test and try to break, and then fixing the problems found.

OSS is not always more secure - however in both theory and practice the OSS security model has proven that it can more quickly respond to and correct security issues. According to

Mil-OSS.org, on average the FireFox project team fixed security issues 37 days after they were found; while Microsoft took an average of 134.5 days to patch security issues they found in their Windows line of products.

Assuming that the goal is to make secure software, it is obvious that the easiest way to find flaws in a project is to make all of the project's code completely transparent. This approach may seem counter-intuitive, if the ultimate goal is anything other than the integrity of the technology.

By openly releasing a project's code and making it readily available via the Internet the community of peer reviewers is expanded exponentially across the globe. The community will quickly find flaws and the project team can take action to fix them. This simultaneously garners exceptionally wide and deep testing feedback from developers who need the code to be as secure as possible for their own use as well as the community's. Both the project owners and community benefit from sharing flaws and fixes.

Contrast this with the ongoing threat faced by the proprietary software industry. As virtualization and cloud computing become the new top-level operating system, as it were, within the datacenter, the hypervisor layer is becoming a more attractive target for breaches and attacks. Would-be hackers going after a virtualized datacenter will look for vulnerabilities within the hypervisor, the virtual machines, or the virtual networks in hopes of being able to find an exploit that can help them get their hands on the keys to the entire kingdom. This leaves some proprietary software companies open to vulnerability.

The 2009 DoD memo expresses confidence in the OSS security model: "*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*."

According to InfoWorld[3]: "*Even though the hypervisor is becoming more of a commodity play with increased competition coming from Microsoft, Citrix, Red Hat, and Oracle, it seems as though VMware has seen a spike in the number of threats made against its virtualization products*." **In 2012**, **three separate incidents of VMware's** confidential source code from the ESX hypervisor were leaked and posted online by hackers and other vulnerabilities were exploited in its desktop virtualization software.

InfoWorld's advice is unnerving: " *In the end, no matter what security update method VMware chooses to go with, one thing is clear: With VMware product threats potentially on the rise, if VMware releases a patch or update that is marked as "critical," don't blink. VMware customers shouldn't take any chances with their virtualized infrastructures*."

Because the OSS security model is established on industry-accepted best practices and the actual code is widely available, projects are widely reviewed, thoroughly scrutinized, practically improved and quickly hardened.

A good example is RDO. This is a community binary distribution of OpenStack with the objective of nurturing and fostering the OpenStack community, development, and testing for enterprise use cases. Analogous to Fedora Linux and its relationship to Red Hat Enterprise Linux, RDO provides the latest

[3] VMware Pledges to Improve Security, Considers Scheduling Patch Updates, InfoWorld, March 2013

cutting-edge code to the community. RDO is also able to instantly generate packages based on the latest repository source code to assist testing and development of upstream code.

Another example is Facebook. As with its data center and server creations, Facebook intends to “open source” its storage designs, sharing them with anyone who wants them. The effort is part of the company’ s Open Compute Project , which seeks to further reduce the cost and power consumption of data center hardware by facilitating collaboration across the industry. As more companies contribute to the project, the thinking goes, the designs will improve, and as more outfits actually use the designs for servers and other gear

Furthermore, the U.S. Department of Homeland Security is **investing in a new five-year, $10 million program** to survey existing open-source software to find those that could fill "open security" needs. Called the *Homeland Open Security Technology program*, or HOST, it also may plant seed investments where needed to inspire innovative solutions that can fill gaps in *cyber security defenses*. With OSS, the U.S. government is not at the mercy of companies that hold the license for proprietary cyber security software. If bugs crop up or an exploiter penetrates the cyber security defenses, programmers can dive right into open-source software to fix it.

This begs the question and gives us an excellent opportunity to open a discussion Red Hat would like to have with the Army – why would you want to base the Army’s entire foundation for virtualization on proprietary code, when more secure, more scalable, and more affordable open source alternatives are available?

Conclusion

Red Hat makes the rapid innovation of open source technology consumable in mission-critical, enterprise environments and we are steadfast in our commitment to build upon our 10 year partnership and help change the way the U.S. Army conducts business as it moves to embrace cloud technologies.

How?

By adopting Red Hat’s supported low-cost OSS solutions at the enterprise program level, the Army can rapidly explore external technical advances, induct the best-in-class solutions, and then re-use all or parts of them to create unique new capabilities, without degrading the functionality, productivity, or mission effectiveness of current and future systems.

In addition, the Army can evolve processes, policies, and procedures in order to keep pace with emerging technologies, including advanced internet-based applications, cloud computing and storage alternatives, databases, virtualization, infrastructure outsourcing, distributed collaboration and development, an increasingly rich menu of social networking technologies, and other innovations that the Army currently can’t exploit or absorb into the current IT environment without reallocating resources from other areas. As Gunnar Hellekson, Chief Strategist with Red Hat’s Public Sector team explains[4]: “*More than any other trend, open source is putting control back in the hands of government agencies, rather than the vendors who are providing them with technology solutions*.”

[4] Modern Government Magazine, Jan-Feb 2013

But Red Hat is more than a software company. We're the bridge between the communities that create open source software and the enterprise customers who use it.

Red Hat competes with large companies like Oracle, VMware, and Microsoft, all of whom are likely in the Army's Top 5 when calculating existing technology spend. By facilitating the adoption of OSS with a provider like Red Hat, the Army will achieve the following:

- Choice and competition in technology areas that have historically been monopolized by a single vendor.
- A stronger negotiating position with large IT vendors by delivering a viable alternative to their product stacks.
- Speed the deployment of new technologies to the warfighter. By using flexible, pre-built foundations, it is quicker and easier to build from them rather than starting from scratch.
- Enterprise capabilities for applications that do not require high cost functionality from other vendors.
- Derive more value from the Pentagon’s contracting budget in alignment with the DoD’s Better Buying Power initiative.
- The ability to harvest emerging technologies from open source development communities, rather than remain shackled to a network of commercial vendors whose priorities and plans aren’t driven by your mission needs.
- Expedite information assurance concerns by sharing flaws and fixes across DoD open source communities such as Mil-OSS.org, Forge.mil and opensourceforamerica.org.
- Provide for the re-use and re-deployment of solutions to common problems – driving innovation and economies of scale.
- A stronger “Defense in Depth” posture with a multi-vendor strategy.
- Ability for end users to determine the best technology for their requirement(s).

For additional guidance on open source software in the DoD, visit the DoD Open Source FAQ.

Open Source Implementations - What are the Keys to Success?

The number one key to success is a well-defined open source strategy. The most successful enterprises have written clear policies and strategies around how they will use open source software – what applications and how support will be delivered.

The second key is to invest in the complementary services around open source software that will make it truly usable. In the past, organizations struggled to implement open source software without having the right kind of help, the right kind of training, and the right kind of support to mitigate risk.

Now, however, the most successful agencies make sure that open source projects are treated right – like any other important project. Federal agencies are investing in training and support services because they believe the product is important.

In conclusion, Red Hat’s core message to the DoD and the U.S. Army remains the same as it has been for the last 10 years. Where possible, avoid proprietary, monolithic server and software architecture in favor of open source technology, standardized, COTS, government-certified and approved IT platforms.

But don't just take our word for it, government leaders across the globe are embracing open source technology to generate efficiencies, meet mission-critical IT demands, and improve service delivery – while putting control back in the hands of the public sector, not the vendors who provide the solutions:

"*We believe in using and contributing back to open source software as a way of making it easier for the government to share data, improve tools and services, and return value to taxpayers*." **The White House**.

"The best scientists and engineers in the world certainly do deserve the best IT they can possibly have - in a balanced and economical way. Open source gives us the ability to give them that world class capability..." **Linda Cureton, NASA CIO.**

"*Open Source gives the UK government and other governments the opportunity to reduce the dependence they've had in the past on a relatively small number of very big IT and software companies...and gives them more flexibility. It acts as a platform for innovation*."
Brian Glick, Editor-in-Chief, Computer Weekly.

"*With the proliferation of issues and the scarcity of resources to address them all, leaders inside and outside the government are turning to the principles of participation, collaboration, transparency, and efficiency to address the challenges facing our country and the world*." **Tim O'Reilly**.

"AWS Test Drive is an exciting program to help drive sales and open new business opportunities with AWS. With the AWS Test Drive labs, customers can register and experience an evaluation of enterprise software solutions using the self-paced hands-on lab platform in a matter of minutes, as opposed to days or weeks. Once a customer completes the AWS Test Drive, they can quickly move to production by working with sponsoring partners. We are excited for Red Hat to launch these new test drive labs and to expand this opportunity to many more Red Hat partners"
Terry Wise, Director, Worldwide Partner Ecosystem, AWS

"*When we rolled into Baghdad, we did it using open source. It may come as a surprise to many of you, but the U.S. Army is the single largest install base for Red Hat Enterprise Linux*."
Brigadier General Nick Justice, PEO C3T, Linux.com, 2007

A decade ago, it was open source against the world. Now, open technology and Linux® are the foundation of the datacenter. Together, we are building the next cloud — just like we built the next operating system. It is open. It is hybrid. And it's all yours. **redhat.com/cloud**

Think Red Hat is just Linux? Think again.

IaaS | PaaS | Cloud management