MEETING DO-278 WITH RED HAT ENTERPRISE LINUX 5

MAÃ SHEPSU MENÅB NUÍRÍÃNKH, RED HAT SOLUTIONS ARCHITECT, RHCE®

1. INTRODUCTION

As part of services engagement proposals now pending with FAA ASRC-MS, this document discusses relevant issues and outlines how we would go about supporting the DO-278 approval process.

1.1 PURPOSE

This purpose of this document is to highlight the features, functions and capabilities of the Red Hat® Enterprise Linux® (RHEL) version 5 operating system (OS) that support the CNS/ATM (Communication, Navigation, Surveillance, and Air Traffic Management) system objectives of DO-278 for approval at assurance level 3 (AL3).

1.2 BASIC ASSUMPTIONS AND FRAME OF REFERENCE

In some ways, it is difficult to compare the features and functions of a software system to the requirements of DO-278 in isolation from the environment in which the software will be used. This is because DO-278 approval is an administrative process whereby authority is granted to use a software system within its operational environment including all of its non-IT (information technology) parts at the FAA. One way to surmount this difficulty is to take a page from the Common Criteria (2) world and separate the evaluation for DO-278 into two parts, a Target of Evaluation (TOE) and the Operational Environment (OE). The TOE in this case would be the RHEL 5 OS. The OE would be the specific application and IT environment within the FAA. For example, in order to apply for DO-278 approval, FAA must first complete a safety assessment (1) to determine the proper Assurance Level (AL) needed for approval.

We would of course welcome an opportunity to assist ASRC-MS and/or other groups within FAA in achieving DO-278 approval. The remainder of this document discusses ideas, and information that would be relevant to that process.

The safety assessment, and the system aspects relating to CNS/ATM software development, objectives for CNS/ATM systems along with the COTS, Commercial Off-The-Shelf (COTS) Software, sections of DO-278 lay out the foundations and requirements for approval. The idea of software integrity assurance hinges on providing sufficient evidence in the TOE and OE that the requirements for a given AL (AL3 in this case) specified by the safety assessment are met.

Two key principles of quality are "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) (10). Therefore a software system that performs the intended functions correctly with acceptable performance levels and zero or near zero defects would be judged as high quality by its users. The better a software system or component does in terms of fit for purpose and minimizing defects, the greater the level of confidence or "assurance" for the end user.

The definition of integrity applied to software revolves around the idea that software is unaltered from its intended form and function and it's ability to perform in a consistent, reliable, stable manner in a given environment. Software integrity also includes the idea that software is unaltered during delivery, and its source is known or identifiable.

1.3 DO-278 APPROVAL PROCESS

The DO-278 approval process provides for two avenues to achieve standardized evaluation criteria. DO-278 Section 3: OBJECTIVES FOR CNS/ATM SYSTEMS defines the criteria for software originally designed and developed with DO-278 compliance in mind. The other avenue available is described in DO-278 Section 4.1: Commercial Off-The-Shelf (COTS) Software. The COTS approval route is appropriate for a general purpose OS such as RHEL 5. The COTS approval approach (see Paragraph 4 below) allows for an after the fact or "as-built" examination of a software system and/or its components. Open source software (OSS) such as Red Hat Enterprise Linux is uniquely suited for this approach to DO-278 approval because the source code for the entire system is readily available and/or provided when obtaining the binary executables.

1.4 CERTIFICATIONS AND ACCREDITATIONS

Red Hat Enterprise Linux is the most certified operating system available today. RHEL has passed the Common Criteria process 12 times on four different hardware platforms. RHEL 5 has even received Common Criteria certification at Evaluation Assurance Level 4 (EAL 4+) under the Controlled Access Protection Profile (CAPP), Label Security Protection Profile (LSPP), and the Role-Based Access Control Protection Profile (RBACPP). These certifications were at a level previously unheard of from a mainstream operating system.

In June 2009, JBoss® Enterprise Application Platform 4.3 achieved Common Criteria certification at EAL 2+ (augmented for flaw remediation). This marks the first Common Criteria certification for JBoss Enterprise Middleware, giving Government agencies and other security-conscious organizations a new choice for enterprise Java applications. Customers can now deploy JBoss Enterprise Application Platform 4.3 with the added confidence that it meets the security standards set forth through Common Criteria.

In early October 2009, Red Hat's Data Services Platform, specifically MetaMatrix 5.5.3, achieved Common Criteria certification at Evaluation Assurance Level (EAL) 2.

Red Hat Enterprise Linux is on the DISA Approved Products Lists for IPv6. The Department of Defense has mandated that IT systems move toward IPv6 while maintaining IPv4 (the currently more common network). Only four operating systems, including RHEL have gone through the certification process (http://jitc.fhu.disa.mil/apl/ipv6.html).

RHEL was recently awarded the COE certification by the US Defense Information Systems Agency (DISA). RHEL is now approved for Department of Defense deployment. This certification further validates Red Hat Enterprise Linux as a mission-critical enterprise platform. COE (Common Operating Environment) certification assures that Red Hat Enterprise Linux meets DISA's stringent requirements for interoperability, performance, and standards compliance **(http://www.redhat.com/solutions/government/coe/)**.

Red Hat Enterprise Linux provides out-of-the-box compliance with the NISPOM Chapter 8 audit requirements. A sample implementation can be found in /usr/doc/audit-1.5.2/nispom.rules in RHEL 5.

RHEL has been used in systems from DCID-6 (DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/3) Protection Level 3 (PL3) up to PL5.

Additional information and the list of certifications for RHEL can be found at: **<http://www.redhat.com/solutions/government/certifications/#tab3>**.

2. THE OPEN SOURCE SOFTWARE DEVELOPMENT MODEL

The open source software development model consists of a world wide "ecosystem" of independent developers collaborating, competing and providing peer review for software projects. The OSS development model is inherently transparent (source code readily available for review and modification), standards based, and typically relies upon the Internet as the means of collaboration and communication. The peer review and end-user feedback (most code is free to download and try out) underpins the process of innovation, continuous improvement and refinement that has come to characterize OSS. Because open source gained hold with the rise of a public, worldwide, computer-network system called the Internet, and the attendant need for massive retooling of the computing source code, the code was often written to generally accepted software, communication, and technology standards in order to provide for interoperability (11).

RHEL is based upon the Linux kernel developed over the Internet as OSS, and many other software programs and components, such as Apache, OpenOffice, Samba, and SELinux. Fedora is a free, community supported Linux distribution sponsored by Red Hat (13), which provides the so-called "upstream" for what eventually become RHEL releases (12).

upstream – (noun) - In free and open source projects, the upstream of a program or set of programs is the project that develops those programs. Fedora is downstream of those projects. This term comes from the idea that water and the goods it carries float downstream and benefit those who are there to receive it (12).

As the upstream for RHEL releases, Fedora provides what could be the largest "beta software" test environment in the world. Consider that there are literally millions of unique users of Fedora (14) as shown in Table 1 below. Also, RHEL 5 is based on Fedora 7 which was released May 31, 2007, and which has been in continuous use by almost 4 million users since it was released. This constitutes a large amount of product service experience to be applied to the requirements of the DO-278 COTS approval process. Although, Fedora is community supported, users are still free to use the Red Hat Bugzilla (see Paragraph 3 below) bug reporting tool for problem reports and requests for enhancement or RFEs. Finally, only a limited subset of Fedora software packages actually make it into a RHEL release. Fedora has about 15,000 unique binary software packages in the repository, and only about 2500 binary packages are selected for inclusion in a RHEL release. These are the ones enterprise customers demand and which are supported by Red Hat (15).

FEDORA 12 (CONSTANTINE UNIFIED STARTING ON 2009-11-17)

Yum Data: Current release connections (connections to yum)

WEEK	DATES	NEW UNIQUE IPS	TOTAL UNIQUE IPS	TOTAL COMPARED TO LEONIDAS
Week 1	2009-11-17 – 2009-11-23	91,620	91,620	87%
Week 2	2009-11-24 – 2009-11-30	88,238	179,858	92%
Week 3	2009-12-01 – 2009-12-07	88,194	268,052	97%
Week 4	2009-12-08 – 2009-12-14	89,622	357,674	97%
Week 5	2009-12-15 – 2009-12-21	90,215	447,889	99%
Week 6	2009-12-22 – 2009-12-28	89,697	537,586	98%
Week 7	2009-12-29 – 2010-01-04	90,096	627,682	97%
Week 8	2010-01-05 – 2010-01-11	98,631	726,313	97%
Week 9	2010-01-12 – 2010-01-18	101,423	827,736	97%
Week 10	2010-01-19 – 2010-01-25	94,734	922,470	96%
Week 11	2010-01-26 – 2010-02-01	108,173	1,030,643	96%
Week 12	2010-02-02 – 2010-02-08	113,659	1,144,302	97%
Week 13	2010-02-09 – 2010-02-15	113,893	1,258,195	97%
Week 14	2010-02-16 – 2010-02-22	117,088	1,375,283	97%

Total repository connections (as of 2010-02-23)

METHOD	FEDORA 7	FEDORA 8	FEDORA 9	FEDORA 10	FEDORA 11	FEDORA 12	RAWHIDE	TOTAL
Mixed	3,974,281	5,957,677	3,351,302	3,860,133	3,349,836	1,375,283	965,616	22,834,128
New	3,995,628	6,039,010	3,506,940	3,860,133	3,349,836	1,375,283	965,616	23,092,446

Total unique IPs: 19,637,402

Initially there were two significant barriers to adoption of OSS for use in mission-critical applications among enterprise class customers, such as Government, banking, aviation, technology industries, and large retail establishments. The two big concerns were around software quality and integrity and paid support attached to service level agreements (SLAs). These questions have been repeatedly addressed through numerous studies and examination of actual source code from open source projects attesting to the high quality of OSS. For, example an OSS quality study by Coverity done for the Department of Homeland Security showed an average defect density of less than 0.0010 for the 32 OSS packages examined. The average defect density for the 32 open source packages analyzed was 0.434 defects per thousand lines of code with a standard deviation of 0.243 (8, pg. 4).

Red Hat has played a pivotal role in OSS by working to enhance the quality of OSS projects, and providing the crucial paid support with attached SLA and the many other products and services which go into making RHEL consumable within the mission-critical portions of the enterprise.

3. RED HAT'S INTERNAL PROCESSES

Red Hat uses a company-wide approach emphasizing engineering, customer support, professional consulting services, and people programs, among others, to foster a corporate culture that nurtures an awareness of how quality and integrity affect our results and empowering employees to "stop the assembly line" if needed.

3.1 ENGINEERING

Red Hat is in a unique position in that we benefit from the best of both worlds as an OSS company. We have the support and trust of the open source community with its ability to rapidly innovate using standards based tools, and the aforementioned peer review process.

At the same time, internally, we are able to apply a disciplined engineering process in order to provide the stability and support required for mission-critical enterprise operations. This includes version/release configuration management, testing and regression testing including quality control measures, bug and RFE tracking using Bugzilla **(https://bugzilla.redhat.com/index.cgi)** and Issue Tracker both internally and externally.

Our RHN (Red Hat Network) and Satellite solutions are best of breed in the industry delivering on-going support, bugfixes, updates, security patches, monitoring, automated installation, provisioning, re-provisioning, system configuration management and customization as part of centralized system life-cycle management. To enhance the integrity of our software distribution system, each RPM or software package is cryptographically signed using Red Hat's private key to allow easy identification of the source of the package, and to prove the package has not been altered. One interesting feature of RHEL, is that the change log for each RPM on the system can be printed out easily with one simple command. Red Hat supplies documentation in the form of release notes, installation, user, and administrative guides as well as system documentation such as man pages and example configuration file templates. We also furnish, deployment instructions to give our customers the information, tools, and confidence to apply our solutions in the field. In addition, we have a software certification test suite and a hardware certification test suite to allow independent software vendors (ISV) and independent hardware vendors (IHV) to self-certify. Those that pass are listed in a public-facing web site **(https://hardware.redhat.com/)** which includes search tools.

3.2 GSS (CUSTOMER SUPPORT)

Global Support Services (GSS) is responsible for customer technical support. Three support level agreements (SLAs) are available through GSS at the L1 support level. We have basic, standard, and premium SLAs which are chosen by a customer at the time of subscription purchase. Basic support provides web only support (where customers submit tickets through Issue Tracker) with unlimited incidents during normal business hours for no additional cost. Standard support provides web and telephone support with unlimited incidents during normal business hours. Premium support gives a customer web and phone support during normal business hours with unlimited incidents and 24x7 support for Severity 1 issues.

More information on the support SLAs is available here: **<http://www.redhat.com/support/policy/sla/production>**.

Because the OSS used in RHEL is free of charge, and because of our subscription based business model, success with GSS and our other services offerings is crucial. In this regard, Red Hat has been ranked the #1 software vendor in the CIO Insight Vendor Value Study for the fifth time in six years (17)(18). GSS also provides the Technical Account Management service or TAM. The TAM is intended for customers who desire the highest level of support from Red Hat. The TAM is the primary technical contact at Red Hat working

with a customer to understand ongoing technology requirements and provide advice about critical bugs and fixes. The TAM acts as a single point of accountability for mission critical issues affecting production systems. GSS creates and maintains the Red Hat Knowledgebase articles and makes them available for public perusal. All GSS support engineers are highly qualified and experienced and have at least an RHCE (Red Hat Certified Engineer, see Paragraph 3.3 below) in order to work in GSS.

3.3 GLS TRAINING AND CERTIFICATION PROGRAMS AND RED HAT UNIVERSITY

Red Hat GLS (Global Learning Systems) is responsible creating and delivering training and certification programs to Red Hat customers and the general public. GLS set the standard in the industry more than 10 years ago by establishing performance based exams and the Red Hat Certified Engineer credential which is one of the most highly regarded and sought after certifications available. The RHCE was recently named the hottest certification in all of IT by CertCities.com (20).

Red Hat was ranked as the leader for IT education in a recent IDC MarketScape study of the industry (19). Red Hat engineers attend the same GLS courses as everyone else, and GPS, GSS, as well as Solutions Architects are required to attain and maintain at least the RHCE certification.

Here is a list of the certifications offered by Red Hat:

- Red Hat Certified Virtualization Administrator (RHCVA)
- Red Hat Certified Technician (RHCT)
- Red Hat Certified Engineer (RHCE)
- Red Hat Certificates of Expertise
- Red Hat Certified Datacenter Specialist (RHCDS)
- Red Hat Certified Security Specialist (RHCSS)
- Red Hat Certified Architect (RHCA)
- JBoss Certified Applications Administrator (JBCAA)

In addition to the GLS training, Red Hat University (RHU) provides a wide range of courses internally for Red Hat employees. The RHU courses and other training available to Red Hat personnel help insure our people are highly competent, having the knowledge, skills, and resources to be effective and efficient in their jobs.

3.4 GPS (CONSULTANTS)

Red Hat Global Professional Services (GPS) provides consulting services and dedicated on-site resources for end-to-end solutions, assessments, architectural designs, and implementations. GPS consultants offer deep subject matter expertise combined with years of industry experience. This is crucial when considering that expert, correct installations and implementations that fit the desired purpose and function in a given situation will be instrumental in providing the system quality needed to achieve DO-278 approval. Along these same lines, Red Hat maintains a database of reference architecture implementations to promote and document industry best practices and standard operating environments.

4. SUMMARY: COTS OBJECTIVES: COMMERCIAL OFF-THE-SHELF (COTS) SOFTWARE

"The use of COTS may mean that alternate methods are used to gain assurance that the appropriate objectives are satisfied. These methods include, but are not limited to, product service experience, prior assurance, process recognition, reverse engineering, restriction of functionality, formal methods, and audits and inspections. Software conformity review may need to be tailored with respect to the approach used for COTS approval. Assurance data may also be combined from more than one method to satisfy the objectives in Section 3." (1, pg. 27)

4.1 PRODUCT SERVICE EXPERIENCE

Product service experience is one of the factors that can be considered by the DO-278 approving authority to gain assurance that COTS, such as an OS, satisfies CNS/ATM objectives. Fedora, the Linux distribution upon which RHEL is based, has been in use by millions of users over a period of years. As part of the its modernization program implemented during 2004 and 2005, the FAA began running the highly complex Traffic Flow Management (TFM) infrastructure and its real-time Enhanced Traffic Management System (ETMS) on RHEL.

4.2 PRIOR ASSURANCE

Since the latest version of DO-278 available is dated March 2002, it seems likely that RHEL has already been approved as satisfying CNS/ATM objectives based upon its use in the FAA's TFM and ETMS systems. Also as shown in Paragraph 1.4 above, RHEL is the most certified OS available today. Many of these certifications such as the Common Criteria, DCID-6/3 PL3 and PL5 and the DISA Common Operating Environment are based on requirements and objectives which are compatible with DO-278. In addition, these accreditations and certifications are the result of examinations and reviews conducted and administered by highly regarded international and Government organizations.

4.3 PROCESS RECOGNITION

The development and long term support and maintenance processes that are applied to RHEL are discussed above in Paragraphs 2 and 3.

4.4 REVERSE ENGINEERING

Reverse engineering of the RHEL OS is not necessary since the source code itself and other sources of documentation are available for review and study.

4.5 RESTRICTION OF FUNCTIONALITY

If restriction of functionality is required by the DO-278 approving authority, RHEL already includes sufficient features and controls to allow the end user of the OS to pick and choose which packages to install, and which services to activate, and filter. RHEL also provides several layers and means of access control to restrict and limit services.

4.6 FORMAL METHODS

Formal methods such as code reviews, and analysis can be used to gain assurance since the source code is readily available for review (which is encouraged by open source philosophy). Something like the Coverity static analysis tool can be used as well. Coverity has even published a report covering this topic: Coverity-Meeting-DO-178B-Requirements.pdf **<http://www.coverity.com/library/pdf/Coverity-Meeting-DO-178B-Requirements.pdf>**.

4.7 AUDITS AND INSPECTIONS

These are already being conducted by DoD and others for the Common Criteria and other certifications held by RHEL. The DO-278 approving authority would be able to perform similar types of audits and inspections in order to gain assurance that approval of the RHEL OS at least at the DO-278 AL3 is warranted.

REFERENCES

1. RTCA/DO-278, GUIDELINES FOR COMMUNICATION, NAVIGATION, SURVEILLANCE, AND AIR TRAFFIC MANAGEMENT (CNS/ATM) SYSTEMS SOFTWARE INTEGRITY ASSURANCE, March 5, 2002 © 2002 RTCA, Inc., Retrieved January 13, 2010 from: **http://www.rtca.org/downloads/DEC%202004%20-%2005-01-06.htm#_Toc92863900**

2. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, July 2009, Version 3.1 Revision 3 Final, Common Criteria Recognition Arrangement (CCRA), Retrieved January 13, 2010 from: **http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.ppdf**

3. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, July 2009, Version 3.1 Revision 3 Final, Common Criteria Recognition Arrangement (CCRA), Retrieved January 13, 2010 from: **http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3%20-%20marked%20changes.pdf**

4. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, Common Criteria Recognition Arrangement (CCRA), Retrieved January 13, 2010 from: **http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-%20marked%20changes.pdf**

5. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3 Final, Common Criteria Recognition Arrangement (CCRA), Retrieved January 13, 2010 from: **http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3%20-%20marked%20changes.pdf**

6. DCID 6/3 - Manual, DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/3 PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS, Retrieved December 2, 2009 from: **http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm**

7. Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009 (INCLUDES UPDATES AS OF 09-14-2009), Information Technology Laboratory National Institute of Standards and Technology (NIST), Gaithersburg, MD, Retrieved December 2, 2009 from: **http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf**

8. Measuring software quality A Study of Open Source Software, March 6, 2006, Coverity Inc., 185 Berry St. Suite 3600, San Francisco, Retrieved February 22, 2010 from: **http://www.docstoc.com/docs/20886683/Measuring-software-quality-A-Study-of-Open-Source-Software**

9. Coverity_White_Paper-Scan_Open_Source_Report_2009, Date Unknown, Coverity Inc., 185 Berry St. Suite 3600, San Francisco, Retrieved February 26, 2010 from: **http://scan.coverity.com/report/Coverity_White_Paper-Scan_Open_Source_Report_2009.pdf**

10. Quality assurance From Wikipedia, the free encyclopedia, Wikimedia Foundation, Inc., San Francisco, California, Date Unknown, Retrieved February 24, 2010 from: **http://en.wikipedia.org/wiki/Quality_assurance**

11. Open source From Wikipedia, the free encyclopedia, Wikimedia Foundation, Inc., San Francisco, California, Date Unknown, Retrieved February 26, 2010 from: **http://en.wikipedia.org/wiki/Open_source**

12. Staying close to upstream projects, © 2010 Red Hat, Inc. and others, January 18, 2010, Retrieved February 26, 2010 from: **http://fedoraproject.org/wiki/Staying_close_to_upstream_projects**

13. Red Hat contributions, © 2010 Red Hat, Inc. and others, January 19, 2010, Retrieved February 26, 2010 from: **http://fedoraproject.org/wiki/RedHatContributions**

14. Fedora Statistics, © 2010 Red Hat, Inc. and others, February 25, 2010, Retrieved February 26, 2010 from: **http://fedoraproject.org/wiki/Statistics**

15. RHEL, © 2010 Red Hat, Inc. and others, February 16, 2010, Retrieved February 26, 2010 from: **http://fedoraproject.org/wiki/RHEL**

16. Community: Open Scrutiny of Open Source Code, linux today, March 18, 2006, Retrieved February 26, 2010 from: **http://www.linuxtoday.com/developer/20060318008260SCYDV**

17. 2009, 2008, 2007, 2006, 2005 Vendor Value Study, CIO Insight Magazine, 2006 - 2010, Retrieved February 26, 2010 from: **http://www.cioinsight-digital.com/cio/200910/; http://www.redhat.com/f/pdf/CIOI_0811_ResearchPDFS.pdf; http://www.redhat.com/f/pdf/CIO_vendor_value_survey_2007.pdf; http://www.redhat.com/f/pdf/CIO_insight_research_study_2006.pdf; http://www.redhat.com/f/pdf/sec/CIO_research5_1205.pdf**

18. CIO Insight Vendor Value Ranking, Copyright © 2010 Red Hat, Inc., Retrieved February 26, 2010 from: **http://www.redhat.com/promo/vendor/**

19. Worldwide IT Education and Training 2009 Vendor Analysis, IDC MarketScape, (excerpt of work by Cushing Anderson), Date Unknown, Retrieved March 9, 2010 from: **https://www.redhat.com/f/pdf/training/IDCVendorAnalysis2009.pdf**

20. CertCities.com's 10 Hottest Certifications for 2006, Becky Nagel, Date Unknown , Retrieved March 9, 2010 from: **http://certcities.com/editorial/features/story.asp?EditorialsID=95&page=4**

RED HAT SALES AND INQUIRIES

NORTH AMERICA
1-888-REDHAT1
www.redhat.com

EUROPE, MIDDLE EAST AND AFRICA
00800 7334 2835
www.europe.redhat.com
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

LATIN AMERICA
+54 11 4341 6200
www.latam.redhat.com
info-latam@redhat.com

www.redhat.com
#2060947_0410