OPEN SOURCE UPDATE

Paul Tibbits, MD
DCIO Architecture, Strategy, and Design
Department of Veterans Affairs

VA Open Source History

- Mar 2011: VA **contract** to establish EHR open source custodial agent & start "Gold Disk" Tiger Teams
- Jun 2012: CIO - work VISTA enhancements by engaging open source community who have followed VISTA releases closely & have supported non-VA users of VISTA derivatives
- Aug 2012: CIO - re-standardize VISTA implementations at VAMCs to VISTA Platinum image & to increase governance over continued Class 2 & 3 development
- Oct 2012: Product Development Code in Flight Program initiated. Start sharing development projects BEFORE they were finalized & released nationally.
- Aug 2013: Directive 6402 on Modifications to Standardized National Software refreshed & new policy on what is permitted for Class 2 & 3 enhancements
- Jun 2014: CIO – expands to all SW products
- Sept 2014: VA public Github at http://usdeptveteransaffairs.github.io
- Jan 2015: CIO - evaluate open source products when VA acquires SW

VA's Expectations of OSEHRA

- VA established EHR open source ecosystem facilitated by Open Source Electronic Health Record Alliance (OSEHRA) to advance introduction of open source EHR SW
- OSEHRA facilitates orderly, reliable, efficient interactions
  - Users acquire, install, use, & maintain Open Source VistA based on certified code base as well as proprietary software that has been certified for code base
  - Any member of community may improve Open Source VistA code base, & contribute to OSEHRA
  - Organizations and commercial vendors can build open source products based on code base, as well as proprietary products & technologies & have them certified
  - Vendors can mix and match proprietary & open source code in their offerings
  - Academic & research institutions can participate in EHR innovation by both using & contributing open source code.

OSEHRA's Expectations of VA

- VA
  - Shares project design plans under development with open source community
  - Shares incomplete code base while it can still be redesigned
  - Engages open source community on business requirements to share burden on development that impacts non-VA health policies and capabilities as well as VA health policies and capabilities
  - Intakes enhancements to VA software that open source community has proven is trustworthy, of quality and is of value, that can also be equally beneficial to VA
  - Participates in Code Convergence efforts to identify single open source VISTA codebase that all VA and non-VA VISTA users will commonly use
  - Minimizes proprietary solutions when seeking IT solutions that are necessary to meet VA's business or technology requirements
  - Maximizes volume of VA software that we share with community or we take in from community

CIO's Expectations of OIT

- Introduce more open source software into VA or share it outside VA without placing VA infrastructure or VA customers at risk of security or legal ramifications
- Keep requirement to meet VA's mission highest priority, while understanding that our efforts & our cooperation can provide solutions outside of VA
- Work transparently in VA code base and be visible to open source community in order to collaborate more openly, without disruption or endangering our project commitments and obligations

Code in Flight Program

- PD's Code in Flight program has been releasing VA software deliverables that are currently in development and/or that have not yet been released since 2012
  - Unreleased software and design plans that have never been shared before
- Ends 30 year history of releasing only final and nationally released software via VA Freedom of Information Act (FOIA) controlled procedures
- Share code & plans regularly from existing recurring builds and documentation reviews without depending on individual PMs & developers to understand governance VA needs to impose
- Code in Flight consists of OI&T goal to release project requirements & design early & often for collaboration, education, or "good neighbor" treatment of open source community
- **CIO stated that open source activities & Code in Flight is no longer JUST applicable to our health products development activities**
- **CIO stated that ALL VA release OUTSIDE VA of ANY VA software in ANY condition must go through single office for preparation prior to release**

Code in Flight

- Event points added to ProPath Sept 2012 Release
- Includes source code, executables, associated SW engineering documents (draft or final), test cases, test scripts
- Must be FOIA redacted to remove
  - Security methods, parameters, constants, etc., from SW, data, docs
  - Commercially licensed content from SW, data, docs.
- Must be validated to make sure VA is permitted by copyright and ULAs to redistribute both source & executable code *as it has been used & altered so VA & users not at risk of legal issues*
- Must have VA OGC Disclaimer Watermarks added
- Published as Technical Journals on OSEHRA site
- May be relocated to public VA Github site

Year	Publications
< 2012	0
2012	4
2013	15
2014	150
2015	74 to date

Seeking more feedback from open source community on publications

FOIA Redaction
…And Why They Love to Hate It

Of 9 FOIA Exceptions, 4 apply to VA:

1. Documents properly classified as secret in interest of national defense or foreign policy;
2. Related solely to internal personnel rules and practices;
3. Specifically exempted by other statutes;
4. Trade secret or privileged or confidential commercial or financial information obtained from a person.

What does redaction do to code and documents?

- Reduces functionality and/or design details. Causes inoperability.

How can we get redaction eliminated from our requirements?

- Design to eliminate redaction
- Move secure content to files more easily removed or substituted
- Adopt software usage policy: 1) avoid commercial SW & data; & 2) use only most liberal, permissive open source license

What Is Redacted From VA Software?

Security-Related Redaction	Licensing-Related Redaction	General Housekeeping
Explicitly named VA physical server identifiers	Copyrighted data tables for CPT codes, categories, and modifiers	Scheduled background tasks*
Explicitly named VA user or group information (any attribute associated to a user/group entry)	Copyrighted data tables for Medication Instructions and Warning Labels	Error logs*
Mail domain identifiers	Copyrighted or protected Dietetics Vendor information	Domain and mail traffic and statistics*
Encryption formulas	DSS, Inc. Dental Record Manager – all components	Audit, log and sign-on files*
	DSS, Inc. Release of Information Manager – all components	References to "VA" in screen displays or print outputs generated by software
	Any other licensed embedded code libraries the user agreements do not allow VA to redistribute in their present state	**applies to redaction of a VISTA running instance only, not software builds*

Code in Flight Steps (ProPath)

Process	Activity	Activity Name	Provide to ossoft@va.gov
Project Planning	PRP-PR1	Conduct Peer Review of RSD	• RSD
	PRP-FR1	Conduct Formal Review of RSD	• RSD
	PRP-PR2	Conduct Peer Review of SDD	• SDD
	PRP-FR2	Conduct Formal Review of SDD	• SDD
Product Design	DES-4.2	Design Logical Database	• Logical Data Model
	DES-4.5	Document Database Design	• SDD
Product Build	BLD-7	Provide to Open Source	• VDD • Build + Source • Test cases, scripts • RSD, SDD, Data Model
Test Preparation	TST-7	Provide to Open Source	• VDD • Build + Source • Test cases, scripts • RSD, SDD, Data Model
Independent Test and Evaluation	ITE-5	Provide to Open Source	• VDD • Build + Source • Test cases, scripts • RSD, SDD, Data Model

VISTA Intake Program

VISTA Intake Program launched in Jan 2015

- Initial focus on FileMan convergence & several VA field-based Class 3 initiatives
- Outcomes from OSEHRA code convergence sprints expected to feed VIP candidates
- Outcomes from OSEHRA joint discussion groups to feed VIP candidates
- Code must be intact with no remaining enhancements necessary to be functional in VA
- Code must be primarily M-based, limited to VISTA environment, and qualify for fast pass PMAS workflow
- Intake queue needs more open source candidates in which VHA has shown interest

Any open source product introduction that is not qualified for VIP must either be approved to be included in existing PMAS project, bug/fix, or obtain approval for new project activation. It must comply with all current technical standards, quality and security reviews and project approval procedures.

Use of Open Source Software

- VA approach has broadened in identification and use of clinical and business software that creates larger footprint as open source alternative.
- OS meets definition of “commercial computer software” and is given appropriate statutory preference in accordance with 10 USC 2377 (reference (b)) (see also FAR 2.101(b), 12.000, 12.101 (reference (c)).
- Executive agencies are required to conduct market research when preparing for procurement of property or services by 41 USC Sec. 253a (reference (e)) (see also FAR 10.001 (reference (f)). Market research for software should include OSS when it may meet mission needs.

Open Source Evaluation Criteria & Governance

Establishing clear OS evaluation criteria will prevent OS that cannot be approved for use. Typical criteria include elements such as:

- Architectural compatibility
- Component modification needs
- License compatibility
- Code quality
- Code stability and maturity
- Quality and completeness of documentation
- Security evaluation
- Availability of support
- Activity level of the community or health of commercial support vendor
- Project maturity and its originating community
- Intellectual Property risk evaluation

License Compliance

- 50+ individual open source licenses to choose from
- In organizations that distribute SW containing OS, compliance with relevant OSS licenses is critical element of OS management
- Compliance requirements of some OS licenses are triggered on alteration, others on distribution, or, for few OS licenses such as AGPL, on delivery of network service using code
- OS policy needs to clarify responsibilities for checking & executing compliance requirements, which must include tests for
  - Code notice compliance
  - Documentation notice compliance
  - Splash or about-screen compliance
  - Contract addenda and terms compliance
  - Source code provisioning compliance
- **Often VA developer has reported no or minimal understanding of the specific usage permissions of OS code that s/he has been asked to identify when redaction has located copyright or user license information in code base**
- **Due to turnover in development resources, some do not know what OS is in their code.**

Licensing Issues

- There is misconception that Government is always obligated to distribute source code of any modified OS to public, & therefore that OS should not be integrated or modified for use in confidential or other sensitive systems
- In contrast, many open source licenses permit user to modify OS *for internal use* without being obligated to distribute source code to public
- However, if VA distributes code outside of VA, then some OS licenses, or conversely VA will, require distribution of corresponding source code
- It is important to understand both specifics of open source license in question & how VA intends to use & redistribute VA-modified OS
- **Several VA products identified during redaction that incorrectly incorporated, altered, or re-distributed inside or outside VA, open source code that was not permissible based on terms of open source license, or user license agreement set in force by original creator**

Open Source Licenses And The Apache 2 Challenge

- VA for several years has allowed reusable code libraries on the One-VA Technical Reference Model that are licensed by a variety of OS license models.
- VA has placed 144 Apache 2 licensed products on the One-VA TRM for use by VA development teams and continues to grow that number.
- VA has not come to a decision or action plan to divest itself of all code that does not allow for an Apache 2 license to be applied.
- Product Development must do an inventory and an impact analysis on the dependency existing and pending products have on all other OS licensing.
- This analysis has not yet occurred.
- VA recognizes the impact of a decision will have on our contributions to open source but must mitigate a change in policy with a plan of action in order to support it.

One-VA Technical Reference Model (TRM) http://trm.oit.va.gov/

January 2010: One-VA TRM Compliance was mandated by the CIO.

- The **OFFICIAL** One-VA TRM website is http://trm.oit.va.gov
- The public **FOIA REDACTED** copy at http://www.va.gov/trm is for PROSPECTIVE vendors ONLY.
- Content on the Intranet site updated every two weeks or sooner if an emergency.
- **Do NOT use the Internet website. Use the Intranet website.**

Major 2014 Changes:

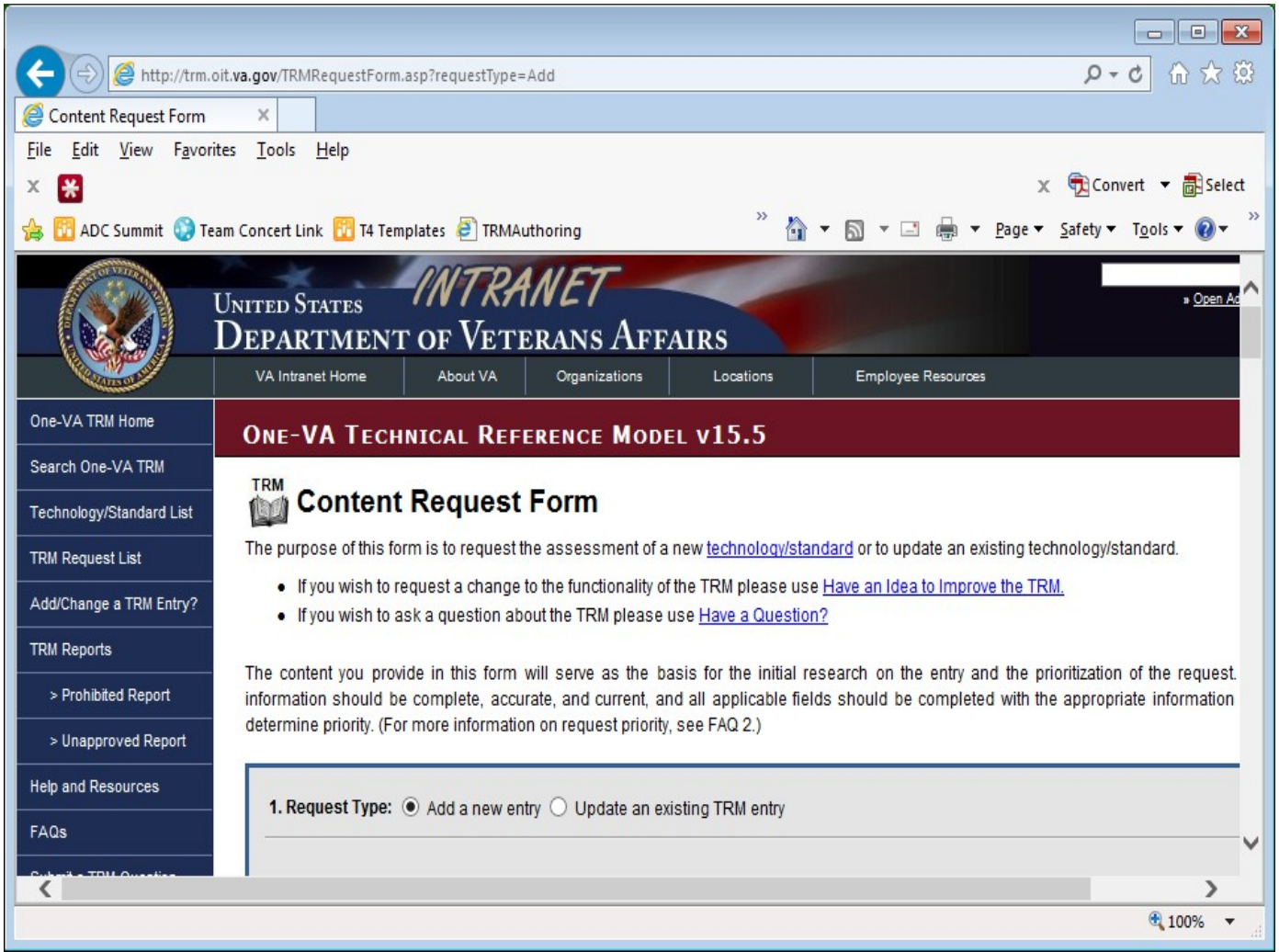
- **Old**: FEA Categorization of Entries. **New**: VA Categorization of Entries.
- **Old**: Decisions by Entry. **New**: Decisions by version and by quarter within entry.
- **Old**: License listed & w/POC info. **New**: ELA License managed by SDE TIP Office
- More attention to dependencies, components, comparable products, and standards.

Major 2015 Changes:

- Reader mail subscriptions to entries, categories, or subcategories.
- Development frameworks; development standards; Class 1 VA applications; Class 1 COTS products; and hardware getting added.
- Correlation between OneVA-TRM, VASI, SCCM, BDNA, and Technopedia catalogs.

One-VA Technical Reference Model (TRM)
http://trm.oit.va.gov/

http://trm.oit.va.gov/TRMRequestForm.asp?requestType=Add



Month	Published
May-14	179
Jun-14	225
Jul-14	146
Aug-14	177
Sep-14	290
Oct-14	299
Nov-14	156
Dec-14	236
Jan-15	216
Feb-15	236
Mar-15	352
Apr-15	157

One-VA TRM and Section 508 Integration

Prompted by recent Red Flag calls about lack of 508 compliance in COTS products in use by nationalized implementations.

As of 4/23/15, Dr. Tibbits announced that 508 compliance information will be included with all new TRM entries.

- "A product is either 508 compliant or not. There will be no ambiguous states of partially compliant, semi-compliant, etc."
- "If the 508 office determines a TRM entry is not 508 compliant the decision will be (regardless of other OIT pillars recommendations) prohibited for further proliferation until such time that 508 compliance is met."
- "Projects or programs using non 508 compliant technologies or standards will be halted."

One-VA TRM and Section 508 – Definite Change

Definite: Leadership **wants known** 508 status available at product's initial TRM entry.

- Incorporate 508 information **on hand** into the TRM.
- Content Request Form change to require **requestors** to submit a VPAT (and/or GPAT).
- Determine and document any known justification to **except** a product from 508.
- Section 508 Office required to document **existing** information **asserted** by the manufacturer *OR* validated by VA.
- Prioritize full 508 testing and analysis based on negotiated priority factors.
- Build 508 content in the TRM entries with more detailed 508 review outcomes as the scheduled 508 tests complete.
- 508 office to work independently to build content with respect to 508.
- **Does not hold up publication of initial decisions**.

One-VA TRM and Section 508 – Possible Change

Possible: Leadership **may want unknown** 508 status to be determined at time of product's initial TRM assessment.

- Require full 508 compliance testing for any TRM request prior to publication in the TRM.
- Determine and document any known justification to except a product from 508 compliance requirements.
- If not excepted, requires a scheduled full 508 hands-on testing and analysis while the product is also under TRM review.
- Both reviews would be necessary to complete prior to communicating a TRM decision to the requestor or any initial publication in the TRM.
- Prioritize a full 508 testing and analysis among the requests currently pending TRM decision.
- **Hold up all TRM decisions until the full 508 results are delivered.**
- Pre-existing TRM content prioritized for their full 508 reviews and **existing TRM decisions adjusted to reflect outcomes from 508 reviews**.

Section 508 Exception Criteria

Exception #	Section	Exception
1	1194.3a	National Security
2	1194.2a	Undue Burden
3	1194.3b	Contractor Incidental
4	1194.3e	Fundamental Alteration
5	1194.3f	Back Office

Commercial non-availability - This is not an exception to Section 508. When procuring products in the commercial marketplace, the Government must buy the most accessible products that meet their business needs.

No Presentation Layer - Machine-to-machine transactions do not have to meet the Section 508 standards. However, the mechanism for someone to request the transaction must be accessible; the viewable output from the transaction must be accessible; and any notifications about the status of the transaction must be accessible.

Undue Burden & Back Office Exceptions

- Of all of the Section 508 exceptions, **Undue Burden** is the least likely to be approved. An agency cannot claim Undue Burden to the Agency just because a product or service that meets the Section 508 standards is significantly more expensive than one that does not.

- Software which is installed or operated on a product which falls under the **Back Office** exception would be exempt from the standards if the software application could only be operated from the physical place where the product is located.
- By contrast, if the software could be operated from a remote workstation, the software would be subject to the 508 standards irrespective of who is using it since the product interface is not located in a physical space which meets the criteria for this exception. This disqualifies most any product that IT management-related, that is **not** restricted to a physically locked down location, albeit limited use purpose.

National Security & Contractor Incidental

- **National Security** applies to technology that is used in intelligence or cryptologic activities as related to National Security **or** it is used in the command and control of military forces **or** it is integral to a weapon or weapons system **or** it is critical to the direct fulfillment of military or intelligence missions.

- **Contractor Incidental** is technology that acquired by a contractor during a services contract that is **purchased by** a Government contractor **for use by** a Government contractor. It is **never** used by Government personnel and is **never** delivered and **never** transitioned to the Government. **Warning:** If IT products, services or deliverables in question were paid for using Government funds or ever used by the Government, then this exception **does not** apply.

Questions?

PD TRM Mail Group: PDTRM@va.gov
Open Source Mail Group: OSSOFT@va.gov