



# **Lessons Learned Automating SAP Testing**

Eric Loeb, PhD

July, 2014



# Overview

- Why software test automation is important
- Summary of the DOT&E/DLA collaboration on SAP test automation using the DISA cloud framework
  - DOT&E: Director of Operational Test and Evaluation
  - DLA: Defense Logistics Agency
  - DISA: Defense Information Systems Agency
- Timeline showing dominance of organizational vs technical issues



# Two Problems in DoD Software

1. Early testing: operational users should test software interfaces during **design** (Best practice for 30+ years)
  - Users often identify new requirements when first exposed to system interfaces
  - Fulfilling those requirements can alter data flows and alter software design
  - “Operational users” also means administrators, maintainers, and network defenders
  
2. Software sustainment starts during **build** (Best practice for 25+ years)
  - Software sustainment includes
    - Configuration control
    - Defect tracking and prioritization
    - Maintenance of a high fidelity test environment
    - Testing of patches and upgrades within the test environment
  - These sustainment activities are needed during development
  - The reliability of software deployed without these activities already in place
    - Is poor
    - And will grow worse with each effort to correct the discovered defects



# Improved Software Sustainment Can Really Help

## Defense Enterprise Accounting and Management System (DEAMS)

- May, 2010 DEAMS Increment 1 Release 1 deployed to 1,100 users as a “technology demonstration”
- Dec, 2010 AFOTEC OA found 245 high priority defects
- June, 2012 PMO claimed all but 18 of 245 defects fixed prior to OA-1
- June, 2012 OA-1 of Inc. 1 Release 1.1, DOT&E found 200 high priority defects
- AFOTEC report\* observed that PMO did not perform any regression testing
- Spring 2013 PMO implemented manual regression testing and improved configuration management
- June, 2014: DEAMS has made substantial progress without introducing new systemic issues. An August 2013 assessment found improved configuration management and that DFAS had, in concert with the FMO, made progress in resolving some of the key deficiencies noted during OA-1

## Navy ERP

- May 2008 Release 1.0 IOT&E: suitable but software unstable and not effective. Poor change management (user communications and cut-over)
- May 2009 Release 1.0 FOT&E: suitable and effective. Improved user communications and cut-over labor
- Oct. 2010, Release 1.1 IOT&E: After 6 month stabilization period, system was still too immature for assessment of effectiveness.
- May 2013 Release 1.1 FOT&E: Improved software Configuration Control Board. Regression testing covers full functionality and is 87% automated. System is effective and suitable.



# New Policies Mandate Better Software Sustainment

## OT&E Policy:

For software in any system, the evaluation of operational suitability will include a demonstrated capability to maintain the software. Program managers must sustain an operationally realistic maintenance test environment in which software patches can be developed and upgrades of all kinds (developed or commercial) can be tested.

(1) IOT&E or a prior test event will include an end-to-end demonstration of regression test, preferably automated, in the maintenance test environment from requirements to test scripts to defect tracing.

(2) IOT&E or a prior test event will include a demonstration of processes used to update the maintenance test environment so as to replicate deficiencies first found in the operational environment.

## Live Cycle Sustainment Policy:

Life-cycle sustainment for information system components ... will identify inherently governmental decisions in software sustainment such as scope and prioritization of upgrades, vendor selection, and acceptance of software patches prior to deployment. ... Application of software sustainment best practices such as version control, defect tracking, establishment of development and test environments, pre-deployment and regression testing will be aligned to support beginning of software development, typically near MS-B, through the program schedule.



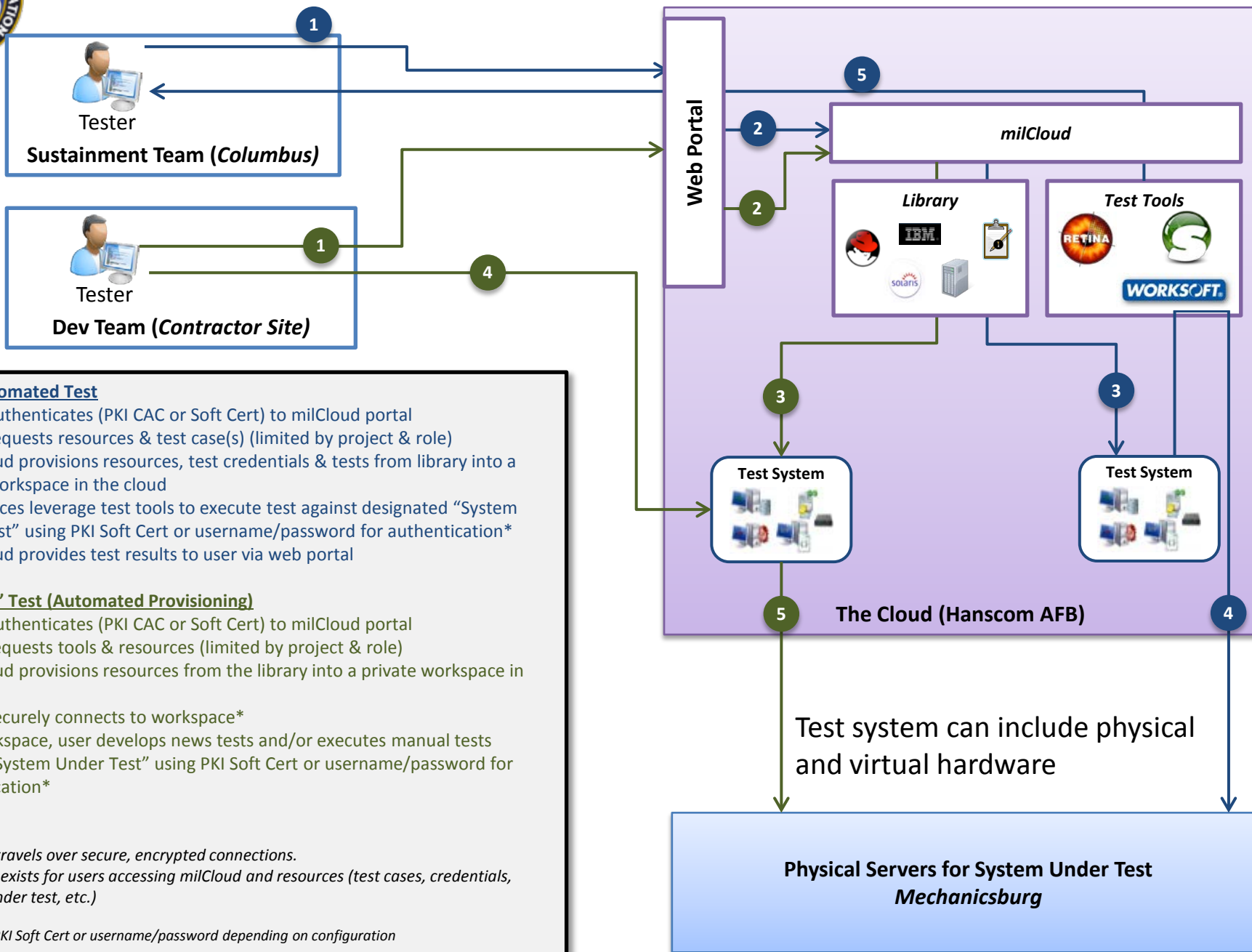
# Faster Sustainment with the DISA Cloud (MilCloud)

- Bare metal: person installs and configures each software package in the software stack onto each machine in network
  - ~8 hours/machine of person time
- Virtual Machine (VM): person installs like bare metal but can then hit a button to clone the VM. Must then configure VMs into real network
  - ~4 hours/machine of person time
- VM Library: person installs various pre-stored virtual **machines** with a button click and then configures VMs into real network
  - ~40 minutes/machine of person time
- MilCloud Recipe: person pushes button to configure virtual **network** AND install AND configure software packages onto each virtual machine
  - ~8 minutes/machine of machine time

Example software stack

<b>DIB Test Data</b>
<b>DIB MDF</b>
<b>DIB Customization</b>
<b>JBOSS</b>
<b>Java JRE 1.6 u33</b>
<b>Java JDK</b>
<b>DIB Prerequisites</b>
<b>Oracle 11g</b>
<b>Red Hat Ent. Linux</b>

# DLA use of MilCloud and Worksoft for SAP testing



## Fully Automated Test

1. User authenticates (PKI CAC or Soft Cert) to milCloud portal
2. User requests resources & test case(s) (limited by project & role)
3. milCloud provisions resources, test credentials & tests from library into a private workspace in the cloud
4. Resources leverage test tools to execute test against designated "System Under Test" using PKI Soft Cert or username/password for authentication\*
5. milCloud provides test results to user via web portal

## "Manual" Test (Automated Provisioning)

1. User authenticates (PKI CAC or Soft Cert) to milCloud portal
2. User requests tools & resources (limited by project & role)
3. milCloud provisions resources from the library into a private workspace in the cloud
4. User securely connects to workspace\*
5. In workspace, user develops news tests and/or executes manual tests against "System Under Test" using PKI Soft Cert or username/password for authentication\*

## Notes

All traffic travels over secure, encrypted connections.  
 Audit trail exists for users accessing milCloud and resources (test cases, credentials, systems under test, etc.)

\* PKI CAC, PKI Soft Cert or username/password depending on configuration



# DLA's SAP Test Automation Results (Nov. 2013)

- **Training**

- milCloud-Trained DLA sustainment staff: **20**
- Certify-Trained DLA staff developing test scripts: **6**
- DLA Staff attending Certify Training in Columbus **14**

- **Test Scripts**

- Manual scripts automated and transitioned: **13**
- Scripts in development: **8**
- Test Processes Library (sub routines) **500+**
- Average setup and execution time
  - Automation: **18 minutes**
  - Manual : **142 minutes**

**~90%  
Improvement**

- **Operations**

- Automated scripts used to date: **3**
  - Nov 23, 2013; 2 scripts for Enterprise Business System (EBS) maintenance window
  - "Routine" (3x) security testing of system and SAP patches and updates
- Automated scripts scheduled for future use: **4**
  - Oct, 2013 – Jan, 2014; Energy Convergence Release 3 regression test
  - "Routine" use of SAP ECC CERT for security testing
  - Dec 14, 2013; EBS maintenance window
    - The November maintenance window script was developed by a user (Noel Sarmiento, Accenture) from existing components in Test Process Library

**This 90% improvement cost \$500,000 in**

**2013**





# DLA's SAP Test Automation Results (June 2014)

**Goal:** Achieve DLA self-sufficiency and integrate automation into regular testing

- **Training**

- MilCloud-Trained DLA sustainment staff **72**
- Certify-Trained DLA staff developing test scripts **39**

- **Test Scripts**

- Manual scripts automated and transitioned **52**
- Total time (staff hours) devoted to script development **927**
- Test Processes Library (subroutines) **1093**

- **Operations**

- Automated tests executed this month **28**
- Process steps executed this month **132,139**
- Defects discovered by automation this month **8,234**  
(process steps that failed in execution)
- Total staff hours (for execution) this month **<1**



## Timeline showing dominance of organizational vs technical issues

10/12/11: DOT&E recommends automated regression testing for MS-C Eprocurement decision

01-05/12: JITC implements 1 script; \$1M proposal for follow-on (hire SAP)

07/27/12: milCloud \$500k proposal approved by DLA

09/30/12: Funding is released

11/01/12: milCloud/Worksoft ready but test system suffers continuing issues

01/09/13: DOT&E forces contractors to work together to develop detailed firewall debugging plan

01/11/13: Firewall/communications working; first Worksoft script working same day

01/14/13: PEO Tinston, Columbus users, Jackpine, DOT&E conference call. "Go!"

02/06/13: Intro call with DLA manual regression testers to define work; Columbus users require SCR

02/13/13: System Change Request (SCR) submitted

03/05/13: SCR sent to Columbus team for cost estimation; questions about soft certs

04/11/13: 2-day kickoff meeting with DLA users starts in Columbus

05/02/13: SAP Cert GUI test script finds unanticipated errors; development effort begun for soft certs

06/27/13: First script handoff to user; soft certs code ready for review

07/20/13: New soft cert login code accepted, but now soft certs have expired

08/03/13: 2<sup>nd</sup> site (Richmond) connected and 2<sup>nd</sup> DLA user developing scripts

08/15/13: Users present business case and demo; 2<sup>nd</sup> year authorized

09/26/13: Soft certs working. Full automation enabled

- 2 calendar years but < 1 FTE of engineering effort
- 2 months of multi-contractor confusion starting Nov. 2012.
- 3 months for staff to move out after told by PEO to move out in Jan. 2013



# Death by 1000 cuts

11/09/12:

Form 2875 rejected by a human being

PDF form printed from Apple had dark circles in the boxes.

11/13/12:

Re-submitted form printed from x86 was accepted

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)	
<b>PRIVACY ACT STATEMENT</b> AUTHORITY: Executive Order 10450, 9307, and Public Law 93-502, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is not intended. Failure to provide the requested information may impede, delay or prevent further processing of the request.	
TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DIRECTIVE <input type="checkbox"/> USER ID	DATE (YYYYMMDD) 20121109
SYSTEM NAME (Platform or Application) USE4 LAN Account	LOCATION (Physical Location of System) Remote User - Hanscom AFB
<b>PART I (To be completed by Requestor)</b>	
1. NAME (Last, First, Middle initial) Chambers, Jeffrey, E	2. ORGANIZATION HQ DLA
3. OFFICE SYMBOL/DEPARTMENT J-622	4. PHONE (DSN or Commercial) 978-263-6025
5. OFFICIAL E-MAIL ADDRESS jeffrey.chambers.cjr@dla.mil	6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP <input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input checked="" type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input checked="" type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) 20120719	12. DATE (YYYYMMDD) 20121109

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)	
<b>PRIVACY ACT STATEMENT</b> AUTHORITY: Executive Order 10450, 9307, and Public Law 93-502, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is not intended. Failure to provide the requested information may impede, delay or prevent further processing of the request.	
TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DIRECTIVE <input type="checkbox"/> USER ID	DATE (YYYYMMDD) 20121109
SYSTEM NAME (Platform or Application) USE4 LAN Account	LOCATION (Physical Location of System) Remote User - Hanscom AFB
<b>PART I (To be completed by Requestor)</b>	
1. NAME (Last, First, Middle initial) Chambers, Jeffrey, E	2. ORGANIZATION HQ DLA
3. OFFICE SYMBOL/DEPARTMENT J-622	4. PHONE (DSN or Commercial) 978-263-6025
5. OFFICIAL E-MAIL ADDRESS jeffrey.chambers.cjr@dla.mil	6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP <input checked="" type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input checked="" type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input checked="" type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) 20120719	12. DATE (YYYYMMDD) 20121110

Form rejected by a person because of difference in these Xs



# Issue Details: Aug-2013 to Nov-2013

Are some accesses easier to acquire (Workbench) than others (cFolders)? Or is this due to a lack of end-to-end team communication?

Softcert expiration significantly delayed portal work. We know when the softcerts will expire... better advance planning and "ownership" required. But we still haven't opened up the DLA firewall to whole environments (i.e. SP3) or mapped certs to roles (e.g. all roles other than those key roles needed right now.

The stability of "the" connection is an ongoing saga. The complexity of the actual communication path from a tester/developer through DLA (Columbus/Richmond), to milCloud (Hanscom), and on through to the DECC (-M/-O) is daunting when trying to isolate a sporadic, ill-defined problem. Add to this, various tester/developer's VPN'ing into DLA when teleworking, and/or differences in DLA workstation configurations (Richmond!=Columbus), differing access to Firefox (local, via Citrix), and every problem is a potential time sink.

08/22: MilCloud Certify virtual workstation requires access to cFolders

08/23: Softcerts expire, no portal access, proceed with GUI work

08/26: Connection stability issues between DLA and milCloud resurface

08/30: Connection stability issues believed to be resolved (relaxing webserver garbage collection)

09/04: Connection stability issues between DLA and milCloud resurface

09/06: MilCloud Certify virtual workstation requires access to EBS workbench

09/06: Local Firefox right-click menu overlays remote Certify right-click menu

09/07: Access to EBS workbench established.

09/09: Daily distribution of the Issues/Blockers log begins.

09/09: New softcerts deployed, need to be mapped to user accounts & roles (SP1/3/4, QP1)

09/11: Firefox right-click menu setting will not be allowed (DLA IA STIG enforcement)

09/13: Alternative connection type (VNC) provided (limited graphics resolution)

09/16: Firefox browser workaround identified (map to middle click)

09/20: Daily distribution of the User-Softcert-Role (by System) matrix begins

09/26: Key softcerts mapped to key user accounts & roles (SP1)

10/08: Access to cFolders established.

10/08: Connection stability issues between DLA and MilCloud resurface

10/25: Connection stability issues believed to be resolved (bypassing DLA proxy server)

Browser issues... DLA baseline is IE8, not supported by milCloud (IE9+). Firefox preferred, but not part of the DLA workstation baseline image. Special request possible. Others in DLA can access Firefox via Citrix. DLA configuration settings for Firefox, IA STIG enforced, cause nuisance issues.



# Conclusions and Recommendations

- Implementing test automation is a business process re-engineering effort
  - Strong, consistent management involvement is needed
  - There will be push-back
- In practice, costs must be low
- But time to execute will be high
- But the problems are mostly internal delays, not technical challenges
- Therefore: contract for a part-time, 2-person team
  - Administrator to manage process (~1/4 FTE)
    - Direct line to senior government leader
    - Must recognize, report, and help fight bureaucratic delays
  - Software engineer to work when possible
    - (0 – 1 FTE at sputtering pace)



# For Further Information

Eric Loeb

DOT&E Special Assistant

[Eric.P.Loeb.Civ@mail.mil](mailto:Eric.P.Loeb.Civ@mail.mil)

703-697-3655