



NDIA #19693: Program Management in HPCMP-CREATE™ (A Family of Large-scale, Physics-based, System-of-Systems, Software Development Projects)

An Application of Risk-based Management Practices in Software Development



**Richard P Kendall, Ph.D. with
D.E. Post, L.G. Votta, P. A. Gibson, L. A. Park and S.M. Sundt
October 2017**

Distribution A: Approved for Public release; distribution is unlimited.

Program Management in CREATE

- If you were starting a new
- distributed,
 - physics-based,
 - system-of-systems
 - HPC-capable

DoD software development project

**How would you manage
it for long-term success?**

...based on the CREATE experience

Program Management in CREATE

Why should you have
confidence in the staying
power of CREATE?

Start by Recognizing that Software Development is a Risky Enterprise

WASHINGTON SPECTATOR

LOU DUBOSE, Editor
JUNE 15, 2012
VOL. 38, NO. 11, ISSN 0887-428X
© The Public Concerns Foundation
www.washingtonspectator.com

Facebook Respond to Zuckerberg's Failed IPO

...who can get shares of the Facebook IPO should have as many shares as possible. ...Cramer's toast on Wall Street, stock, and ...'s writing "an in-depth look at the Facebook IPO should ...er's good fortune that he is not legally responsible for ...e broadcasts. Trial lawyers who understand securities ...e filed lawsuits against Facebook in federal courts ...s, representing investors who acted on the sort of hype ...s was selling. (See "Legal Distillates," page 2.)

The litigation will take some time. And it will take Facebook public in a way the company didn't anticipate, as the discovery process opens up the files and e-mail accounts of principals, bankers, and traders who worked the social network's initial public offering. The markets promptly delivered their verdict.

Ten days after Facebook's over-heated May 18 IPO, investors were dumping the shares at a low of \$28.05. That is \$14 a share below the highest quote on the day of the offering, when the price was artificially inflated by the price as Facebook's IPO.

Morgan Stanley, the book runner, Morgan Stanley through the first day of the stock offering, creating the released huge blocks of stock with the intention of creating a rebound of demand. It worked for a day. Even if the investment bankers didn't get the huge IPO "pop" they were trying to create, they defended their price as the stock opened at \$38, climbed to \$42, and closed at \$38.23.

One week later, the jig was up and the price was down. If you were a retail buyer on May 18, you were the sucker. Or the sucker. You lost. Mark Zuckerberg won. A billionaire many times over. The Facebook founder and CEO finds it easier to absorb the loss of \$20 billion in market capitalization than does the small investor absorbing a 30 percent loss in the value of stock purchased on his honeymoon in Italy. Zuckerberg personally lost \$4 billion. Morgan Stanley's junior futures trader and analyst I have touched the Facebook

Mexico Considers Legalizing Drugs

Billions Wasted on DoD Software

The victors in battles are those who create, modify and deploy ideas faster and more nimbly than opponents. Regrettably, limiting the U.S. military's access to ideas risks failure.

For years, the U.S. military has been losing an asymmetric battle that involves not improvised explosive devices, bullets and bombs, but instead swarms of defense industry contractors seizing control of taxpayer-funded ideas because government policy and regulations were engineered to buy iron and steel, not to deploy a software-based military.

Just like the battles in Iraq and Afghanistan, the rapid and continual evolution of technology demands that the military operate just as rapidly, and the only way is to manage the ideas it has funded.

A common theme since 9/11 is that the U.S. government lacks imagination. We have not misplaced our imagination; we are simply unable to deploy new ideas as effectively or as quickly as we could. This loss of agility stands in stark contrast to the private industry, foreign governments and nonstate actors, who are adopting and deploying software technologies once they are in the military domain.

China deploys advanced electronic warfare technologies, Iran builds unmanned aircraft, al-Qaida evolves weapons, and private companies like FedEx and eTrade create complex, redundant and failsafe command-and-control systems.

It is the fabric that enables planning, weapons and logistics systems to function. It might be the only infinitely renewable military resource. New software builds on the raw material of previous software, evolving capabilities. Software is not just a tool; it is the final expression of a military idea transformed into human readable code and deployed to a battlefield.

The Department of Defense spends tens of billions of dollars annually creating software that is rarely reused and difficult to update. Instead, much of this software is allowed to become the property of defense companies, resulting in the military funding the same solutions or, worse, repaying to use previously created software.

A coherent set of policies and regulations for the DoD's intellectual property has eroded the U.S. military's competitive advantage, leading to compromised missions and lost lives. Improvised explosive device countermeasures are upgraded rapidly without replacing entire systems; personnel position systems can't update in real time; and software updates don't interoperate.

Regulations governing the military's intellectual property portfolio use an antiquated rights structure where the military retains copyright, and therefore effective monopoly, control over taxpayer-funded software ideas. By contrast, the private industry ruthlessly exercises control over its own software ideas.

Congress has legislated a structure that the defense industry will do right by the military. However, the defense industry's interests are best served by its shareholders: maximize profit.

Standards that reduce costs and decrease adaptability and agility in military software. Examples include the canceled Future Combat Systems, where only one company can produce and manipulate the software. Imagine if only the manufacturer of a rifle were allowed to clean, fix, and maintain that rifle. This is where the military finds itself: one contractor with a monopoly on the knowledge of a technology.

To require all taxpayer-funded software ideas to be licensed with an open source software copyright, we would define the rights, roles and responsibilities for the military and defense industry and simplify the process. To keep the U.S. military ahead of its adversaries, the DoD and defense industry must embrace a dysfunctional partnership of nonsharing.

Software intellectual property regime would broaden the defense industrial base by enabling industry to compete, thereby increasing competition and eventually lowering costs. Over time, DoD would evolve a software intellectual property regime that would broaden the defense industrial base by enabling industry to compete, thereby increasing competition and eventually lowering costs. Over time, DoD would evolve

COMPUTING / SOFTWARE

Who Killed the Virtual Case File?

How the FBI blew more than \$100 million on case-management software it will never use.

HARRY GOLDSTEIN / SEPTEMBER 2005

In the early 1990s, Russian mobsters partnered with Italian Mafia families in Newark, N.J., to sell illegal fuel in New Jersey state gasoline and diesel taxes. Special Agent Larry Depew set up an investigation under the direction of Robert J. Chiaradio, a supervisor at the Federal Bureau of Investigation's headquarters.

Depew collected reams of evidence from wiretaps, interviews, and financial transactions over the years. Unfortunately, the FBI couldn't provide him with a database program that would help organize the information, and interviews, but he could not import information from other investigations that might be helpful. It wasn't until Depew mentioned the name of a suspect to a colleague that he obtained a breakthrough.

Depew had been holding since 1989.

When it came to the FBI's Virtual Case File (VCF), it was a treasure trove of information about who's involved in the conspiracy, including names, addresses, and phone numbers. The Genovese family, and the Russian components. It listed percentages of who got involved in the conspiracy, the number of gallons. It became a central piece of evidence. Depew got the FBI's New Jersey Regional Computer Forensic Laboratory, in Hamilton, where he is a supervisor. Chiaradio, would land him a job managing his first IT project—the FBI's Virtual Case File.

In 1999, the FBI's VCF team was an auspicious start to what would become the most highly regarded project in FBI history. The VCF was supposed to automate the FBI's paper-based work environment, allow analysts to share vital investigative information, and replace the obsolete Automated Case File (ACF). The FBI claims, the VCF's contractor, Science Applications International Corp. (SAIC), had written 100,000 lines of code so bug-ridden and functionally off target that this past April, the bureau canceled the \$105 million project, including \$105 million worth of unusable code. However, various government reports show that the FBI—lacking IT management and technical expertise—shares the blame for the project's failure.

A 2005 audit, released in 2005, Glenn A. Fine, the U.S. Department of Justice's inspector general, found that contributed to the VCF's failure. Among them: poorly defined and slowly evolving design requirements; ambitious schedules; and the lack of a plan to guide hardware purchases, network deployment, and software development for the bureau.

Years after terrorists crashed jetliners into the World Trade Center and the Pentagon, the FBI's VCF was not "connecting the dots" in time to prevent the attacks, still did not have the software to do so. The VCF's continued delays in developing a new dots that might come along. And won't for years to come.

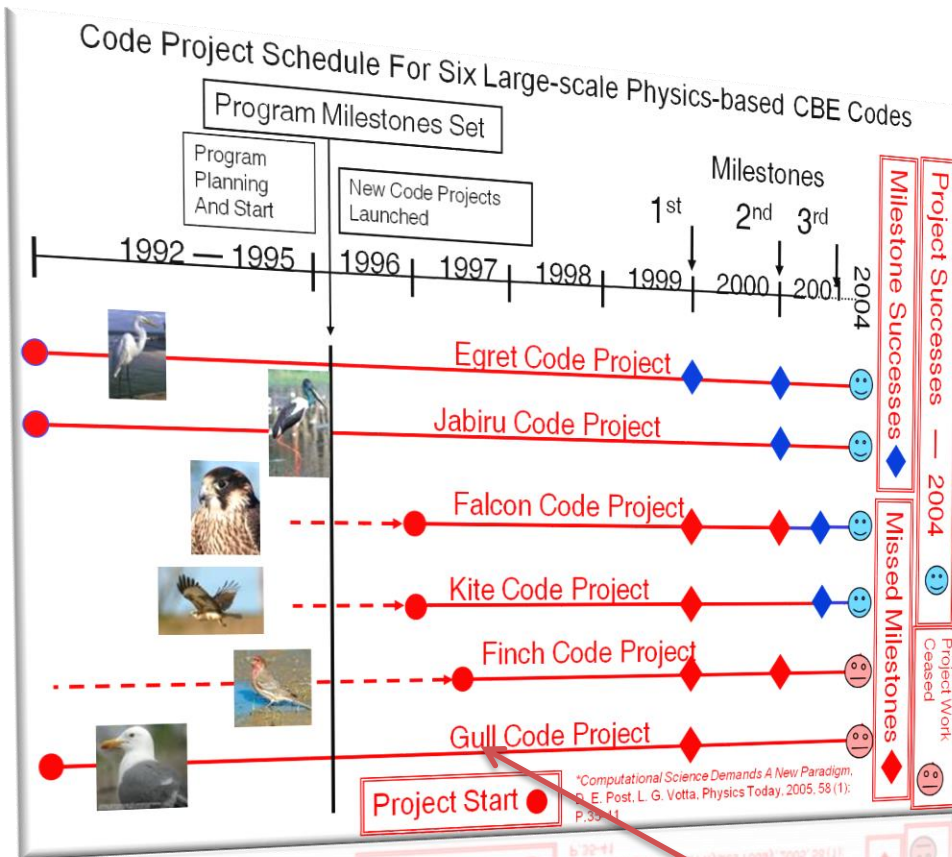
The VCF's continued delays in developing a new dots that might come along. And won't for years to come.



Gov't Software: A Legacy of Risk Management Failure!

Examples of Failure Similar to CREATE

- DOE ASCI (Multi-Physics, HPC) < 50% Success



SOFTWARE PROJECT MANAGEMENT AND QUALITY ENGINEERING PRACTICES FOR COMPLEX, COUPLED MULTIPHYSICS, MASSIVELY PARALLEL COMPUTATIONAL SIMULATIONS: LESSONS LEARNED FROM ASCI

**D. E. Post
R. P. Kendall**
LOS ALAMOS NATIONAL LABORATORY,
LOS ALAMOS, NM, USA (POST@LANL.GOV)

Abstract
Many institutions are now developing large-scale, complex, coupled multiphysics computational simulations for mission-critical applications. The simulation of the performance of nuclear weapons and certification of the performance of research in climate and weather prediction, magnetic fusion energy, environmental systems, astrochemical systems, and other areas. The successful development of these simulations is aided by attention to sound software project management and software engineering practices that the Department of Energy National Nuclear Security Agency has sponsored to develop nuclear weapons simulations over the last 50 years. We find that development practices (rather than processes) commonly employed for non-technical software and we identify those that we judge add value. Another key finding, consistent with project schedule and resource level are solely determined by the requirements once the requirements are fixed.

Key words: Software engineering, verification, validation, software project, management, computational science

Acknowledgments
The authors are grateful for discussions with and suggestions from Tom Adams, Marvin Alme, Bill Archer, Donald Burton, Gary Carlson, John Ceruti, William Chandler, Randy Christiansen, Linnea Cook, Larry Coc, Tom De...

1 Introduction
In the middle of 1996, the Department of Energy (DOE) launched the Accelerated Strategic Computing Initiative (ASCI) to develop an enhanced simulation capability for the nuclear weapons in the US stockpile. The Los Alamos National Laboratory (LANL) and Lawrence Livermore National Laboratory (LLNL) were tasked with developing this capability for the physics performance, and the Sandia National Laboratory (SNL) for the engineering performance of weapons systems. The ASCI program is now almost eight years old and now has been renamed to Advanced Simulation and Computing (ASC). It is an appropriate time to assess the progress and to develop "lessons learned" to identify what worked and what did not. This paper presents the "lessons learned" for successful code development during the ASCI project so far. The major points are summarized in Table 1.

In the absence of testing, improved nuclear weapons simulation capability is needed to sustain the US defensive capability. Following the fall of the Soviet Union and the cessation of testing nuclear weapons by both Russia and the US in the early 1990s, the US inaugurated the "Stockpile Stewardship" program to maintain its nuclear stockpile. Even though the Russian Federation poses a much reduced threat to the US compared to the Soviet Union, history, particularly the history of the twentieth century, has amply demonstrated that any nation that does not possess a strong defense based on modern military technology can - and often will - fall victim to an aggressor. The US and Russia have been in the process of reducing their stockpiles from the level of tens of thousands of warheads needed to counter a "first strike" to the US reduced stockpile for the foreseeable future. The existing stockpile consists of weapons systems highly optimized for specific missions and for the maximum year half life to weight ratio. They were designed for a 15-30 year shelf life with little consideration given to possible longer-term aging issues. The weapons program now has the challenge of adapting the existing warheads for different missions, and extending their lifetimes to 40 to 60 years without the ability to test the nuclear performance. The strategy developed for "Stockpile Stewardship" has four major elements:

CREATE-Scale Project Cancelled

CREATE Core Risks

10 Core Risks Identified in 2008

- 1. Creating and inventing new, innovative software technologies**
within the existing DoD program and project management structure.
- 2. Loss of credibility due to defects**
or insufficiently accurate models in the software that result in inaccurate results.
- 3. Building and managing software development teams**
that are embedded in, and part of, the DoD customer organizations.
- 4. Significant losses of core development staff**
and their corporate knowledge, due to severe funding reductions and other institutional turmoil.
- 5. Program coordination within the diverse management cultures**
especially security management—within different DoD organizations.
- 6. Requirements creep and relevancy**
over the project's major development phases.
- 7. Rapidly changing computational and computer technologies**
especially rapidly changing computer architectures and environments.
- 8. Loss of DoD stakeholder and sponsor support**
due to frequent turnover of senior DoD personnel.
- 9. Loss of control of intellectual property rights**
In the absence of domestic copyright protection.
- 10. Supporting CREATE software users without impacting development.**

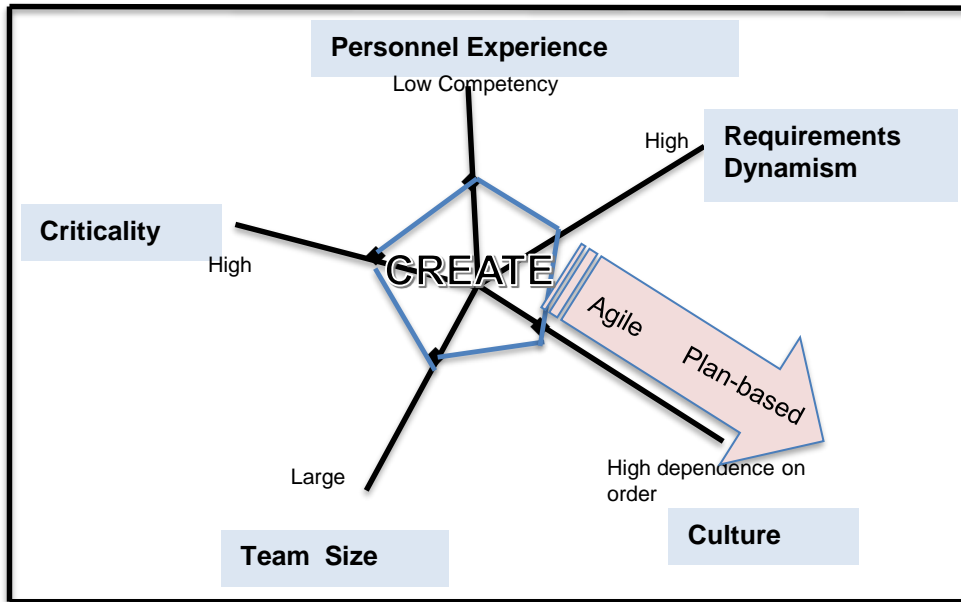
CREATE Risk Management Principles

Addressing the Core Risks

- Develop a compelling, credible vision and endeavor to communicate it.
- **Develop a long-term strategic plan and define the essential processes required to execute it.**
- Recruit the right team leaders and strong, multidisciplinary teams.
- **Balance the need for development team empowerment with the need for accountability.**
- Recognize that program management must extend to the risks most outside its control: stable funding, stakeholder support and deployment to customers.
- **Protect the development effort from institutional turmoil.**
- Implement a rigorous verification and validation program.

The CREATE Approach: Principles to Practices to Mitigate Risk

Development Environment Indicators



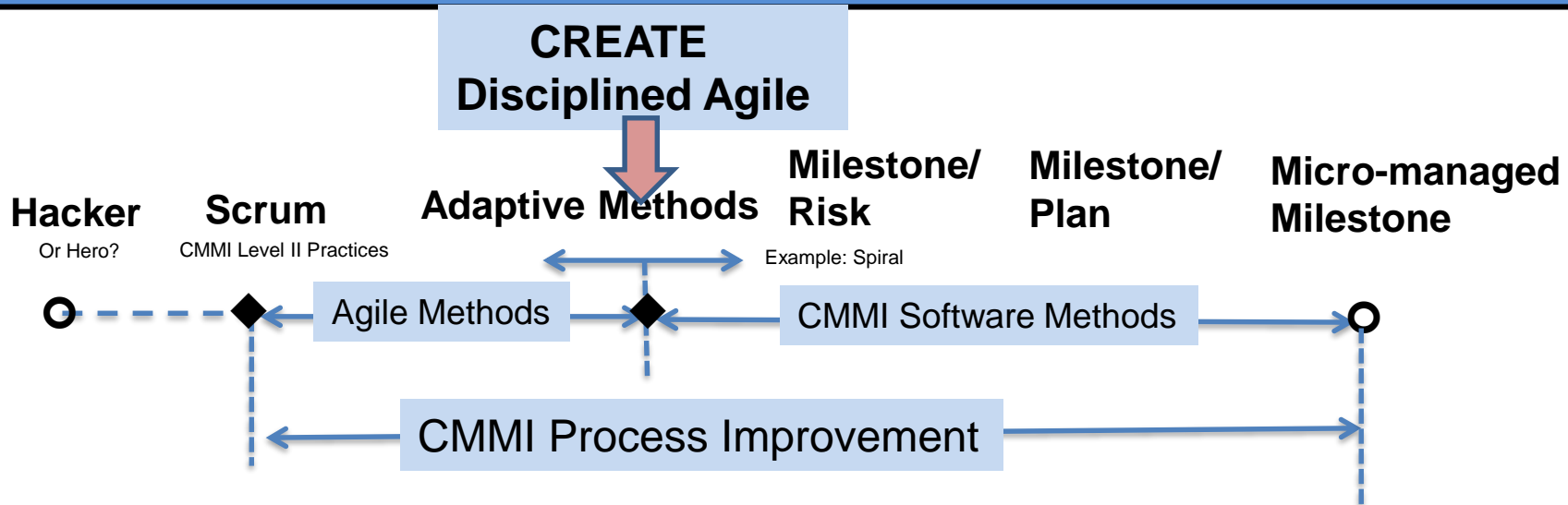
Notional Home Ground Chart for CREATE

after Boehm, Using Risk to Balance Agile and Plan-Driven Methods, IEEE Computer Society, 2003

“Principles” translated into shared “Practices”, as opposed to “Processes”, best fit the need for flexibility for CREATE operating within the three Armed Services

Risk 1: Challenge of developing new, innovative software within the DoD Program Management structure

- Mitigating Practice: Strive for flexible execution with risk-mitigating milestones



after Boehm, "Getting Ready for Agile Methods with Care", IEEE Software, 2002

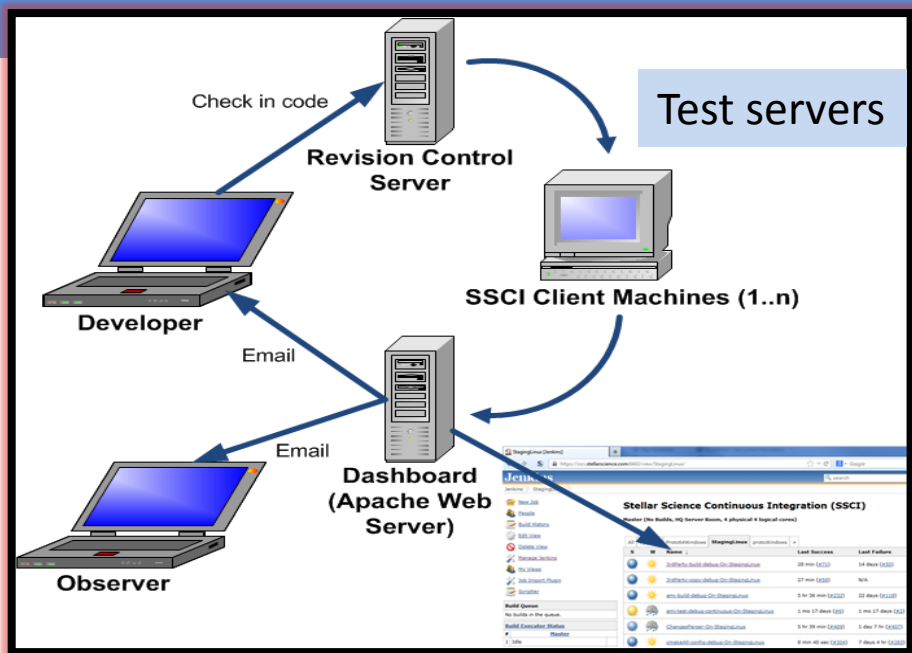
CREATE Development Approach: A Disciplined Agile Workflow Management Approach based on Scrum

Risk 2: Loss of credibility

due to software defects or inaccuracies

Mitigating Practice: *Implement a testing program compliant with National Research Council Guidelines; strive for continuous integration with automated regression tests for each commit, and test coverage measurements*

Regression testing after every commit →



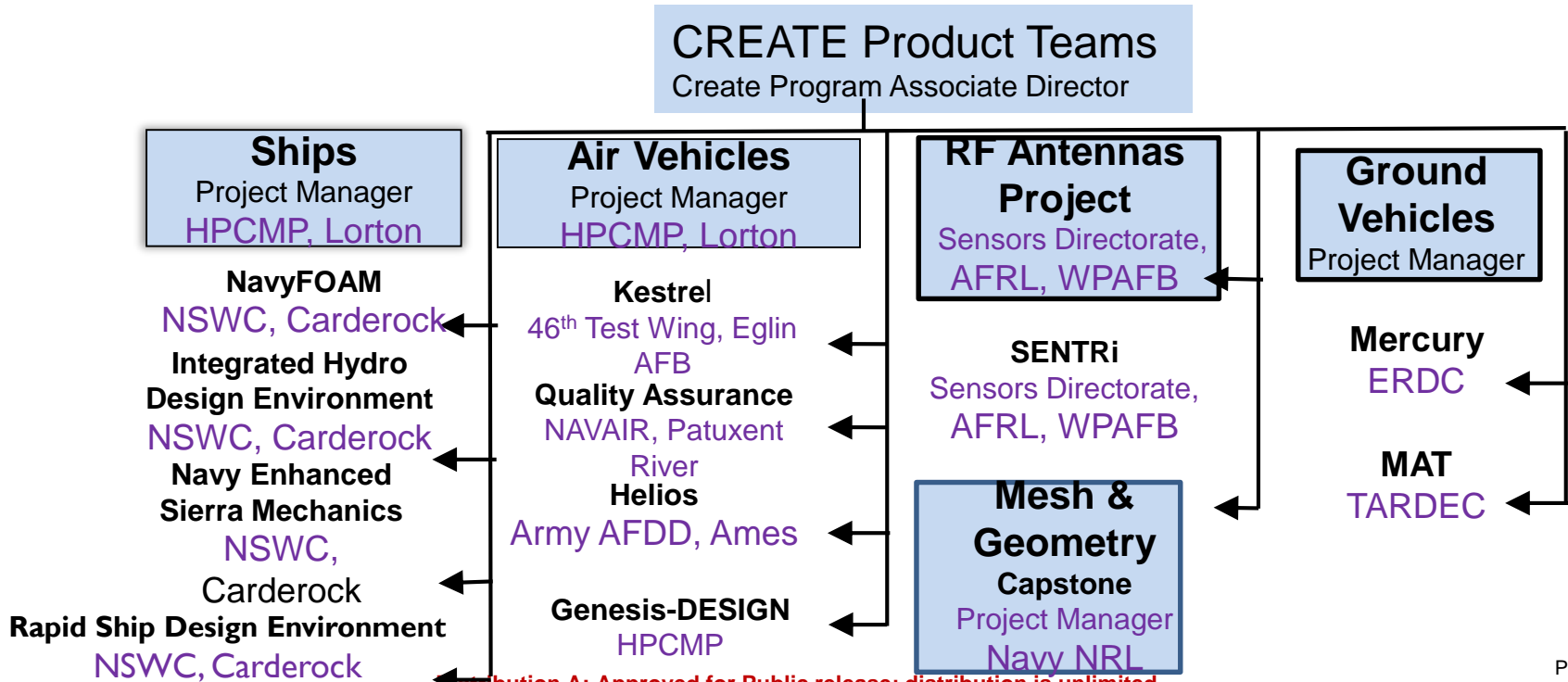
CREATE-RF Continuous Integration Platform

Discover problems before they are hard to fix

Risk 3: Difficulty building software teams

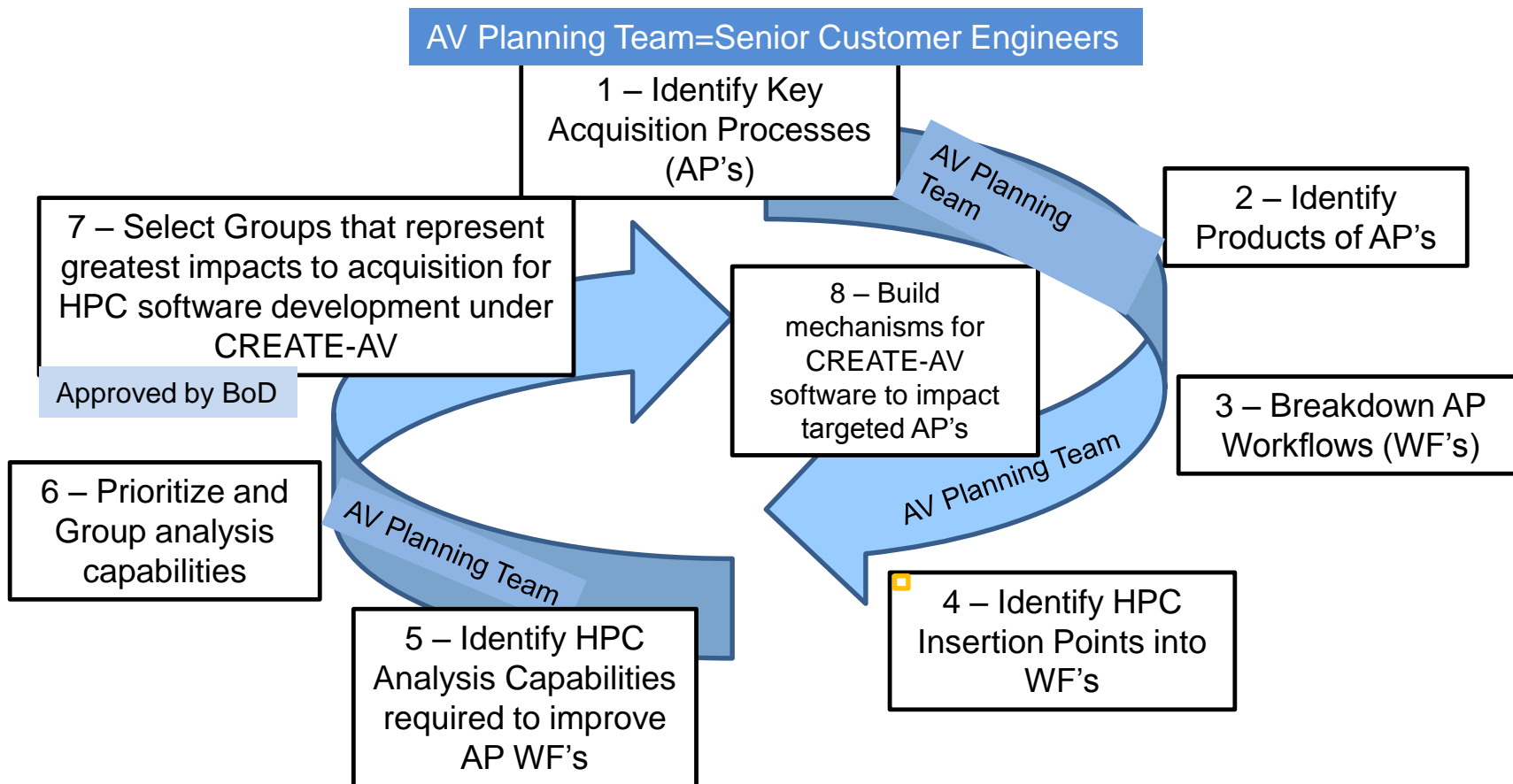
under DoD constraints

- Mitigating Practice: *Identify a principal developer within customer organizations (in CREATE's case, the Services)*
- Mitigating Practice: *Recruit lean (5 -15 member) development teams lead by technical experts (typically from the DoD S&T community)*



Risk 4. Funding Reductions

- Mitigating Practice: *Reach out to the customer with Pilot Projects that demonstrate value*

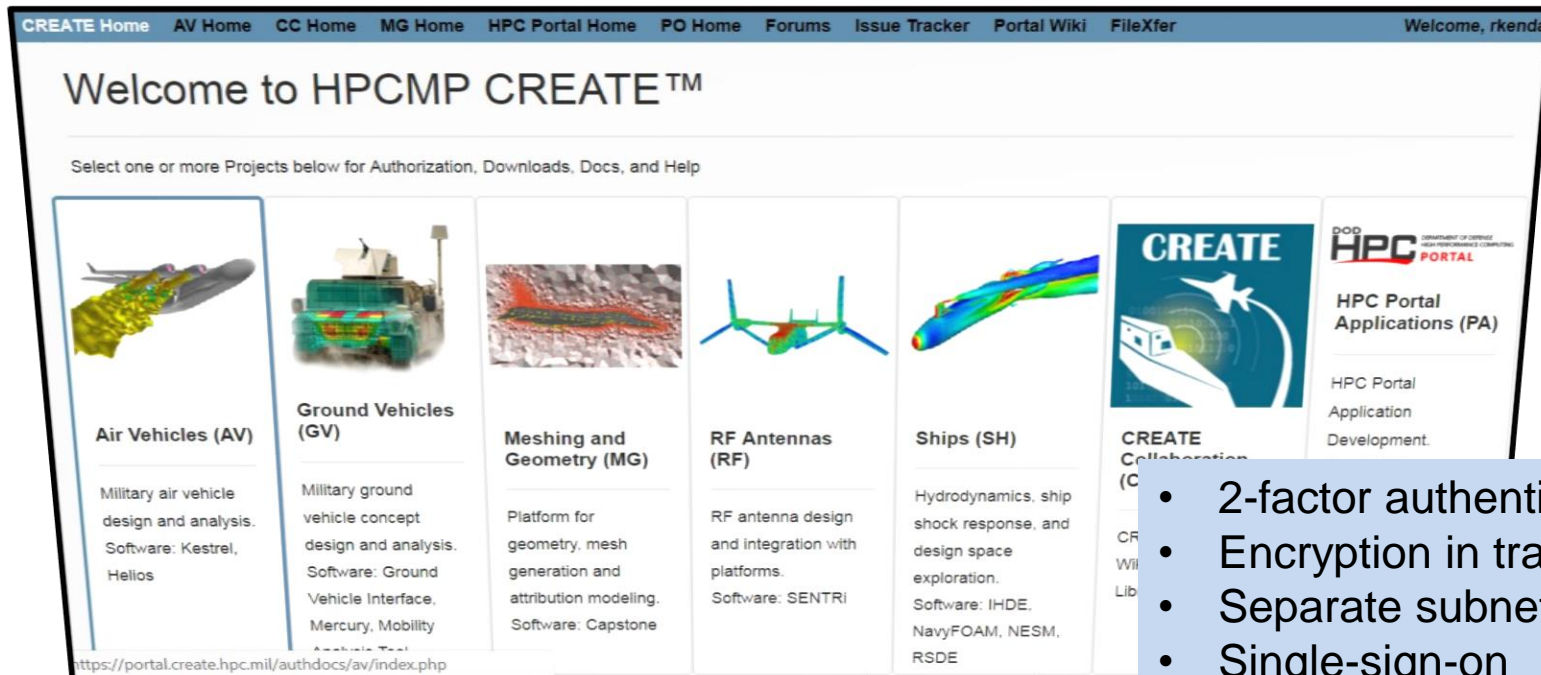


This helps demonstrate value and promotes customer commitment

Risk 5: Difficult program coordination

in an environment of diverse management cultures—especially security-related

- Mitigating Practice: *Establish browser access to CREATE software and support*



The screenshot shows the HPCMP CREATE portal with a navigation bar at the top containing links like 'CREATE Home', 'AV Home', 'CC Home', 'MG Home', 'HPC Portal Home', 'PO Home', 'Forums', 'Issue Tracker', 'Portal Wiki', and 'FileXfer'. The main content area is titled 'Welcome to HPCMP CREATE™' and includes a sub-header 'Select one or more Projects below for Authorization, Downloads, Docs, and Help'. Below this, there are several project category cards, each with an image and a brief description. The 'Air Vehicles (AV)' card is highlighted with a blue border. To the right of the main content area, there is a sidebar with the 'CREATE' logo and 'HPC Portal Applications (PA)' section, which includes links for 'HPC Portal Application Development'.

- 2-factor authentication
- Encryption in transit and at rest
- Separate subnet
- Single-sign-on

Secure access without downloading software

Risk 6: Requirements creep and product relevancy

Mitigating Practice. Express requirements as use-cases in language that customers and developers both understand.

CREATE-Capstone Foundational¹ Capability Requirements

ID	Description
MG-00	Import Externally Generated Geometry (CAD, ...)
MG-01	Create Parameterized Geometry
MG-02	Support Dependency-Based Associative Mod...
MG-03	Repair Externally Generated (eg CAD) Geome...
MG-04	Support De-featuring and Idealization of Geor...
MG-05	Provide Robust Surface Meshing Algorithms
MG-06	Provide Robust Volume Meshing Algorithms
MG-07	Provide Geometry-based Mesh Generation an...
MG-08	Support Multi-scale Models
MG-09	Support Legacy Component Integration
MG-10	Support Analysis Model Attribution
MG-11	Provide Accurate and Scalable Runtime Geom...
MG-12	Core Framework (Internal requirements to supp... above)

MG-06 Use-Cases

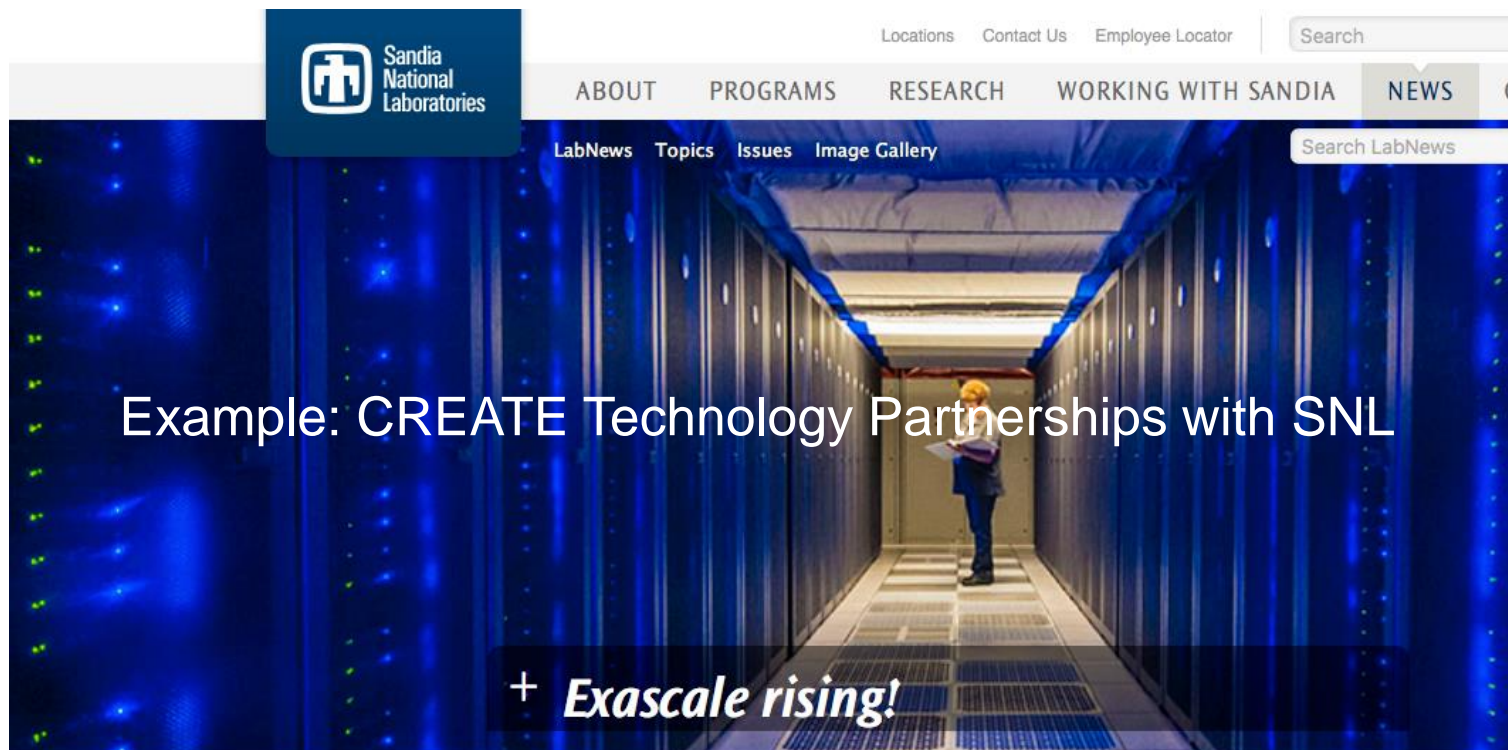
MG-06-UC-01	Unstructured all-tetrahedral volume meshing
MG-06-UC-02	Unstructured hexahedral-dominated hybrid meshing
MG-06-UC-03	Boundary Layer meshing with triangular wedge elements in the viscous region transitioning to tet. No interference from other BL
MG-06-UC-04	MG07-UC04 with complex geometries and multiple intersecting boundary-layers
MG-06-UC-05	Boundary layer meshing with hex,prism in the viscous regin transitioning to hex/tet
MG-06-UC-06	MG06-UC05 with complex geometries & multiple intersections
MG-06-UC-07	Volume mesh handing for high order element (first approach)
MG-06-UC-08	Matching volume meshes for periodic boundary condition
MG-06-UC-09	Exterior volume meshing up to a given truncation boundary
MG-06-UC-10	Support for 'strand-meshing' paradigm
MG-06-UC-11	Support for moving parts
MG-06-UC-12	Support for 'strand-meshing' paradigm

The focus is on shared understanding of requirements

¹ Established in 2008

Risk 7: Anticipating and responding to rapidly changing HPC environments

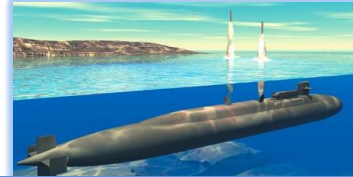
Mitigating Practice: *Ensure that the CREATE program maintains an awareness of evolving state of the art in high performance computing*



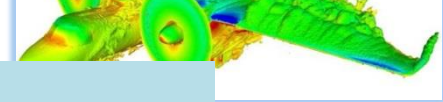
BY NEAL SINGER | PHOTOGRAPHY BY RANDY MONTOYA

Risk 8: Loss of sponsor support

due to frequent turnover of senior DoD personnel

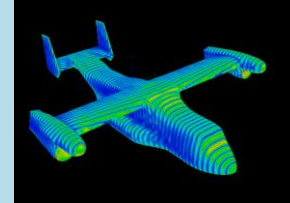


• Mitigating Practice: *Continually reach out to new senior- and middle-level members of the DoD acquisition engineering community.*

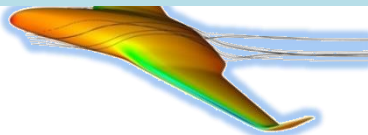


Examples of Outreach:

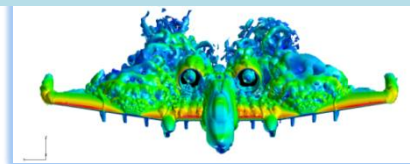
- 3 BAAs or CRADAs
- 60+ CREATE Pilot Projects
- Dozens of training courses
- 100's of technical articles(45+ in 2016 alone)



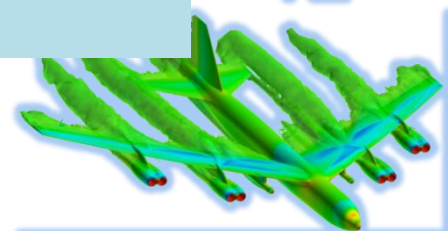
F-15 SA/DB-110



Strategic Airlift CP&A



A-10



V-22

B-52

Risk 9: Loss of control of IP rights

*HPCMP CREATE™ Software
User Agreement*

Authorized to U.S. Government agencies and their contractors in support of a current contract or technology transfer agreement with the U.S. Government

Distribution Control Number: 1313674496

Warning – This document refers to technical data, the export of which is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

1. Introduction

- a. This Software User Agreement is made by and between the Department of Defense as represented by the High Performance Computing Modernization Program (hereinafter, "HPCMP") and the undersigned Software User Agreement Recipient

• Mitigating Practice: *Require a standard software distribution agreement (a license for use).*

Recipient has no right to receive, use or examine any source code or design documentation relating to the Product, except as specifically authorized by approved collaborative development and source code agreements. HPCMP retains all right, title and interest in the Product and any portion thereof and in all copies, modifications and derivative works of the Product and portions thereof including, without limitation, all rights the Government may have to patent, copyright, trade secret, trademark and other proprietary or intellectual property rights. Recipient has no rights, by license or otherwise, to use, disclose or disseminate the Product, in whole or in part, except as otherwise expressly provided herein. Recipient may not use any name, mark or designation of the Product except for the express purposes in this Software User Agreement.

- c. Unless otherwise permitted by the HPCMP, Recipient shall utilize the Product exclusively to support United States Government programs. Recipient agrees that it shall not provide or allow access to this material to persons other than its employees or persons acting on its behalf in support of U.S. Government programs, without permission of the HPCMP.

2. Rights of Use

Rights to use this Product are granted under this Software User Agreement only for the intended use as determined by the HPCMP, and as documented in the Purpose section of this Software User Agreement. Requests for other uses must be submitted in writing to the HPCMP. The HPCMP has the sole right to approve such requests, and will do so in writing.

3. Restrictions

- a. The Recipient shall not re-distribute, sell, or use the Product for any purposes not approved the HPCMP, in whole or in part. The Recipient may produce copies of the Product or portions of the Product for use solely by the Recipient, or for use by a U.S. contractor/sub-contractor organization authorized in writing by HPCMP. Recipient shall require each authorized U.S. contractor/subcontractor organization receiving a copy of the Product or portion of the Product to execute and enforce the terms and conditions of this Software User Agreement, and limit use of the Product to the specific purpose stated within this Software User Agreement. A copy of the authorized copy of the Product or portion of the Product shall be provided to the HPCMP for its review and approval. Recipient shall be responsible for compliance with the terms and conditions of this Software User Agreement.

b. The HPCMP may change the terms and conditions of this Software User Agreement at any time without notice to the Recipient.

- c. The Recipient bears full responsibility for the control of the Product and any controlled material in or related to the Product. The Product is subject to the Arms Export Control Act of 1979, as amended, Title 50, U.S.C., App. 2401, et seq. Violations of these export laws are subject to severe criminal penalties.

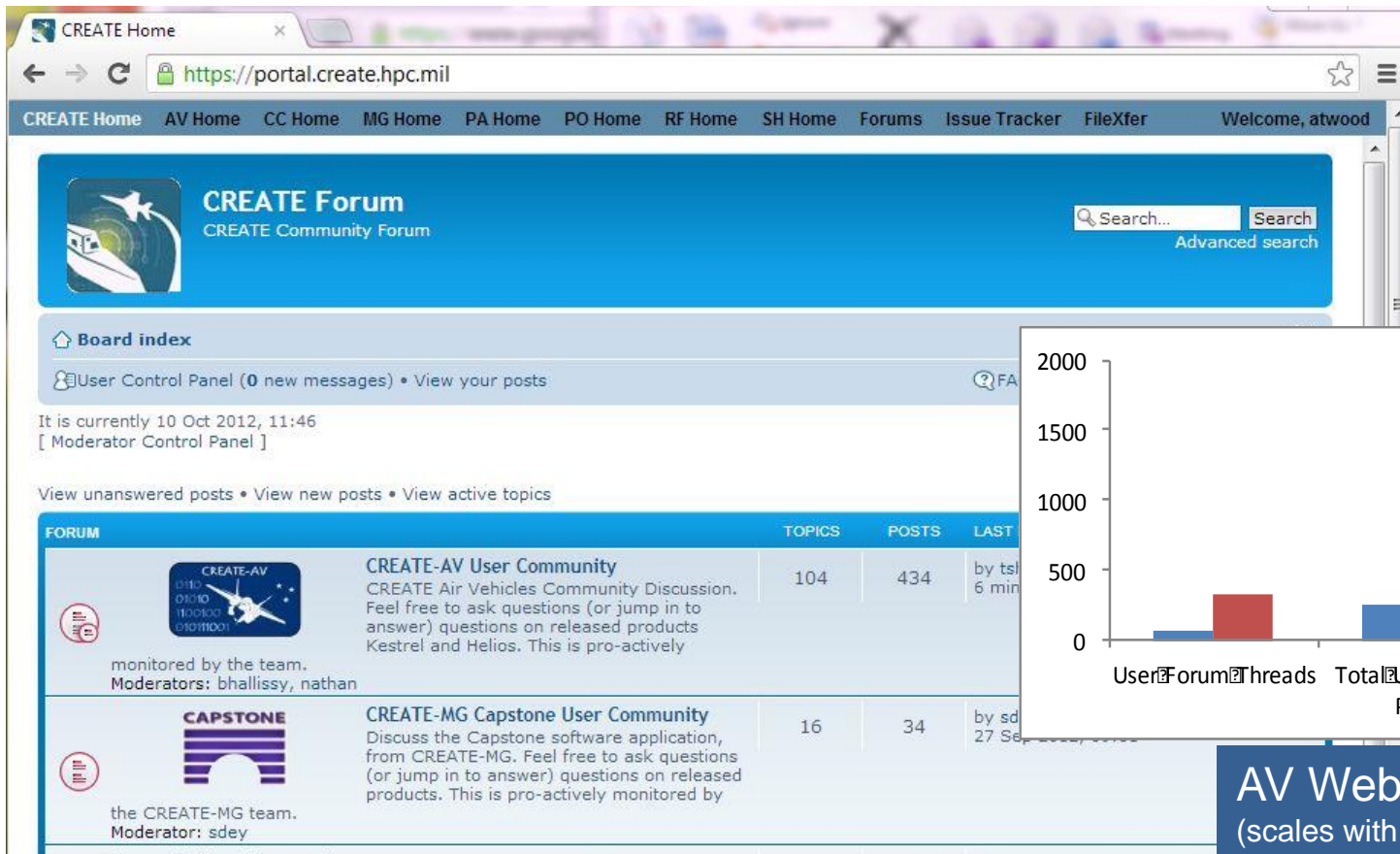
- d. The Recipient acknowledges that the Product may be controlled by the International Traffic In Arms Regulation (ITAR), 22 CFR Sections 121 through 128, and may require an export distribution agreement before assigning any FOREIGN NATIONAL or FOREIGN REPRESENTATIVE to perform work using the Product or before granting any FOREIGN NATIONAL or FOREIGN REPRESENTATIVE access to the Product, and/or technical data generated by the Product. Furthermore, such persons must be approved by the HQUSACE designated Foreign Disclosure Officer before beginning such work.

• Practice: *Acquire the necessary rights (DFARs) in contracts and licenses.*

Risk 10: Supporting CREATE users

without impacting product development

- Mitigating Practice: *Look for scalable self-help solutions, like Web Forums*



CREATE Home AV Home CC Home MG Home PA Home PO Home RF Home SH Home Forums Issue Tracker FileXfer Welcome, atwood

CREATE Forum
CREATE Community Forum



Search... Search
Advanced search

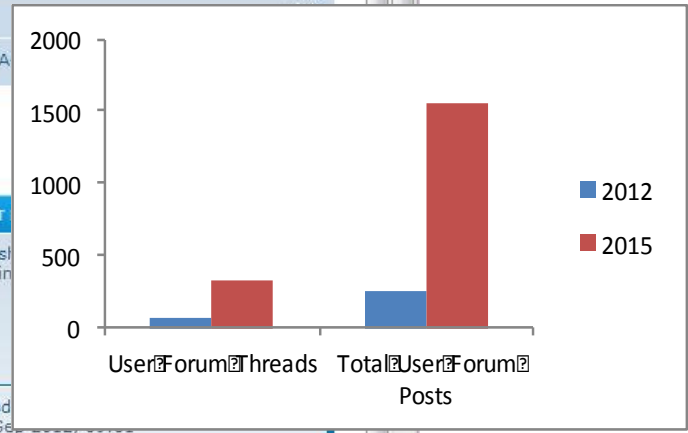
Board index

User Control Panel (0 new messages) • View your posts

It is currently 10 Oct 2012, 11:46
[Moderator Control Panel]

View unanswered posts • View new posts • View active topics

FORUM	TOPICS	POSTS	LAST
 CREATE-AV User Community CREATE Air Vehicles Community Discussion. Feel free to ask questions (or jump in to answer) questions on released products Kestrel and Helios. This is pro-actively monitored by the team. Moderators: bhallissy, nathan	104	434	by tsl 6 min
 CREATE-MG Capstone User Community Discuss the Capstone software application, from CREATE-MG. Feel free to ask questions (or jump in to answer) questions on released products. This is pro-actively monitored by the CREATE-MG team. Moderator: sdey	16	34	by sd 27 Se



AV Web Forum Use
(scales with the user base)

CREATE Program Management

What has made it work?

- Leadership beyond program management
- Balance between developer freedom and responsibility
- Embedded in CREATE's primary customer organizations
- Customer-defined use-cases
- Frequent product releases
- Browser-based access and Customer Forums

Richard P. Kendall, Ph.D.

Software Engineering Consultant

DoD High Performance Computing Modernization Program

(505) 660-0976

Richard.p.kendall4.ctr@mail.mil