# 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

DOD HPC MODERNIZATION PROGRAM

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

# 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**

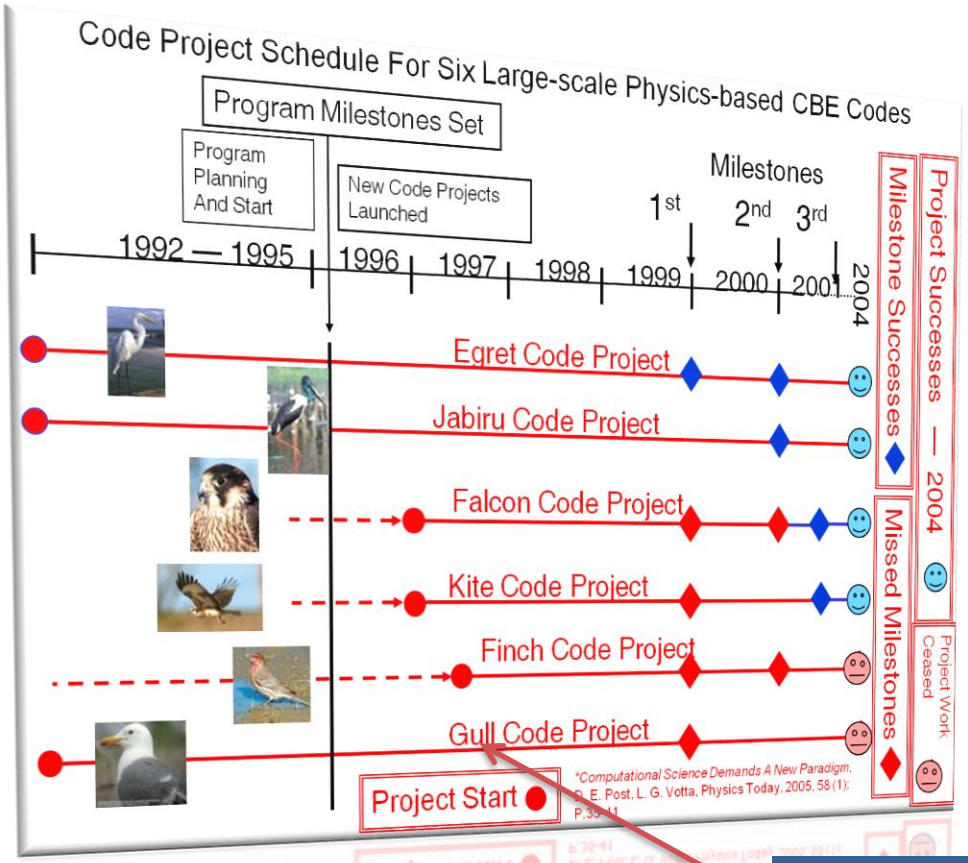
# Program Management in CREATE

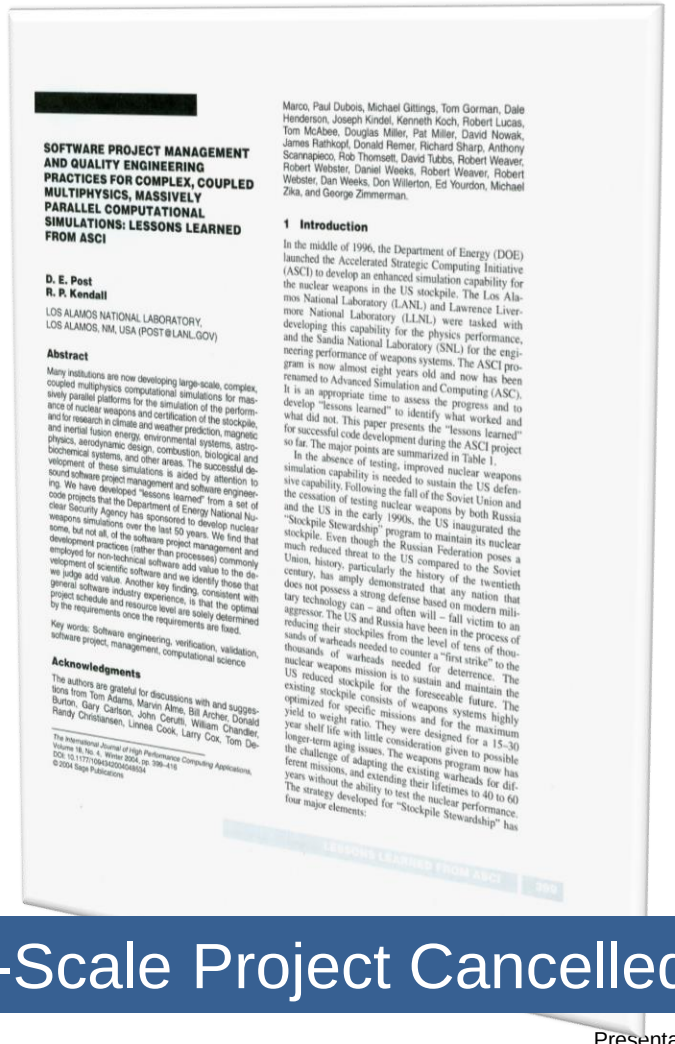
**Why should you have confidence in the staying power of CREATE?**

# Start by Recognizing that Software Development is a Risky Enterprise

# 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 massively parallel platforms for the simulation of the performance of nuclear weapons and certification of the stockpile, and for research in climate and weather prediction, magnetic and inertial fusion energy, environmental systems, astrophysics, aerodynamic design, combustion, biological and biochemical systems, and other areas. The successful development of these simulations is aided by attention to sound software project management and software engineering. We have developed "lessons learned" from a set of code projects that the Department of Energy National Nuclear Security Agency has sponsored to develop nuclear weapons simulations over the last 50 years. We find that some, but not all, of the software project management and development practices (rather than processes) commonly employed for non-technical software add value to the development of scientific software and we identify those that we judge add value. Another key finding, consistent with general software industry experience, is that the optimal 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 Cerutti, William Chandler, Randy Christiansen, Linnea Cook, Larry Cox, Tom DeMarco, Paul Dubois, Michael Gittings, Tom Gorman, Dale Henderson, Joseph Kindel, Kenneth Koch, Robert Lucas, Tom McAbee, Douglas Miller, Pat Miller, David Nowak, James Rathkopf, Donald Remer, Richard Sharp, Anthony Scannapieco, Rob Thomsett, David Tubbs, Robert Weaver, Robert Webster, Daniel Weeks, Robert Weaver, Robert Webster, Dan Weeks, Don Willerton, Ed Yourdon, Michael Zika, and George Zimmerman.

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 thousands of warheads needed for deterrence. The US reduced stockpile for the foreseeable future. The nuclear weapons mission is to sustain and maintain the existing stockpile consists of weapons systems highly optimized for specific missions and for the maximum yield 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:

The International Journal of High Performance Computing Applications, Volume 18, No. 4, Winter 2004, pp. 399–416
DOI: 10.1177/1094342004048534
©2004 Sage Publications

**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.

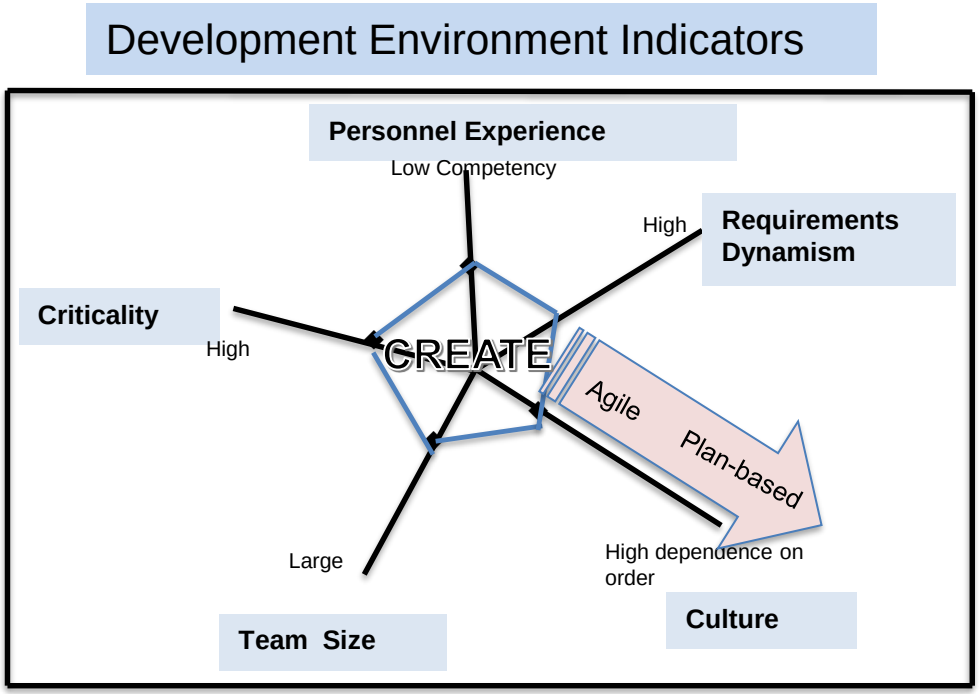
**10.Supporting CREATE software users without impacting development.**

# 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



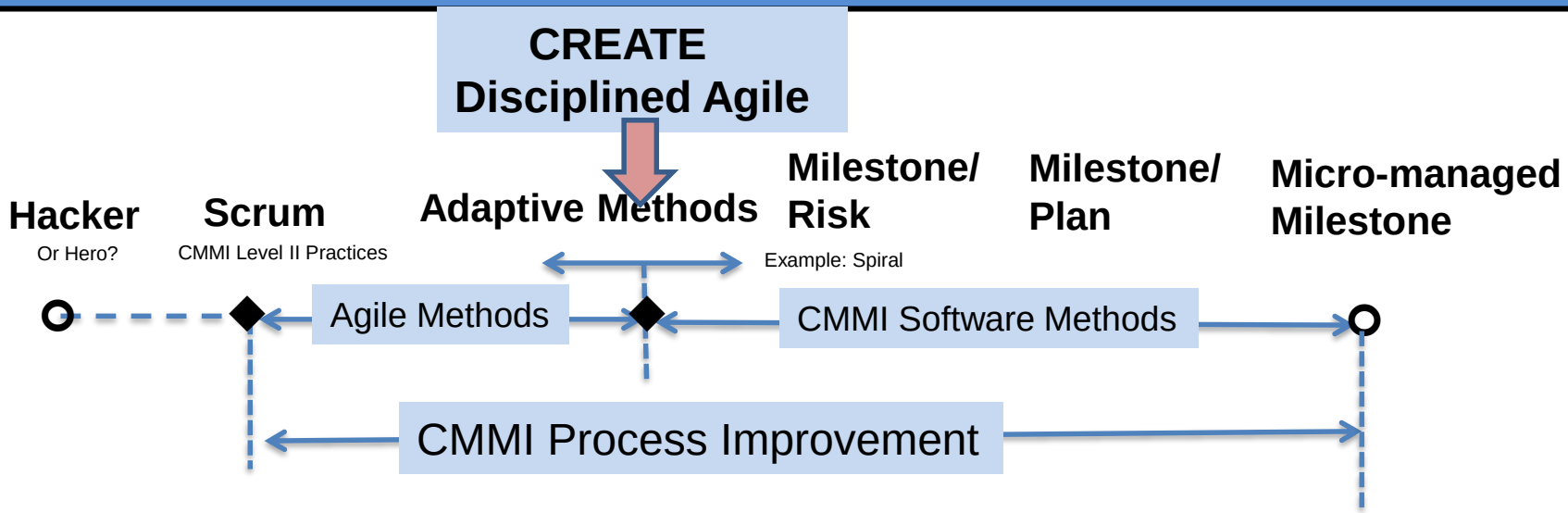

**Notional Home Ground Chart for CREATE**

*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

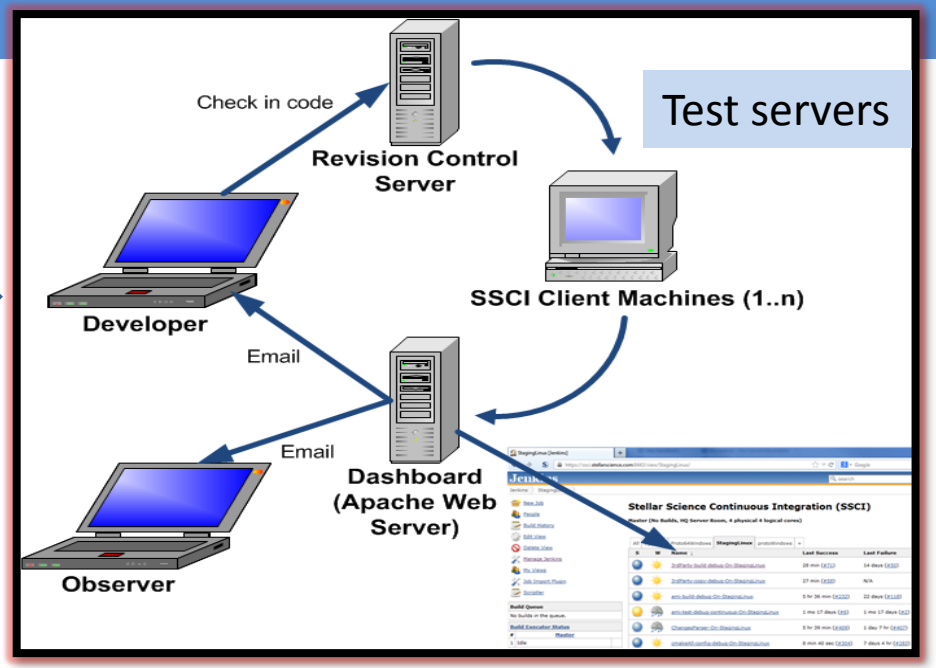
CREATE Development Approach: A Disciplined Agile Workflow Management Approach based on Scrum

# 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



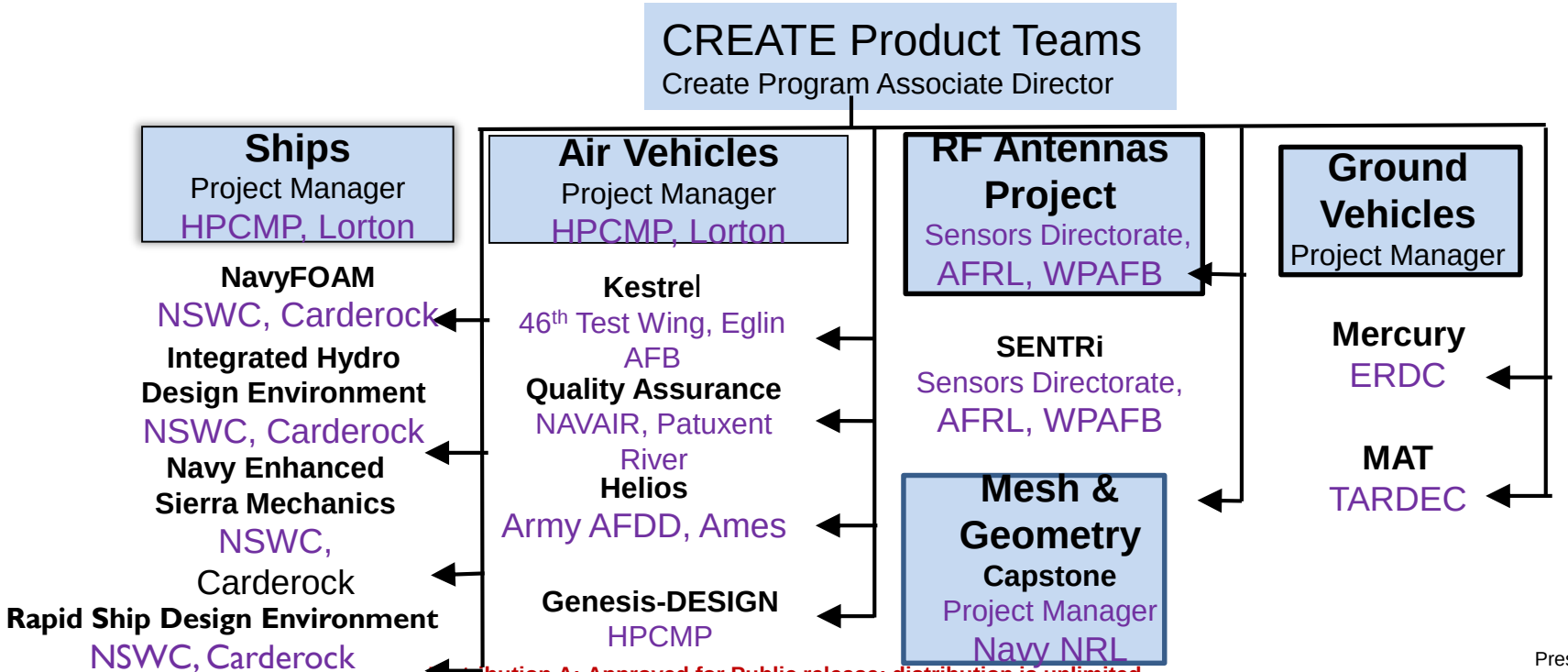

**CREATE-RF Continuous Integration Platform**

Discover problems before they are hard to fix

# Risk 3: Difficulty building software teams

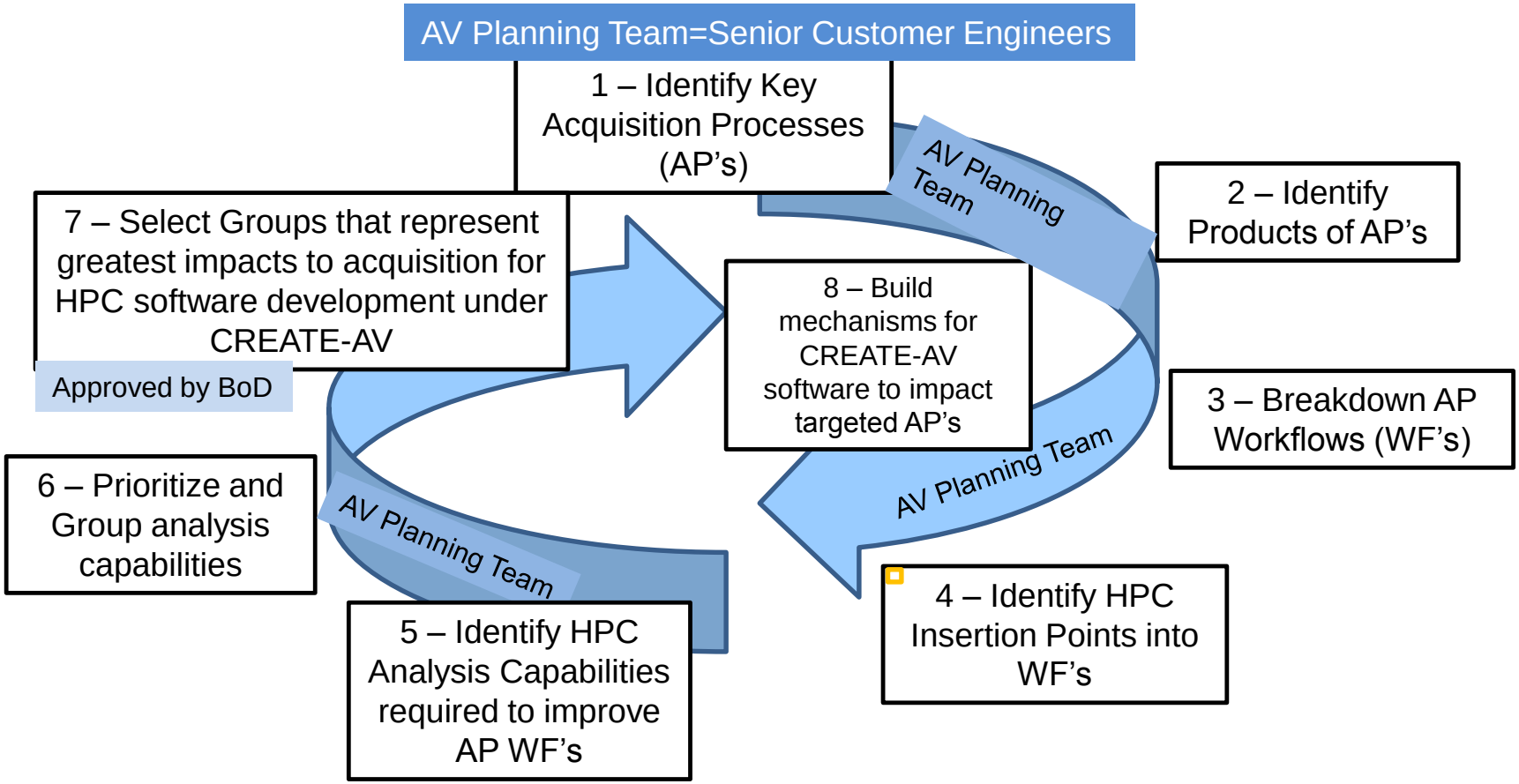
**under DoD constraints**

- 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***

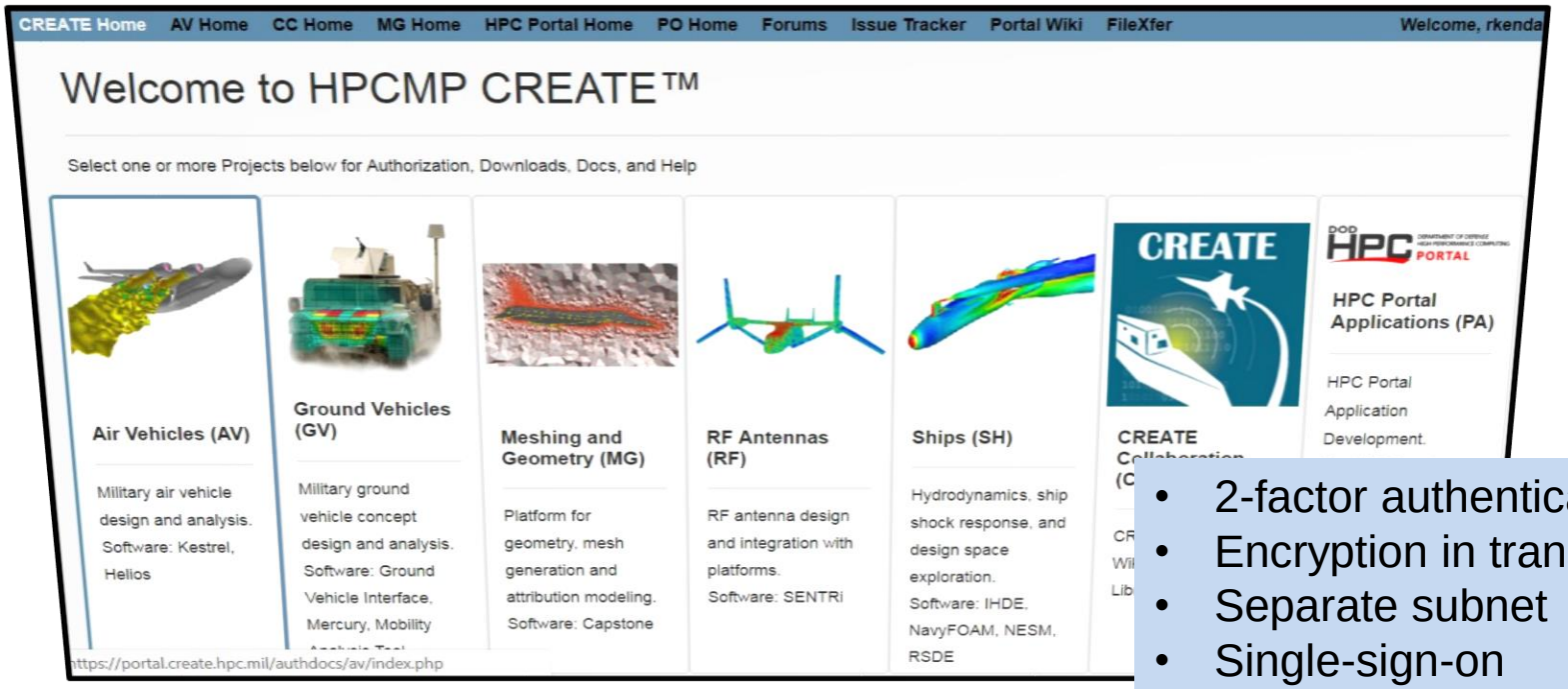



This helps demonstrate value and promotes customer commitment

# 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*




- 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 Foundational[1] 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

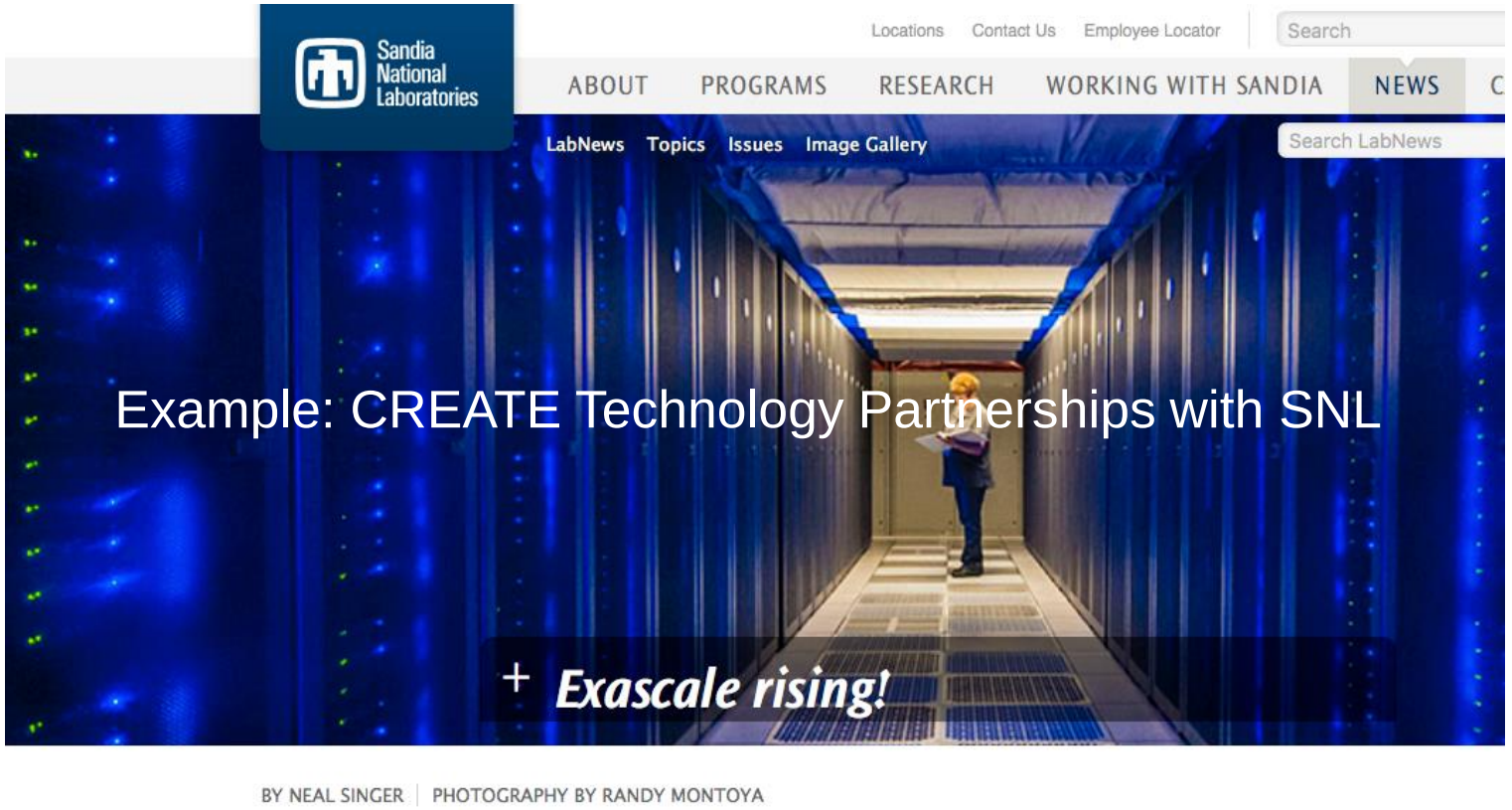
| | |
|---|---|
| MG-06-UC-01 | Unstructured all-tetrahedral volume meshing |
| MG-06-UC-02 | Unstructured hexahedral-dominated hybrid meshing |
| MG-06-UC-03 | Boundary Layer meshing with triangular wedge elements in the viscous region transitioning to tet. No interference from other BL |
| MG-06-UC-04 | 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 |
| | sources |
| | 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*

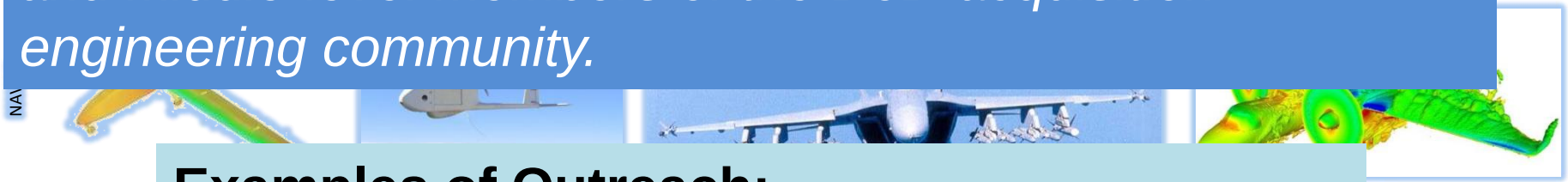



Example: CREATE Technology Partnerships with SNL

# Risk 8: Loss of sponsor support

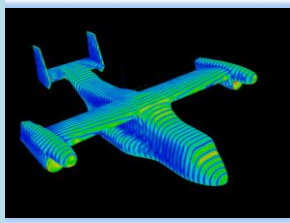
**due to frequent turnover of senior DoD personnel**


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

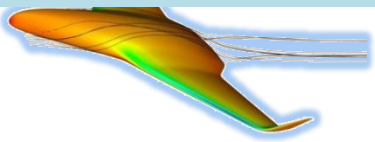


**Examples of Outreach:**

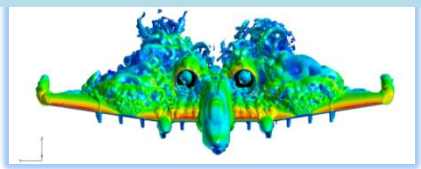
- 3 BAAs or CRADAs
- 60+ CREATE Pilot Projects
- Dozens of training courses
- 100's of technical articles( 45+ in 2016 alone)

F-15 SA/DB-110

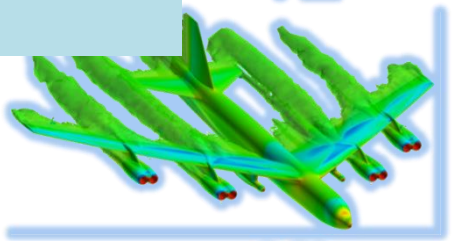


Strategic Airlift CP&A



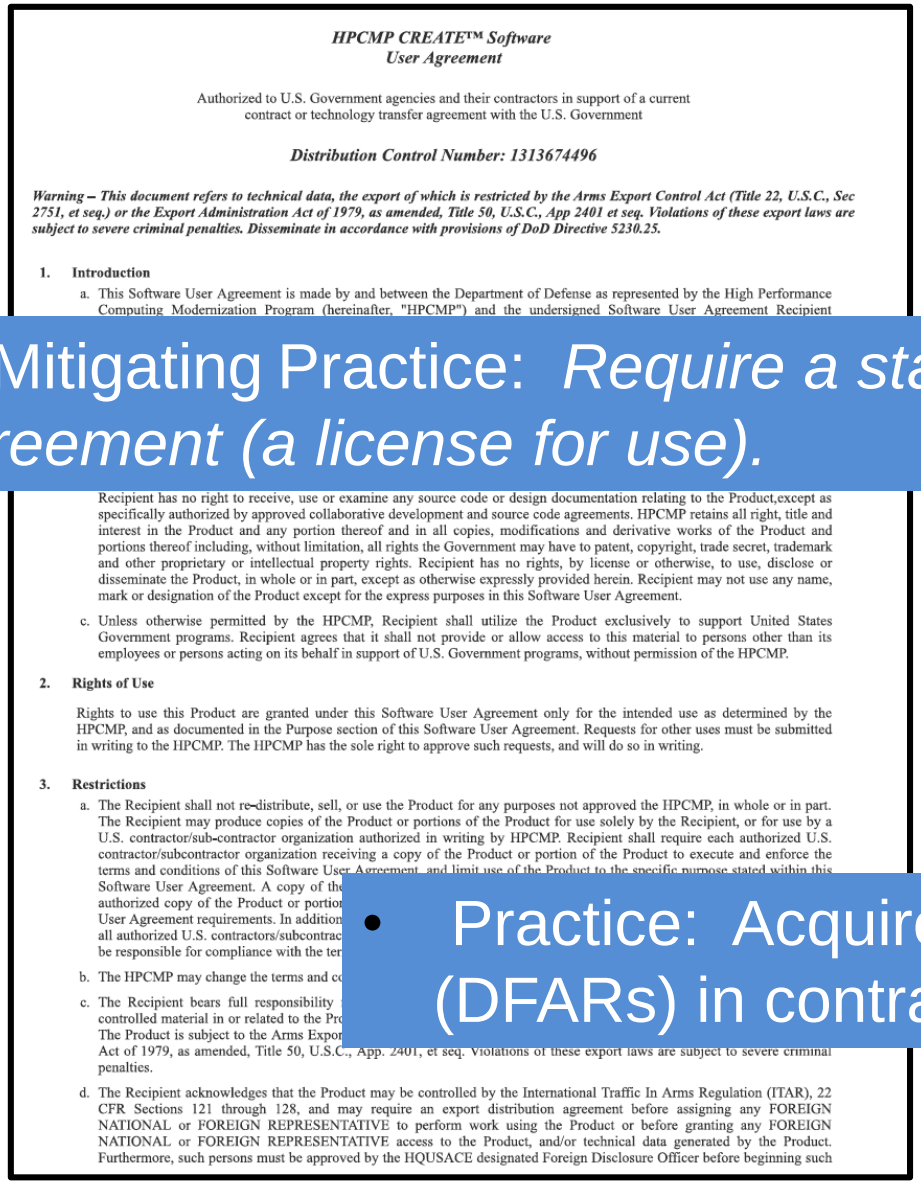
A-10

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

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 th
authorized copy of the Product or portio
User Agreement requirements. In addition
all authorized U.S. contractors/subcontrac
be responsible for compliance with the ter

b. The HPCMP may change the terms and c

c. The Recipient bears full responsibility
controlled material in or related to the Pr
The Product is subject to the Arms Expor
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

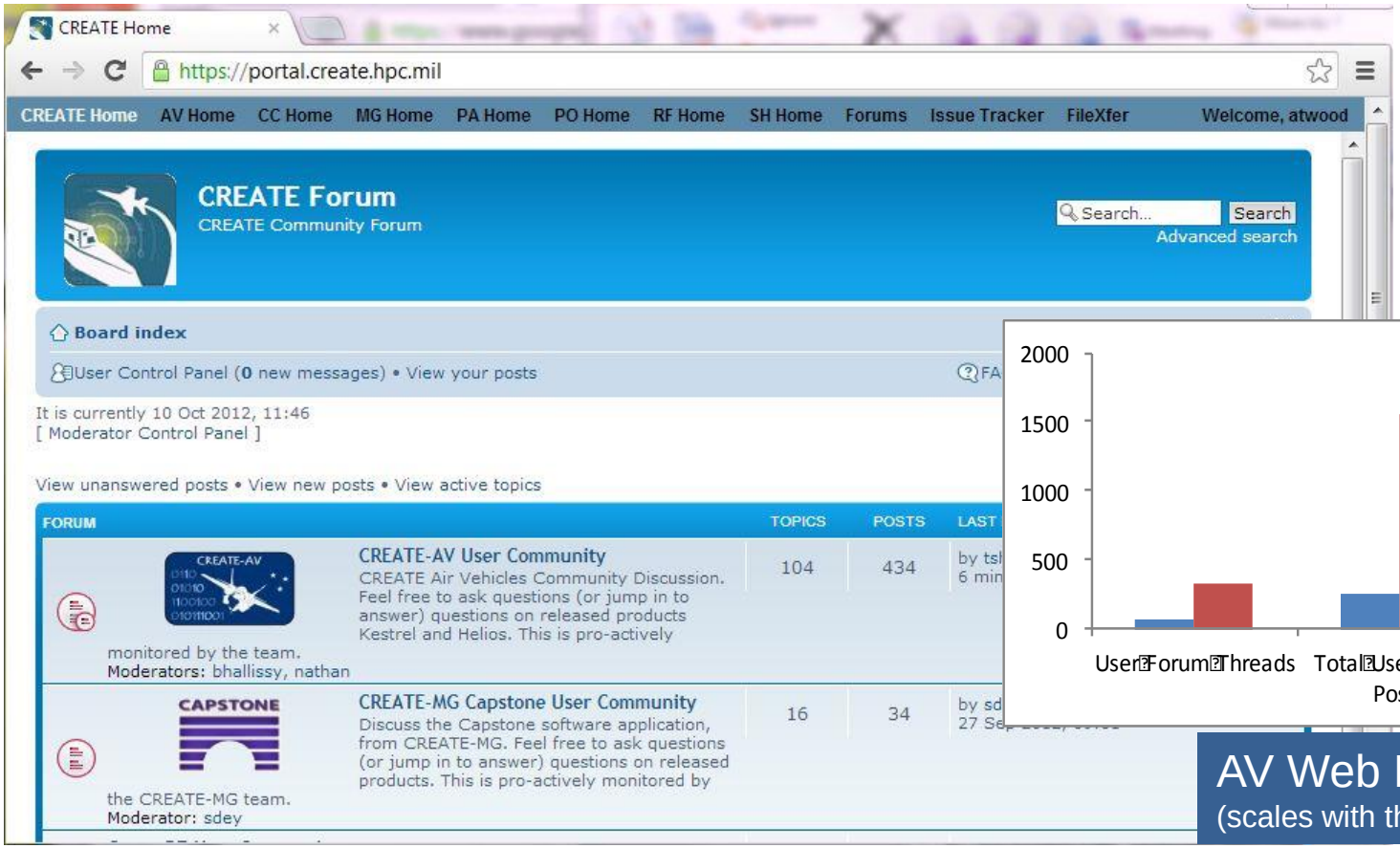
- Mitigating Practice: *Require a standard software distribution agreement (a license for use).*

- 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*




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

# NDIA #19693


## Richard P. Kendall, Ph.D.

Software Engineering Consultant
DoD High Performance Computing Modernization Program
(505) 660-0976
Richard.p.kendall4.ctr@mail.mil