

ICCRTS 2014

Agile and Adaptive IT Ecosystem, Results, Outlook , and Recommendations (paper 011, track 4)

Harvey Reed (MITRE)

John "Nano" Nankervis (Joint Staff J6)

LtCol Jordon Cochran (OUSD / AT&L)






Rajeev Parekh, US BICES Chief Engineer, (MITRE)

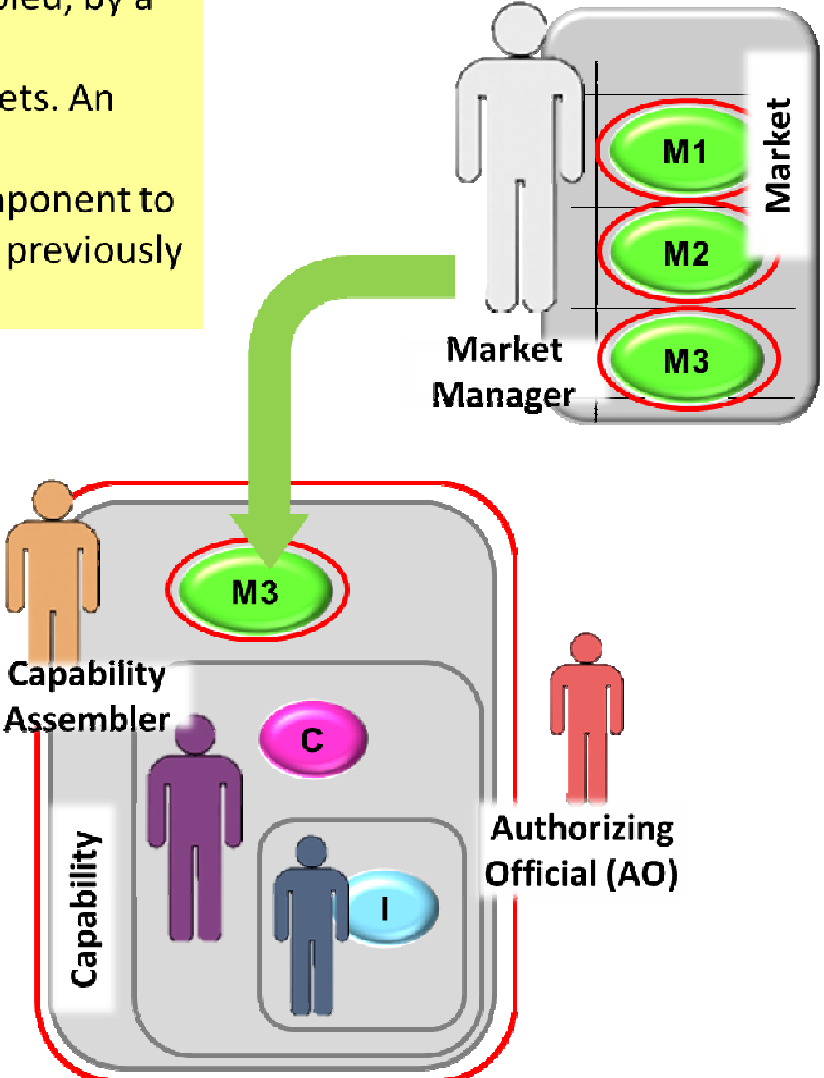
Fred Stein, Col. U.S. Army (ret) (MITRE)

Vision: Assemble IT Capabilities

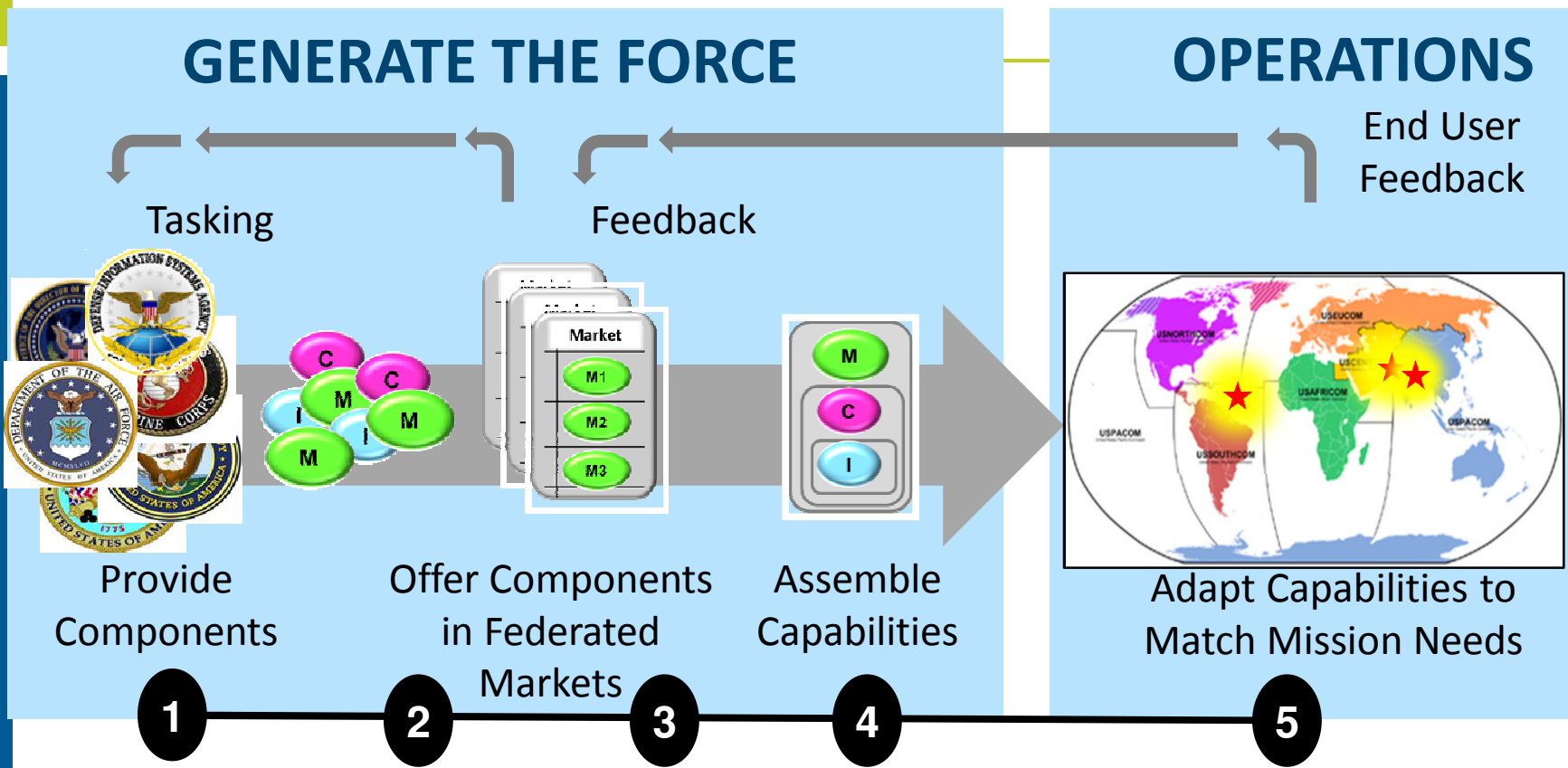
IT Capabilities can be assembled, by a Capability Assembler, from components offered in Markets. An Authorizing Official uses the assessment of a mission component to authorize it for inclusion in a previously accredited boundary.

LEGEND

	Mission Component e.g. WebApp
	Core Component e.g. Server
	Infrastructure Component e.g. Cloud
	Assessment of mission component
	Accreditation boundary for assembled capability



Agile and Adaptive Ecosystem



Multi-Party Engineering grows the AAE:

1. Provide components
2. Offer components in markets
3. Certify components to shared agreements
4. Use Components to assemble capabilities
5. Solicit and respond to feedback from users

Results 1 of 2

Type of Effort	Description	Activity Level	Examples
IT Capability	Use a variety of mission and core infrastructure components to assemble an IT capability	Significant	<ul style="list-style-type: none"> Joint Logistics Enterprise Data Sharing (JLEDS), complete C-130 Electronic Flight Bag, in progress
New components; components harvested by deconstructing legacy components	Employ methods that range from community-wide data calls to identify new and/or potentially reusable services, to harvesting as a result of legacy deconstruction. Some components are traded across joint and/or family of systems organization boundaries.	Significant	<ul style="list-style-type: none"> Global Command and Control System – Joint (GCCS-J) and ACF (Agile Client Framework), complete Defense Intelligence Information Environment-Framework (DI2E-F), in progress Theater Battle Management Core System-Unit Level (TBMCS-UL), Command and Control Information Systems / Command and Control Air Operations Suite (C2IS/AOS), in progress
Hosting, platform	Engage in efforts ranging from classic hosting to cloud migration	Significant	<ul style="list-style-type: none"> Global Combat Support System – Air Force (GCSS-AF), complete Federal Risk and Authorization Management Program (FEDRAMP), complete CIO Cloud Strategy, complete Defense Information Systems Agency (DISA) Cloud Broker, in progress

Results 2 of 2

• Type of Effort	Description	Activity Level	Examples
• Mobile	Effort to use smartphones and other mobile devices	Very significant	<ul style="list-style-type: none"> • CIO Mobility Strategy, complete • National Geospatial-Intelligence Agency (NGA) Geospatial Intelligence (GEOINT) App Store, in progress • DoD Mobility, in progress • General Services Administration (GSA) Managed Mobility, in progress
• Markets and federation	Broad need to trade components across Title 10 and other organization boundaries.	Emerging	<ul style="list-style-type: none"> • Combatant Commands (COCOMs) and Services, in progress
• Component cybersecurity reciprocity	Ability to trade components across designated Authorizing Official (AO) boundaries	Emerging	<ul style="list-style-type: none"> • DoD Widget Working Group (WG), in progress

Maturity Scale (1 of 2)

Based on Multi-Party Engineering Tenets

Multi-Party Engineering Tenet	Example Activity
1. Provide Components	Both the Agile Client and Ozone Web Framework marketplaces demonstrate that program offices can build and/or acquire a component for their own use.
2. Certify components to Shared Agreements	Ongoing activities within DI2E-F aim to understand what it means for the community to agree (certify) that a service (component) is suitable for reuse, at least within the certifying community. Activities within DISA and NSA are seeking approaches to standardize vetting of mobile apps.
3. Offer Components in markets	Some markets are relatively mature, such as the NGA GEOINT app store; other markets are only beginning to develop. In some tactical cases, the DoD does not use markets in order to prevent changes to component configuration in the field.

Maturity Scale (2 of 2)

Based on Multi-Party Engineering Tenets

Multi-Party Engineering Tenet	Example Activity
4. Use components to assemble capabilities	<ul style="list-style-type: none"> • GCSS-AF presents a very mature example of full-service hosting • Some early examples of dedicated function-assembled capabilities (e.g., JLEDS) are appearing. • For dashboards, a server hosts several instances of web apps that are visualized as tiles in a browser for the purpose of organizing data for the user • Rapid assembly of mobile apps is gaining popularity. The DoD CIO and DISA are establishing strategies.
5. Solicit and respond to feedback from users	<p>MPE grows an AAE over time, at many scale levels by using feedback from end users as input to the requirements and governance of markets. No central planning takes place; however, developers receive feedback from users through local and community centers of federated governance. Some feedback loops are emerging at the direct, community, and enterprise levels. The feedback loops are ultimately the most important feature of the ecosystem</p>

Challenges

- 1. Cybersecurity reciprocity for mission-oriented software-only components.**
- 2. Create a business model(s) that enables repeatable and rapid acquisition of components and assembled capabilities**
- 3. Market federation to enable trading of components via markets across Title 10 and other boundaries.**
- 4. Build a community(s) that facilitates highly matrixed sharing of practices and case studies across direct, community, and enterprise efforts.**
- 5. Create and maintain a baseline of infrastructure and platforms that host various types of components.**

Outlook

- **JIE**

- Currently the bulk of direct, community, and enterprise efforts using Multi-Party Engineering are developed, deployed, and operated in the context of the U.S. and regional and mobile networks that are evolving to the JIE.

- **Mission Partner Environment**

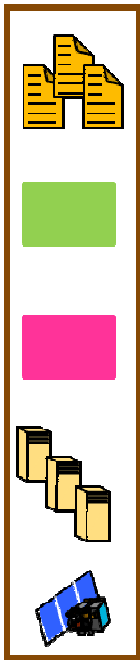
1. The components, markets, and assembled IT capabilities are starting to add value in the JIE. The value will be fully realized once DoD programs can deploy assembled capabilities to operational networks, including the Mission Partner Environment.
2. The agreement structure required for assembling IT capabilities resembles the agreement structure in Mission Partner Environment

Changing Perspectives

Today:

Each system requires
One dedicated program office

Acquisition/Accreditation Boundary

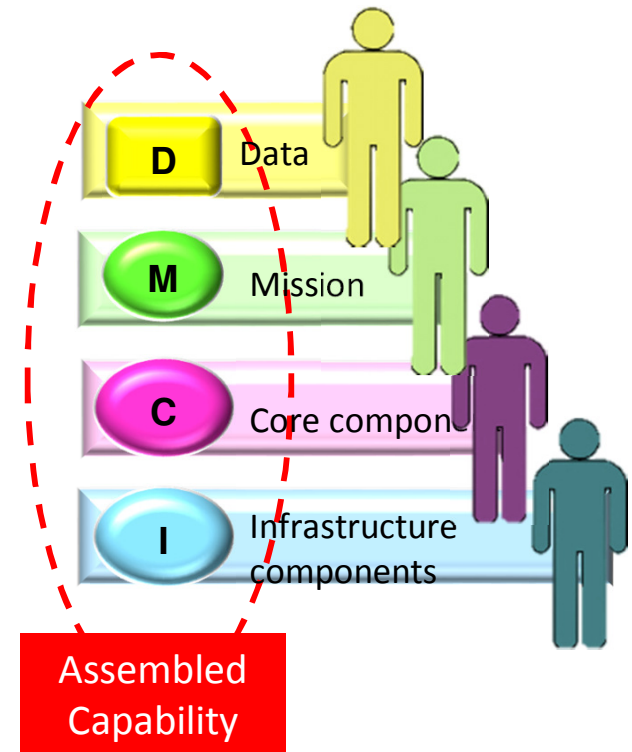


- Mission Information
- Mission Functionality
- Core / Middleware
- Computing
- Network



Tomorrow:

Each assembled capability requires
Multiple program offices



Competencies: Provide components, Assemble capabilities, Manage dependencies

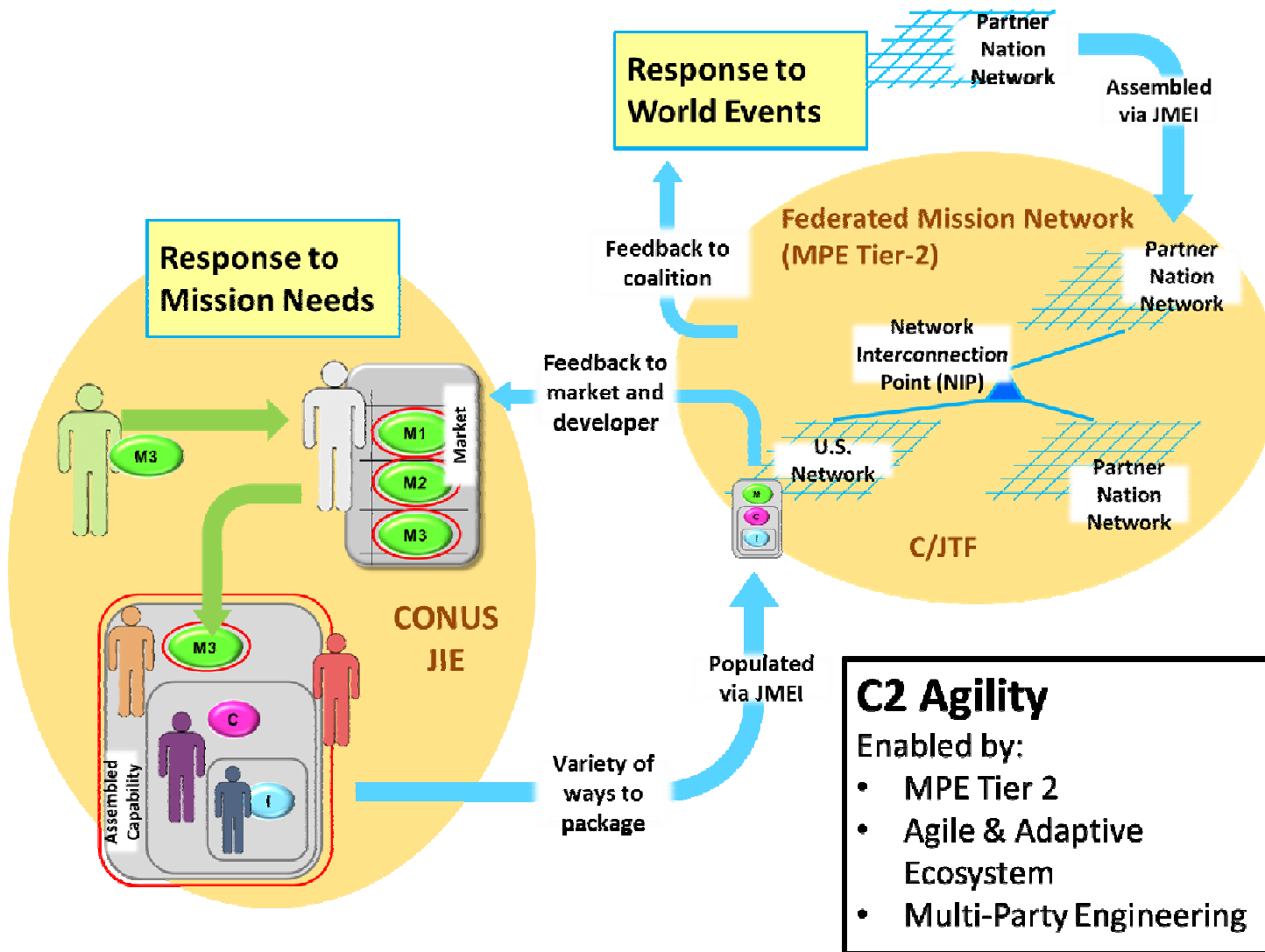
Recommendations

- 1. Create a nominal component lifecycle:**
 - Foster agreement among stakeholders across direct efforts as to the generic and repeatable nature of cybersecurity actions.
- 2. Create agreed 8510.01 product-level Security Assessment Reports (SARs) for each component type:**
 - This is in contrast to current 8510.01 SAR templates, which are oriented toward system development.
- 3. Create a nominal component adoption “organizational readiness” scale:**
 - Ensure organizations are aware of the change of perspectives, and challenges to meet.
- 4. Create an enterprise roadmap for enabling adoption of components and assembling capabilities:**
 - High-level goals for the enterprise, such as that expressed by JIE.
 - Must be guided by feedback from end users and direct efforts.

Conclusion: 2014 is a “Tipping Point”

- **Increasing need**
 - World events happen at an accelerating pace
 - Adversaries increasingly agile
- **Compelling Vision**
 - Commercial industry creating component technology at an accelerating pace
 - Practices starting to come into focus, i.e. Multi-Party Engineering which grows an Agile and Adaptive Ecosystem
- **Closing of Current Options**
 - Declining budgets
 - Very few “new starts” for big systems
- **Increasing Momentum**
 - DoD starting to adopt and understand necessary changes
 - Industry organizing to understand, partner and help drive change, i.e. Industry Advisory Group (part of AFEI/NDIA)

Vision: Assemble IT, Assemble C/JTF



IT Capabilities can be assembled and then populated into a federated mission network of a C/JTF; where the mission network is itself assembled via JMEI (Joining, Membership, Exiting Instructions).

- C2 Agility**
 Enabled by:
- MPE Tier 2
 - Agile & Adaptive Ecosystem
 - Multi-Party Engineering

Team

■ Authors

- Harvey Reed, Multi-Party Engineering, MITRE, hreed@mitre.org
- John Nankervis, Mission Partner Environment, CIV Joint Staff J6, john.t.nankervis.civ@mail.mil
- LtCol Jordon Cochran (USAF), OUSD(AT&L), jordon.t.cochran.mil@mail.mil
- Rajeev Parekh, US BICES Chief Engineer, MITRE, rparekh@mitre.org
- Fred Stein, Col. U.S. Army (ret), Network Centric Warfare, MITRE, fstein@mitre.org

■ POC

- Harvey Reed, hreed@mitre.org

■ Contributing

- Robert (Pat) Benito, Multi-Party Engineering, MITRE, rbenito@mitre.org
- Chris Magrin, DISA PEO-C2C Chief Engineer, MITRE, cmagrin@mitre.org
- Diane Hanf, Multi-Party Engineering, MITRE, dhanf@mitre.org
- Michelle Casagni, Multi-Party Engineering, MITRE, mcasagni@mitre.org

Multi-Party Engineering is emerging from Community and Direct Efforts

