

# Moving to the IC Cloud

Eric Blaine Werner

Software Solutions Conference 2015

November 16–18, 2015



Software Engineering Institute

Carnegie Mellon University

© 2015 Carnegie Mellon University

Distribution Statement A: Approved for Public Release;  
Distribution is Unlimited



Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

**NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.**

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

DM-0003049



# Agenda



**NIST and Cloud Computing**

**INSA: Doing in Common what is  
Commonly Done – IC ITE**

**IC ITE Strategy**

**IC ITE Perspectives**

**DI2E**

**SEI Work with DI2E and others**

**Cloud Challenges**





**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Special Publication 800-145

---

## The NIST Definition of Cloud Computing

---

Recommendations of the National Institute of Standards and Technology

---

Peter Mell  
Timothy Grance

---

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Special Publication 500-291, Version 2

---

## NIST Cloud Computing Standards Roadmap

---

*NIST Cloud Computing Standards Roadmap Working Group  
NIST Cloud Computing Program  
Information Technology Laboratory*

**NIST** National Institute of Standards and Technology • U.S. Department of Commerce



# Essential Characteristics

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability<sup>1</sup> at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

## The NIST Definition of Cloud Computing



# Service Models

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure<sup>2</sup>. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.<sup>3</sup> The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

## The NIST Definition of Cloud Computing



# Deployment Models

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

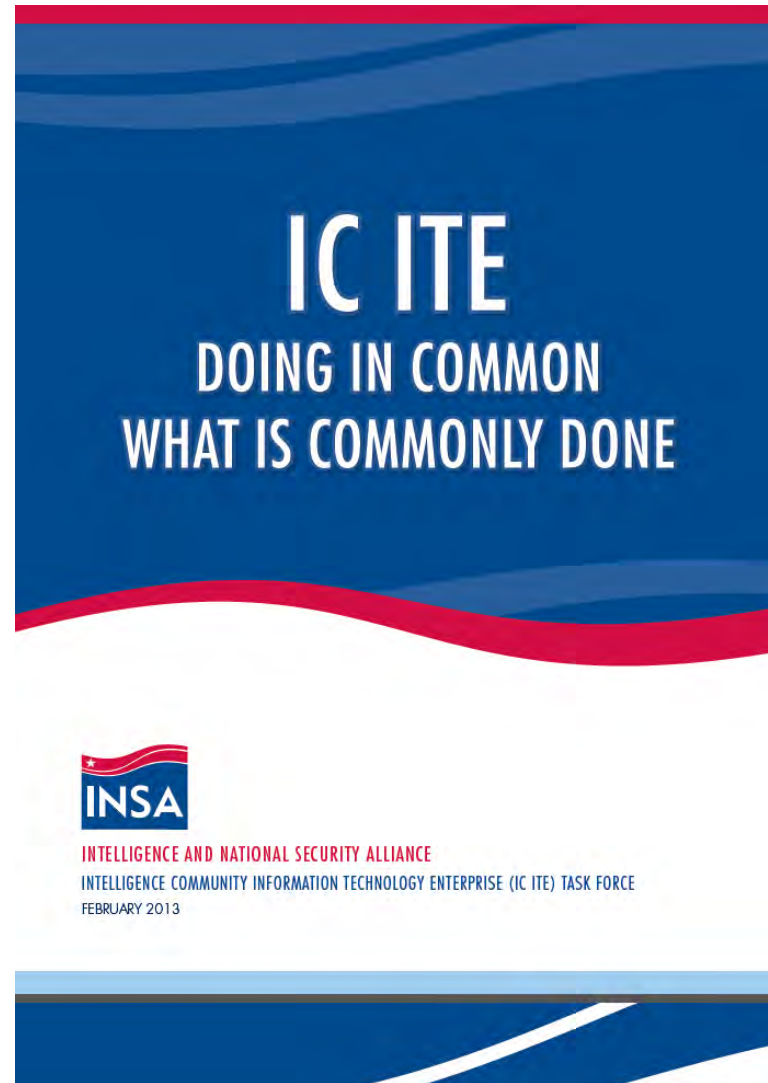
Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

## The NIST Definition of Cloud Computing

# INSA: Doing in Common what is Commonly Done



INSA: Doing in Common what is Commonly Done



# IC ITE



## IC ITE Vision and Future Direction

“Do in common that which is commonly done.” This is the theme that is frequently cited by IT managers within the IC to explain the IC ITE. IC ITE is a significant shift in how to plan for, develop and operate IC IT – moving the community from a collection of agency-centric enterprises to a single, secure, coherent, mutually operated and integrated IC IT Enterprise.

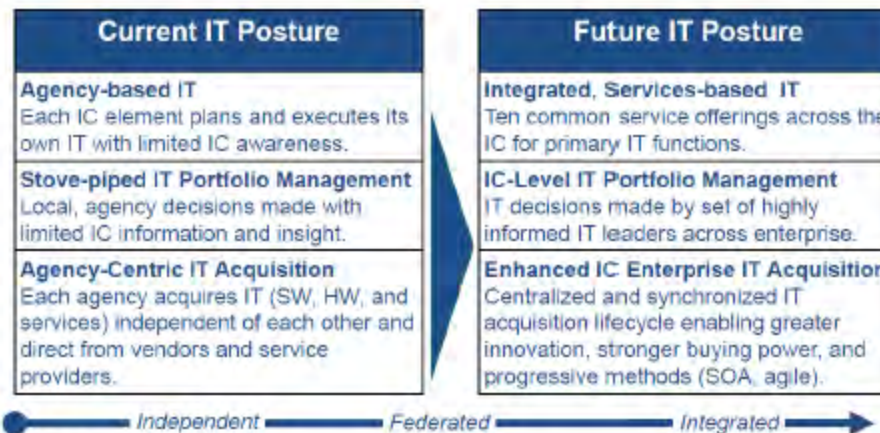


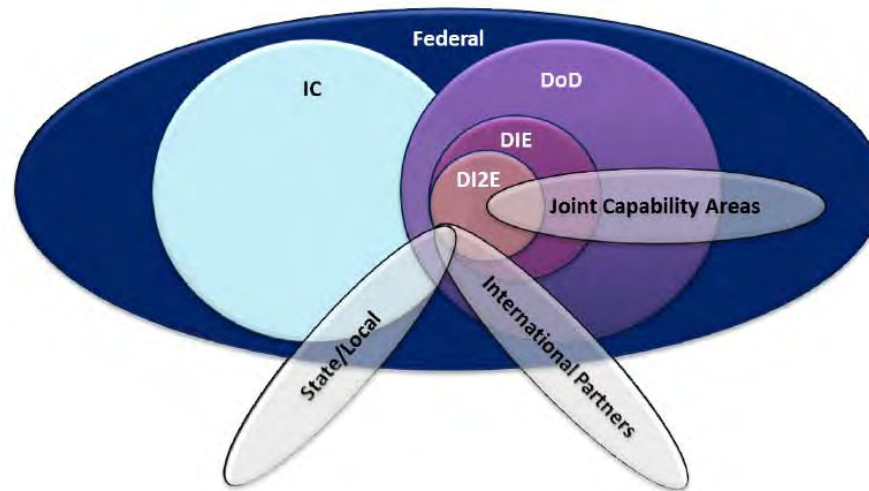
Figure 1 IC IT Current and Future

The IC ITE focuses on greater integration, information security, and information sharing while seeking substantial cost reductions through shared infrastructure and service models. The IC recognizes that each agency has particular strengths or core competencies that can be better leveraged by designating IC elements to act as Service Providers for specific capabilities for the entire Community. The DNI designates the IC Service Providers who are responsible for determining investment requirements and using their respective budget and acquisition and contract authorities to execute their IC ITE responsibilities. Currently identified common services and their respective providers include: the Desktop Environment, DIA and NGA; IC Cloud Services, NSA and CIA; Transport, NRO; Applications Mall, NSA; and Applications Stores, all agencies.

INSA: Doing in Common what is Commonly Done



# How IC ITE Fits in



## Must Operate Across A Broad Spectrum: White House to the Foxhole

TS Networks Dominate	↔	SECRET, REL, UNCLAS & Open Networks Dominate
Fixed Facilities	↔	Mix of Fixed, Temporary and Mobile Platforms
Stable MissionSet	↔	Dynamic Mission Sets
Stable Communities of Interest	↔	Dynamic Coalitions
Enduring Problem Sets	↔	Mission-based Intelligence Problems
High Bandwidth/Reliable Comms	↔	Mix of Comms (Reliable/Bandwidth Constrained) capabilities
Single Functional Agencies (i.e. HUMINT, SIGINT, GEOINT)	↔	Multi-Functional Military Services, COCOMs & CSA'

INSA: Doing in Common what is Commonly Done



# Shared Services

## IT Shared Service Model

Current IT standards, architectures, and approaches do not scale in the face of the austere budget. “One of the common complaints we hear from the field, from theaters involved in operations, is that all these people bring all their own networks and architectures with them”, said Neill Tipton, Director of Information Sharing for the Undersecretary of Defense for Intelligence. “You sit at a headquarters and you’ve got NSA guys on their NSA net, the NGA guys on the NGA net, the CIA’s on its own network. They’re all doing the same mission, supporting the same commander and working at the same objectives. But their idea of sharing data is sending emails to each other across their different networks. When we can roll into a theater of operations and bring in a single network to provide intel support to that theater that will be success”.<sup>3</sup>

### What is an IT shared service model?

Ask the question in the public sector and opinions vary. Some organizations define *true* shared services as the consolidation of IT functions from several departments or agencies into a single, stand-alone organizational entity whose only mission is to provide services as efficiently and effectively as possible.

Shared services frees up scarce resources to allow departments and agencies to focus on core business and customer needs while providing organizational flexibility to have IT structures independent of front-line activities and structures.

In a shared services model, the only function of the IT shared services organization is to run IT functions as effectively and efficiently as possible. IT shared services elevate the importance of administrative functions to the highest management levels.

INSA: Doing in Common what is Commonly Done



# Culture



## Culture

Moving to a shared architecture and IT shared services model will require significant cultural change in the IC, driven by the overarching need to share mission-related data.

By the very nature of organizations, culture pushes back on change and can get in the way of progress. Technology enablers can create platforms to enable and help facilitate the desired cultural changes on the mission side, while also fomenting complementary cultural changes in the IT organizations and workforces. As more clarity is achieved about the implementation details for IC ITE, greater differences between groups within the Community and apprehension about “how does this affect me” at the individual level will occur. Leaders in both the government and industry will need to engage in ongoing conversations with their employees to create a stronger collaborative culture among the IC members.

INSA: Doing in Common what is Commonly Done



# Industry and Academia

## The Role of Industry and Academia

Successful implementation of the IC ITE will depend on cultural, procedural and organizational shifts not only in government, but also in industry and academia. Without defense and commercial industry, as well as academia, the objectives of IC ITE and the building of an integrated, collaborative community will be difficult to achieve. Fundamental changes to sales approaches, business models, and staffing and education will be required.

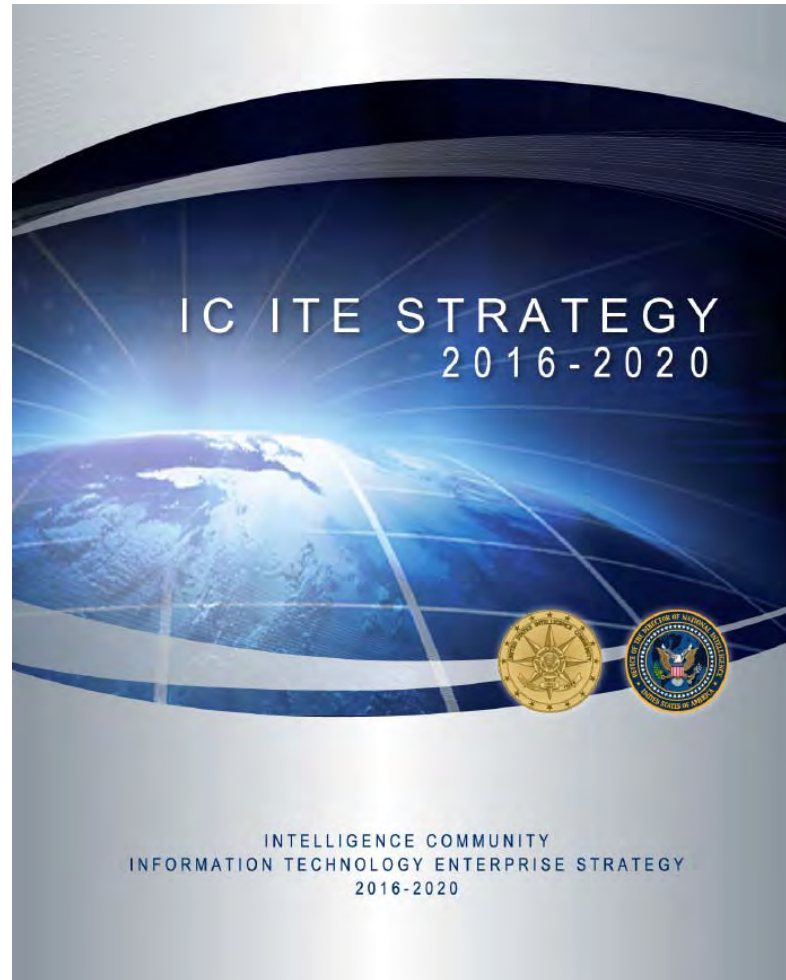
Both industry and academia have a long history of partnership with the IC and are paying close attention to the impending changes associated with the IC IT Enterprise. History and logic suggest they want to effectively support the effort, while trying to anticipate how the changes impact their current and future work, focus and deliverables. Their roles will need to be clarified as the IC IT effort progresses. The IC CIOs, for their part, are actively involved in outreach efforts with industry and academia to ensure they are cognizant of the “way forward,” to include multiple interactive forums such as IC/Industry Day partnership meetings and publications such as this INSA paper. As suggested earlier, consistent communications and leadership will be critical.

INSA: Doing in Common what is Commonly Done





# IC ITE Strategy



IC ITE Strategy 2016-2020





# Vision, Mission, Operating Principles

## VISION:

An Integrated Intelligence Enterprise

## MISSION:

To enable intelligence collection, analysis, and sharing through innovative, robust, and secure IT capabilities

## OPERATING PRINCIPLES:

### **Mission First**

Make decisions based on intelligence mission needs.

### **Lead**

Provide strategic leadership across the IC.

### **Partner**

Achieve unity of effort through teamwork, collaboration, and transparency.

### **Innovate**

Leverage technology to increase effectiveness and drive efficiency.

### **Achieve**

Deliver an integrated, secure enterprise to satisfy the highest mission priorities.

IC ITE Strategy 2016-2020



# Strategic Goals



**STRATEGIC GOALS**

- 1 Enhance Intelligence Integration**  
Promote the Intelligence Community's ability to integrate and unify intelligence activities by fully leveraging IC ITE.
- 2 Optimize Information Assurance to Secure and Safeguard the IC Enterprise**  
Enhance IC mission success through a trusted collaborative environment while protecting national intelligence information, sources, and methods as well as privacy and civil liberties.
- 3 Operate as an Efficient, Effective IC Enterprise**  
Achieve an IC ITE operating model that employs common business practices and Community teams to deliver, adopt, and sustain shared enterprise services and capabilities across the IC.

IC ITE Strategy 2016-2020





# JIE and IC ITE



## Navy's Journey to the JIE and IC ITE

A process not a destination

By Sharon Anderson - September 15, 2014

[Darren Sawyer](#) is the senior advisor for Navy Enterprise Information Technology for the Deputy Chief of Naval Operations (DCNO) for Information Dominance (N2/N6) and the lead for the Navy's journey to the Intelligence Community Information Technology Enterprise (IC ITE) and Defense Department Joint Information Environment (JIE).

In his role as a Senior Advisor for Navy Enterprise Architecture, Sawyer provides direct support to the Deputy Director of Naval Intelligence (OPNAV N2/N61), [Ms. Lynn Wright](#) on Navy intelligence architecture alignment, to the Deputy Chief Information Officer [Ms. Janice Haith](#) (OPNAV N2/N6BC) on intelligence architecture policies and portfolio compliance, and to the Assured Command and Control Division under [Mr. Matt Swartz](#) (OPNAV N2/N6F), for afloat and ashore Sensitive Compartmented Information (SCI) programs of record.

Working across these staff elements is very exciting, Sawyer said, as the Navy operationalizes its Information Dominance Strategy through better positioning of the information dominance pillars of Assured C2, Battlespace Awareness and Integrated Fires.

It is his task to work within the Navy to ensure these core information dominance pillars enable alignment to IC ITE and JIE, Sawyer said, at an AFCEA event in Norfolk, Virginia, Sept. 9. Both initiatives require enterprise architecture changing transformations. These transformations are fundamentally changing how the Navy will deliver information technology and cyber capabilities in a joint setting — and as part of the national intelligence community.

Both IC ITE and JIE are focused on driving toward greater efficiencies: delivering IT services at lower costs, greater effectiveness, and delivering the right IT enablers for warfighting effects, intelligence mission sets and greater security — and raising the security postures against increasingly sophisticated and persistent cyber threats.

Email

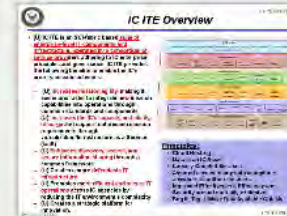


Figure 1. An overview of IC ITE.

Program (P-101000)	Information System
Operational Decision Environment (ODE)	DES and PICA
Operational Core (OC)	CIA
Operational Core (SOC)	NSR
Application - Not IAW	NSR
Intelligence Development System - Identity Authentication User	DES and PICA
Information Management (IAM)	NSR and CIA
Network Performance and Engineering Service (NRES)	NSR
Security Credential System (SCS)	IC CID

Figure 2. List of IC ITE Service Providers.




<http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=5497>



# Service Providers



UNCLASSIFIED



## IC ITE Service Providers

Enterprise Service	Responsible Agency
Common Desktop Environment (DTE)	DIA and NGA
Commercial Cloud (C2S)	CIA
Government Cloud (GovCloud)	NSA
Applications Mall (AML)	NSA
Enterprise Management Services	DIA and NGA
Identity Authentication and Authorization Management (IAA)	NSA and CIA
Network Requirements and Engineering Services (NRES)	NRO
Security Coordination Center (SCC)	IC CIO

Responsible Agency	Enterprise License Agreements
DIA	Microsoft, McAfee, BMC
CIA	Adobe, CITRIX
NGA	Symantec, ESRI, Raytheon, Overwatch
NSA	Red Hat, TIBCO, VMWare, Oracle, HP
NRO	IBM

UNCLASSIFIED <http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=5497>

# IC ITE Goals



## IC ITE Goals

UNCLASSIFIED

### (U) Goal 1: Fortify the Foundation

• Define, develop, implement and sustain a single, standards-based, interoperable, secure, and survivable IC IT Enterprise architecture that accomplishes mission objectives, and yet substantially increases efficiencies and safeguards across the enterprise, encompassing all security domains.

### (U) Goal 2: Deliver User-Focused Capabilities

• Provide seamless, secure enterprise solutions for trusted collaboration - people to people, people to data, and data to data - delivering user experiences that enhance mission success while ensuring protection of intelligence assets and information.

### (U) Goal 3: Operate as an IC Enterprise

• Adopt an operating model that employs standards, common business practices, commodity IT, and joint Community teams to deliver and sustain common enterprise services and capabilities across the IC.

### (U) Goal 4: Establish Effective Governance and Oversight

• Define and implement transparent IT governance and oversight processes that are driven by data.

### (U) Goal 5: Forge Strategic Partnerships

• Enhance trusted partnerships to better leverage innovative capabilities and integrate intelligence missions.



### Key Components/Capabilities

- IC Cloud (CLD) (GovCloud/C2S)
- Desktop Environment (DTE)
- Applications Mall (AML)
- Identification, Authentication and Authorization (IAA)
- Enterprise Service Management (EMT)
- Security Coordination Center/Services (SCC)
- Network Requirements and Engineering Service (NRES)

UNCLASSIFIED

8

<http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=5497>





# IC ITE Overview - perspectives



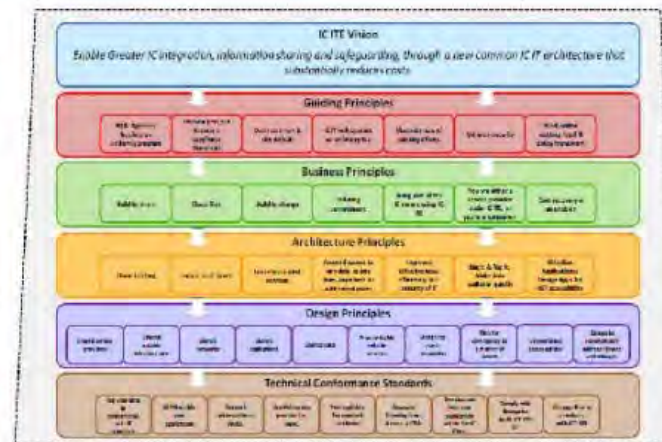
UNCLASSIFIED

## IC ITE Overview

- (U) IC ITE is an SCI-fabric based **suite of enterprise-level IT components and infrastructure, operated by a consortium of service providers** adhering to IC enterprise principles and governance. IC ITE provides the following benefits to enable the IC's priority mission activities:
  - (U) **Increases mission agility**, making it easier and faster to integrate new mission capabilities into operations through common standards and components
  - (U) **Increases the IC's capacity and ability to surge** and support unforeseen mission requirements through virtualization/Infrastructure as a Service (IaaS)
  - (U) **Enhances discovery, access, and secure information sharing** through a common framework
  - (U) Creates a more **defendable IT infrastructure**
  - (U) Promotes more **efficient and secure IT operations** across IC agencies by reducing the IT environment's complexity
  - (U) Creates a strategic platform for innovation.

UNCLASSIFIED

7



### Principles:


- Cloud Hosting
- Data is an IC Asset
- Loosely Coupled Services
- Assured access to any data at anytime, anywhere to authorized users
- Improved Effectiveness, Efficiency and Security are not mutually exclusive
- Bag It, Tag It, Make Data Available Quickly

UNCLASSIFIED

<http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=5497>



# DI2E



OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

## The DI2E Story

<http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-West.pdf>





# DI2E

 OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

## The DI2E Framework is...





An agreed to set of building blocks for the Defense Intelligence Community to more efficiently, effectively and securely develop, deliver, and interface their mission-based architectures.

**Focused on Interoperability - Convergence "When & Where it Makes Sense"**

Standards and web service specifications are the key DI2E Framework building blocks.

### Resulting In...

- ✓ Reduced Cost
- ✓ Improved Interoperability
- ✓ Improved Mission Success
- ✓ Faster, More Responsive Delivery
- ✓ Improved Security
- ✓ Faster Adoption of Commercial IT

 Reduced Cost	 Improved Interoperability	 Improved Mission Success
 Faster, More Responsive Delivery	 Improved Cyber Security	 Faster Adoption of Commercial IT

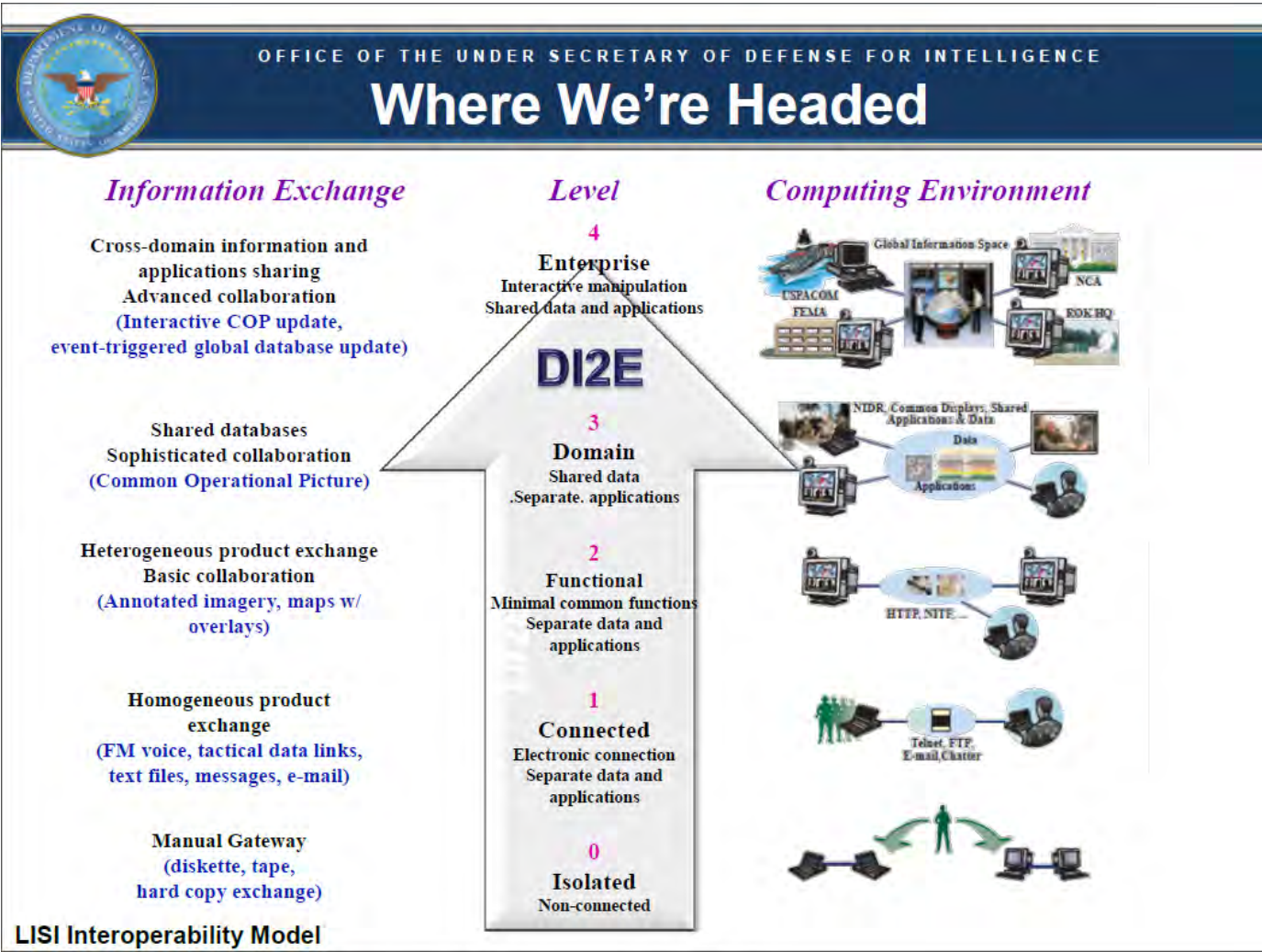
**Capitalizing on the "Wisdom of Crowds"**

12

<http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-West.pdf>



# DI2E

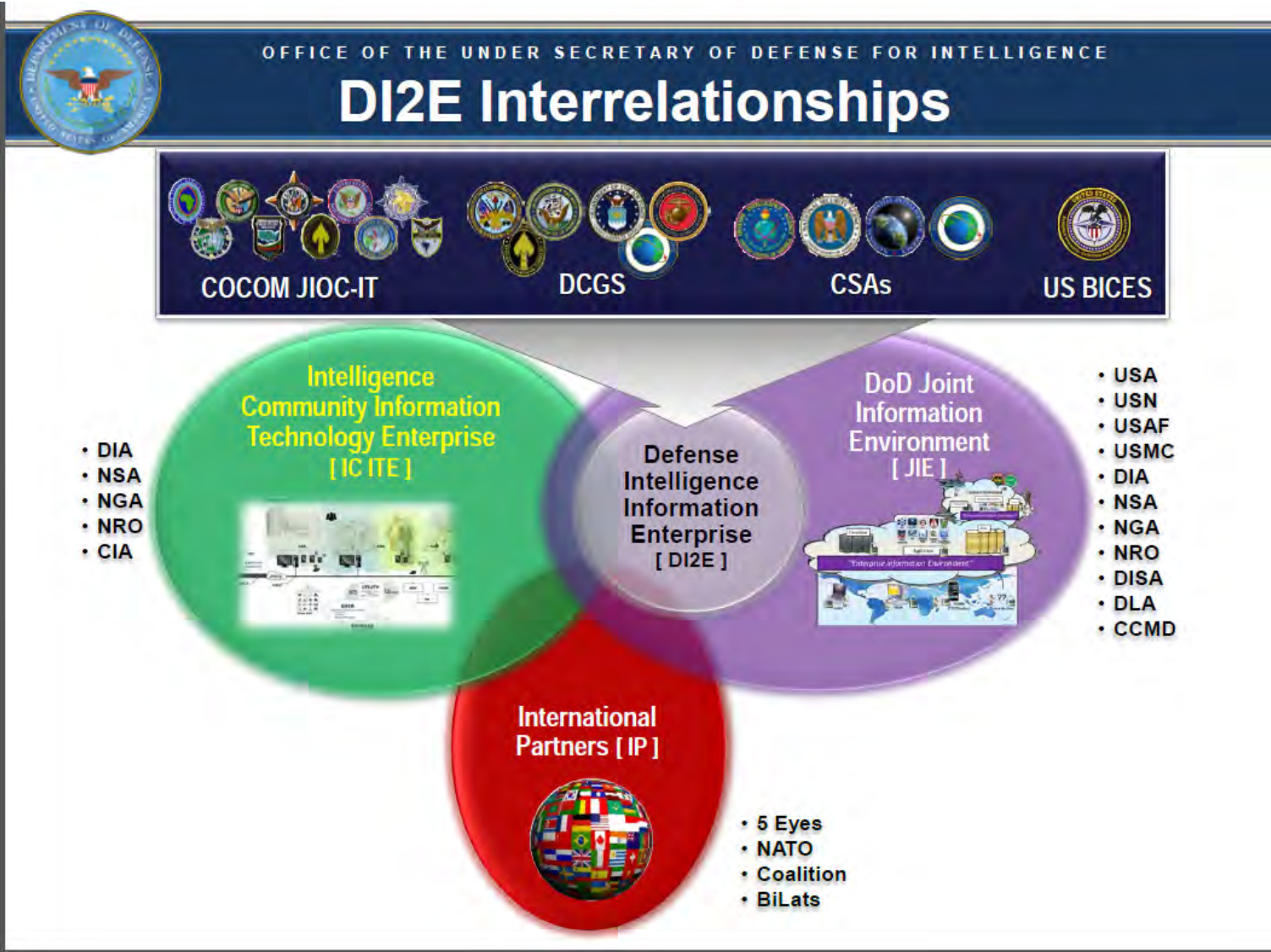


<http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-West.pdf>





# DI2E



<http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-West.pdf>





# DI2E – SEI Work

## SEI Blog

The Latest Research in Software Engineering and Cybersecurity

### ■ Open Architectures in the Defense Intelligence Community

POSTED ON OCTOBER 27, 2014 BY ERIC WERNER IN COMMON OPERATION PLATFORM ENVIRONMENTS (COPES)



In an era of [sequestration and austerity](#), the federal government is seeking software reuse strategies that will allow them to move away from stove-piped development toward open, reusable architectures. The government is also motivated to explore reusable architectures for purposes beyond fiscal constraints: to leverage existing technology, curtail wasted effort, and increase capabilities rather than reinventing them. An open architecture in a software system adopts open standards that support a modular, loosely coupled, and highly cohesive system structure that includes the publication of key interfaces within the system and full design disclosure.

One area where the Department of Defense (DoD) is concentrating on the development of service-oriented architectures and common technical frameworks is in the intelligence community, specifically the [Defense Intelligence Information Enterprise \(DI2E\)](#). As this blog post details, a team of researchers at the [SEI Emerging Technology Center \(ETC\)](#) and the [Secure Coding Initiative in the SEI's CERT Division](#), are working to help the government navigate these challenges in building the DI2E framework, which promotes reuse in building defense intelligence systems.

#### Foundations of Our Work

Our work focused on development of a framework for DI2E, the non-command-and-control (C&C) part of the [Distributed Common Ground System \(DCGS\)](#) and the [Combat Support Agencies \(CSAs\)](#). The DI2E Framework provides the building blocks for the [Defense Intelligence Community](#) to more efficiently, effectively, and securely develop, deliver, and interface their mission architectures. The core building blocks of the DI2E framework are components that satisfy standards and specifications, including web service specifications that enable a stable but agile enterprise supporting rapid technology insertion.

The key objective of the DI2E Framework is to increase operational effectiveness, agility, interoperability, and cybersecurity while reducing costs. The framework consists of a reference implementation (RI), a test bed, and a storefront. When completed, the DI2E will provide a fully

[https://insights.sei.cmu.edu/sei\\_blog/2014/10/open-architectures-in-the-defense-intelligence-community.html](https://insights.sei.cmu.edu/sei_blog/2014/10/open-architectures-in-the-defense-intelligence-community.html)





[About Us](#) [Advertise](#) [Contact Us](#) [Subscribe](#) **New!** [Editorial](#) [Tech Briefs](#)



[POLICY](#) [MANAGEMENT](#) [EXEC TECH](#) [WHO & WHERE](#) [THE HILL](#) [A](#)

**Intelligence**

# ICITE faces 'cultural resistance'

*By Sean Lyngaas* Mar 03, 2015

Bureaucratic resistance is slowing the intelligence community's adoption of a common IT architecture, according to former acting Defense Intelligence Agency Director David Shedd.

"The single biggest problem" for adopting the IC Information Technology Enterprise (ICITE) is "cultural resistance" from intelligence officials clinging to the IT status quo, Shedd told FCW on March 3. "I don't even think it's technological, and it's not budget."



# Moving to the IC Cloud

## Questions / Discussion

