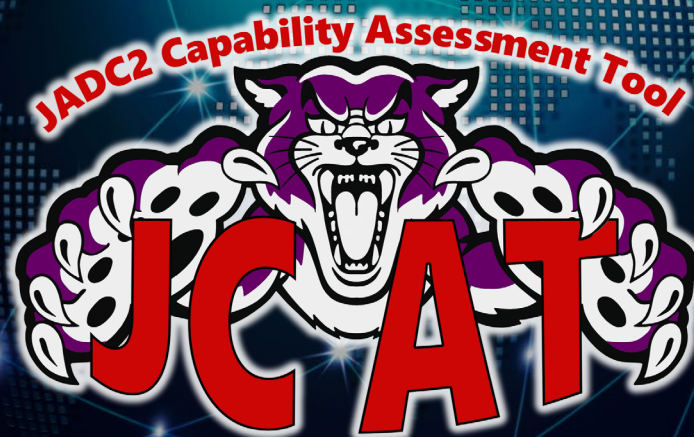




Joint All-Domain Command and Control (JADC2) JADC2 Capability Assessment Tool (JCAT)



**Joint Chiefs of Staff J6
Joint Assessment Division (JAD)**

Version 2.0

Instructions:

The JADC2 Capability Comparison Form measures:


- (1) JADC2 Design (low-high)
- (2) Maturity (low-high)
- (3) Operational Impact (low-high).

The results of this Form will be used to prioritize candidates for JADC2 assessment. Please provide as much information as possible. Any questions should be directed to the Joint Staff, J6 Joint Assessment Division (JAD).

Please fill out the questions and send by email
(Preferably Encrypted email or zip with password)

Lloyd Ashby (GS-14)

Joint Staff J6/DDC5I
116B Lakeview Parkway
Suffolk, VA 23435-2663

 **Desk:** (757) 203-5117

 **NIPR Email:** lloyd.s.ashby.civ@mail.mil

 **SIPR Email:** lloyd.s.ashby.civ@mail.smil.mil

You can also use <https://safe.apps.mil/> to send the Controlled Unclassified Information (CUI) form if needed.

Thank you for your time and efforts.

LINKS:

NOTE: The JCAT Tool is in the link to the left "JADC2 Capability Assessment Tool (JCAT)

NIPR: https://intelshare.intelink.gov/sites/jadc2/_layouts/15/start.aspx#/SitePages/Home.aspx

SIPR: https://intelshare.intelink.sgov.gov/sites/jadc2/_layouts/15/start.aspx#/SitePages/Home.aspx

(U) Primary Point of Contact (POC)**A) Name (last)****B) Name (First)****C) Job Title****D) Rank****E) Unit / Organization:****F) Directorate / Division / Office:****G) Email (Government / Business):****H) Phone:****(U) Alternate Point of Contact (POC)****I) Name (last)****J) Name (First)****K) Job Title****L) Rank****M) Unit / Organization:****N) Directorate / Division / Office:****O) Email (Government / Business):****P) Phone:**

CAPABILITY

Q) (U) What is the name or title of the capability? Please include long title, acronym, and version / release number.

Name or Title of The Capability:

Version / Release Number:

R) (U) Provide a brief description of this capability and its operational contribution to achieve JADC2 . If applicable, include whether the capability is in operational use, as well as any operational assessments or tests that may have been performed, (either on the capability itself or on the Agile DevSecOps delivery process), and completed cybersecurity testing.

S) (U) What organizations are using this capability to accomplish an operational mission? Please identify if the user(s) is also a proponent / developer of the capability.

T) (U) What organizations (include POCs) are sponsoring and developing this capability?

U) (U) What organization is the Program Management Office (include POC) for this capability?

V) (U) Provide URLs for any on-line references (Home page, Share Point, Wiki, Research Articles, etc.).

JADC2 CAPABILITY QUESTIONS

DESIGN

1)	Which Service(s) are the intended users of the capability (Army, Navy, Air Force, Marines, Space Force)? <u>(Select Only One)</u>
	Data Not Available
	Subset of a Single Service (ex. Naval Air)
	Single Service (ex. Army)
	Multi-Service (2 or more services)
	All Services
2)	Who are the prospective (“as is” and “to be”) users of the capability? <u>(Select Only One)</u>
	Data Not Available
	US DoD Only (Services, Combatant Command and Joint Forces)
	US DoD and US Non-DoD Mission Partners
	Multilateral (US plus 2 or more nations)
	Five Eyes
	Alliance/Coalition (e.g., NATO)
3)	To what level is (will) the capability be interoperable with Coalition and Multi-national partners by design? <u>(Select Only One)</u>
	Data Not Available
	US only
	Bilateral integration with one (1) nation
	Multi-lateral integration with multiple nations (3 or more) located across one Combatant Commander Area of Responsibility
	Multi-lateral integration with nations located across 2 or more Combatant Command Areas of Responsibility
	Multi-lateral integration within an Alliance/ Coalition (e.g. NATO)
	Integrated in a S//REL MPE-compliant environment
4)	Which operational domain or domains will be supported by the capability (Space, Air, Maritime, Land, Cyberspace)? <u>(Select Only One)</u>
	Data Not Available
	Subset of a Single Operational Domain (ex. Cyberspace – Defensive Ops)
	Single Operational Domain (ex. Cyberspace)
	Multi-Operational Domain (2 or more Domains)
	All Operational Domains
	All Operational Domains plus Electro-Magnetic Spectrum Operations

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

5)	Which Joint Functions are supported? <u>(Select All That Apply)</u>
	Data Not Available
	C2
	Fires
	Intelligence
	Movement
	Protection
	Sustainment
	Information
6)	How does the capability contribute to direct or indirect command and control (C2) of Joint and Coalition Forces? <u>(Select Only One)</u>
	Data Not Available
	Does not support C2
	C2 Enabling (i.e. infrastructure)
	C2 Supporting (i.e. provides data / information to C2 processes)
	Provides C2 of forces (Plans, directs, monitors, or assesses)
7)	Which aspect(s) of command and control are supported? <u>(Select All That Apply)</u>
	Data Not Available
	N/A
	Situational Awareness
	Force Employment
	Planning and Force Projection
8)	Who owns the rights to the capability? <u>(Select Only One)</u>
	Data Not Available
	Proprietary solution
	Partially proprietary and partial government owned, relies on contract sustainment (training, FSR, configuration, or operation)
	Government owned and sustained
9)	Who owns the rights to the data generated by the capability? <u>(Select Only One)</u>
	Data Not Available
	Proprietary data controlled by contract
	Partially proprietary and partial government owned (i.e, at least a portion of the resulting data is controlled by the contract)
	Data is Government owned, stored, and sustained

10)	Select the JADC2 Core Enablers and Design Principles you are implementing.
	a) Does the capability enable Identity, Credential and Access Management (ICAM)? <u>(Select Only One)</u>
	Data Not Available
	N/A
	Implements an independent ICAM solution/protocol
	Leverages enterprise ICAM
	Leverages enterprise ICAM that is federated with other ICAM services
	b) Does the capability enable Zero Trust concepts? <u>(Select All That Apply)</u>
	Data Not Available
	N/A
	Data has been metadata labeled (tagged) which includes data classification and the metadata is registered with the data source
	Communications are secure both within and external to network location
	Access to data or other IT resources is granted on a per-session basis
	Access granting is by dynamic policy (e.g. digital policy check, etc.) including behavioral and environmental attributes
	All assets are monitored for integrity and security posture
	Resource Authentication and Authorization is enforced before access is allowed
	JADC2 environment (data, IT assets, network infrastructure, communications, nodes, etc.) security posture dynamically refined based upon real time status.
	c) Does the capability utilize Cloud Services? <u>(Select Only One)</u>
	Data Not Available
	N/A
	Hosted in a commercial cloud environment
	Hosted in a DoD cloud environment
	Hosted in a DoD cloud environment that has been integrated/federated with other DoD / IC Cloud environments
	d) Does the capability utilize resilient (95% Up Time), robust (<24 Hr Mean Time to Repair) transport and networking services? <u>(Select Only One)</u>
	Data Not Available
	N/A
	Leverages commercial transport only (ex. ISP)
	Leverages existing DoDIN transport
	Leverages a combination of transport methods under an approved DoD program/ policy that implements software (vs. hardware) defined networking

e) Does the capability utilize data services that are accessible and discoverable?

(Select All That Apply)

Data Not Available

N/A

Data is distributed to pre-determined recipients based upon mission/system requirements

Data is multi-cast on a network and accessible to subscribers who know the data is available and request access

Data is available via a data store/lake for access by a wide variety of subscribers agnostic of application, system, or platform.

Data is registered as a data source with its associated metadata in a catalog and provides an API or other interface access for IT services/application to incorporate the data.

All the catalogs are federated to the DoD catalog hub

f) If the capability is developed in a DevSecOps environment, does it align with the ten (10) Plays outlined in the DoD DevSecOps Playbook?

(Select All That Apply)

Data Not Available

N/A

Developing organization has adopted a DevSecOps Culture

Adopted Infrastructure as Code

Adopted Containerized Microservices

Adopted a Capability Model, not a Maturity Model

Drove continuous improvement through key capabilities

Established a Software Factory

Defined a meaningful DevSecOps pipeline

Adapted an Agile Acquisition Policy for Software

Tirelessly pursued cyber resilience

Shifted Test and Evaluation (T&E) left into the pipeline

g) Does the capability support a Mission Partner Environment (MPE), Secret and Below Releasable Environment (SABRE)?

(Select Only One)

Data Not Available

N/A

Capability is designed and developed with releasable versions (releasable to Mission Partners)

Capability is conformant with Federated Mission Network (FMN) Spiral Specifications

Capability can fully connected to the MPE based on discrete Communities of Interest (COIs) bounded by common and interoperable data

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

11)	Are emerging technologies integrated into the capability? (Select All That Apply)
	Data Not Available
	N/A
	Artificial Intelligence / Machine Learning (AI/ML)
	Virtualization
	Integrated Tactical Networks
	Cross Domain Security and Sharing
	Internet of Things (IoT)
	Edge Computing
	Extensible S/W platform enabling addition of new capabilities, algorithms, analytics from other sources
MATURITY	
12)	Identify the development phase of the capability.
	a) If program is formal acquisition according to DoD 5000.2: (Select Only One)
	Data Not Available
	N/A
	Basic research activity, pre-Milestone A
	Concept & Technology Development, pre-Milestone B
	System Development & Demonstration, pre-Milestone C
	Production & Deployment, pre-IOC
	Operations & Support, pre-FOC
	b) If the capability is a Rapid Defense Experiment Reserve (RDER) Initiative, Joint Capability Technology Demonstration (JCTD) or otherwise government sponsored: (Select Only One)
	Data Not Available
	N/A
	Prototype development
	Advanced development; demonstration
	Full scale development
	c) If the capability program is not government sponsored (enter the name of the sponsoring entity in the comment block at the end of the survey): (Select Only One)
	Data Not Available
	N/A
	Prototype development
	Demonstration
	Full scale development

	d) If program is following the Software Acquisition Pathway: Non-Agile Development <u>(Select Only One)</u>
	Data Not Available
	N/A
	Inception
	Design
	Implementation
	Maintenance
	e) If program is following the Software Acquisition Pathway: Agile Development <u>(Select Only One)</u>
	Data Not Available
	N/A
	Concept
	Inception
	Iteration
	Release
	Maintenance
13)	Indicate the capability's funding approval status. <u>(Select Only One)</u>
	Data Not Available
	Not government sponsored or funded
	FYDP - funding begins 1+ yrs. out
	Funding approved for concept development
	FYDP - current year funding
14)	Indicate the capability's funding adequacy. <u>(Select Only One)</u>
	Data Not Available
	Funded at < 60% of required level (over length of program or FYDP) as compared to the Program/Capability IGCE?
	Funded at 60%-80% of required level (over length of program or FYDP) as compared to the Program/Capability IGCE?
	Funded at > 80% of required level (over length of program or FYDP) as compared to the Program/Capability IGCE?
15)	What is the projected timeframe to reach Initial Operating Capability (IOC), or comparable milestone? <u>(Select Only One)</u>
	Data Not Available
	10+ years
	5-10 years
	3-5 years
	0-3 years
	IOC Achieved

16)	What is the projected timeframe to reach Full Operational Capability (FOC), or comparable milestone? <u>(Select Only One)</u>
	Data Not Available
	10+ years
	5-10 years
	3-5 years
	0-3 years
	FOC Achieved
17)	Are there any institutional barriers impacting continued development of this capability solution? <u>(Select Only One)</u>
	Data Not Available
	None
	Policies
	Procedures
	Processes
	Laws
	Situational
18)	Indicate the degree of risk to achieving the required technical performance. a) Independence from Special/New Technology or Materials: <u>(Select Only One)</u>
	Data Not Available
	Heavy dependency on new technology or material, and the technical know-how for which is still under development
	Moderate dependency on new technology or material, which is expected to be available imminently, or low dependency on new technology or material that are still under development.
	Minimal dependency or no dependency on new technology or material.
	b) Technology Readiness Level (TRL) of the capability as of date of input to this Survey: <u>(Select Only One)</u>
	Data Not Available
	1-3 Research
	4-6 Development
	7-9 Deployment
	c) Independence from Supporting Systems <u>(Select Only One)</u>
	Data Not Available
	Medium to heavy dependency on other supporting products/systems, and other supporting products/systems are not expected to be completely developed prior to the development of the candidate product/system/capability
	Medium to heavy dependency on other supporting products/systems that are already developed, or low dependency on other supporting products/systems that are under development
	Minimal dependency or no dependency on other supporting products/systems

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

19)	<p>Indicate the degree to which the necessary training support for operators has been established. (Select Only One)</p> <p>Data Not Available</p> <p>N/A</p> <p>Training Plan required but not yet developed</p> <p>Training Plan in Development</p> <p>Training Program Established or no additional training program development required</p>
20)	<p>Indicate the degree to which the capability has been evaluated for cybersecurity. (Select Only One)</p> <p>Data Not Available</p> <p>N/A</p> <p>The capability has not yet been evaluated</p> <p>Actively using Risk Management Framework</p> <p>Vulnerability (Red Team) Assessment Complete</p> <p>Penetration Testing (Red Team) Completed</p>
21)	<p>Does the capability have an Authority to Operate or Connect (ATO/ATC)? (Select Only One)</p> <p>Data Not Available</p> <p>N/A</p> <p>ATO/ATC not yet sought</p> <p>ATO/ATC in progress</p> <p>cATO/ATO/ATC fully acquired</p>
OPERATIONAL IMPACT	
22)	<p>Does the capability address validated capability gaps?</p> <p>a) CCMD Integrated Priority List (IPL) (Select Only One)</p> <p>Data Not Available</p> <p>None</p> <p>Contributes to resolution of CCMD IPL (i.e., necessary, but not sufficient to resolve the IPL)</p> <p>Primary effort providing CCMD IPL resolution</p> <p>b) Joint Emergent Operational Need (JEON) or Joint Urgent Operational Need (JUON) (Select Only One)</p> <p>Data Not Available</p> <p>No</p> <p>Contributes to resolution of a JEON or JUON (i.e., necessary, but not sufficient to resolve the need)</p> <p>Primary effort providing JEON/JUON resolution</p>

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

	c) JADC2 2021 Posture Review Capability Gap (Concept Required Capabilities (CRC's)) (Select All That Apply)
	Data Not Available
	No
	CRC 01 Pre-bundled and Tiered Authorities
	CRC 02 Enhanced Machine Element Capabilities
	CRC 03 Re-focused Human Element Performance
	CRC 04 Tailored Organization Structure
	CRC 05 Mapping the Non-physical Battlefield
	CRC 06 All Domain Inventory and Authority Description
	CRC 07 All Domain Fire Control
	CRC 08 Protect
	CRC 09 Data Interoperability
	CRC 10 Wargames, Experiments, Exercises, Demonstrations and Training
23)	Does the capability directly contribute to execution of the Joint Warfighting Concept scenarios? (Select Only One)
	Data Not Available
	Neither
	Directly contributes to EUCOM scenario
	Directly contributes to INDOPACOM scenario
	Directly contributes to both scenarios
24)	Select the Combatant Commands that are supported with this capability. (Select All That Apply)
	Data Not Available
	NORTHCOM
	CENTCOM
	INDOPACOM
	EUCOM
	SOUTHCOM
	AFRICOM
	CYBERCOM
	SPACECOM
	SOCOM
	STRATCOM
	TRANSCOM
25)	To what extent does the capability improve existing mission accomplishment functionality? (Select Only One)
	Data Not Available
	Already is a fielded capability, or replaces an existing capability with minimal additional impact to mission accomplishment
	Provides near-term, specific improvement to an existing capability
	Provides long-term, wide-reaching improvement to existing capabilities
	Provides a new capability that does not exist today

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

26)	At what Tier Levels are users of this capability? (Select All That Apply)
	Data Not Available
	Tier 0 National Command Authority
	Tier 1 Between CCMDs
	Tier 2 Between CCMDs and Subordinates
	Tier 3 Between Joint Force Commander and Subordinates
	Tier 4 Tactical Edge
27)	Does the capability promote or improve C2 joint or Coalition interoperability? (Select Only One)
	Data Not Available
	No impact to current levels of C2 interoperability
	Resolves specific or near-term C2 interoperability issues
	Resolves systemic or critical changes to C2 interoperability issues
28)	Does the capability operate in Denied, Degraded, Intermittent, or Limited Bandwidth (D-DIL) environments? (Select Only One)
	Data Not Available
	N/A
	No, relies on centralized services or guaranteed connectivity
	Maintains some basic functionality in D-DIL environment, but with significant impact to interoperability, resilience, and QoS
	Maintains all critical functionality in D-DIL environment with sufficient interoperability, resilience, and QoS; however, doctrinal authorities have not yet been defined to support D-DIL operations
	Maintains all critical functionality in D-DIL environment and doctrinal pre-approved authorities have been defined to support D-DIL operations of the capability
29)	Will the capability comply with current doctrine? (Select Only One)
	Data Not Available
	Requires development of new doctrine
	Requires significant changes to current doctrine
	Requires minimal/no changes to current doctrine

General Comments

(Please place any additional information in this section that you feel needs to be added for your Capability)