DoD Directive 5101.21E

DoD Executive Agent for Unified Platform and Joint Cyber Command and Control (JCC2)

Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	June 4, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Deputy Secretary of Defense Memorandum, "Designation of Executive Agent for Unified Platform and Joint Cyber Command and Control," May 17, 2017
Approved by:	David L. Norquist, Deputy Secretary of Defense

Purpose: This issuance:

- Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (DoD EA) for Unified Platform (UP) and JCC2 in accordance with DoD Directive (DoDD) 5101.01.
- Designates the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) to serve as the Principal Staff Assistant to oversee the DoD EA for UP and JCC2.
- Establishes governance structures to assist in the prioritization and execution of acquisition efforts for UP and JCC2 capabilities.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 3
1.1. Applicability. 3
1.2. Policy. 3
SECTION 2: RESPONSIBILITIES 4
2.1. USD(A&S). 4
2.2. Director, Test Resource Management Center (TRMC). 4
2.3. SECAF. 4
2.4. Secretary of the Army. 6
2.5. CC/S/As. 7
2.6. Secretaries of the Military Departments, CDRUSCYBERCOM, and Commander, U.S. Special Operations Command. 7
2.7. CDRUSCYBERCOM. 7
SECTION 3: UP AND JCC2 GOVERNANCE STRUCTURE 9
3.1. Governance. 9
3.2. Councils of Colonels. 9
GLOSSARY 11
G.1. Acronyms. 11
G.2. Definitions. 11
REFERENCES 13

FIGURES

Figure 1. Governance Structure 10

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD.

1.2. POLICY.

a. The DoD-wide UP and JCC2 effort will optimize investments, close critical cyberspace capability gaps, and ensure delivery of resilient, agile, secure, and effective cyberspace capability solutions to the warfighter.

(1) The primary purpose of UP is to integrate disparate cyber capabilities, systems, infrastructure, and data analytics, allowing the Cyber Mission Force (CMF) to conduct integrated cyber processing, analysis, exploitation, and dissemination supporting full spectrum cyber operations.

(2) The primary purpose of JCC2 is to deliver integrated solutions that provide decision makers, planners, analysts, and operators at all JCC2 echelons with capabilities that facilitate cyber situational awareness, rapid planning, course of action selection, orders development, dynamic mission management, decision support, and unified direction of cyber mission forces.

b. DoD cyberspace capability solutions that integrate seamlessly across the physical domains (air, space, land, and maritime) will provide the joint force with enhanced multi-domain capabilities. These capabilities will contribute to an interoperable and scalable network that allows integrated planning and execution of the full spectrum of cyberspace operations.

SECTION 2: RESPONSIBILITIES

2.1. USD(A&S).

The USD(A&S):

a. Oversees the SECAF's functional areas of DoD EA responsibility.

b. Appoints representatives to additional governance bodies that the SECAF establishes.

c. Coordinates with the Director, Cost Assessment and Program Evaluation, to ensure equitable DoD-wide resourcing support for the SECAF's DoD EA responsibilities consisting of 30 percent funding each from the Army, Navy and Air Force, and 10 percent from the Marine Corps.

2.2. DIRECTOR, TEST RESOURCE MANAGEMENT CENTER (TRMC).

Under the authority, direction, and control of the Under Secretary of Defense for Research and Engineering, the Director, TRMC, is the DoD EA for Cyber Test Ranges in accordance with DoDD 5101.19E. The Director, TRMC coordinates SECAF efforts with respect to DoD cyberspace test ranges to consider UP and JCC2 acquisition and capability development solutions.

2.3. SECAF.

With respect to both UP and JCC2, under the oversight of the USD(A&S), and in addition to the responsibilities in Paragraphs 2.5. and 2.6., the SECAF:

a. Monitors and coordinates with the Commander, U.S. Cyber Command (CDRUSCYBERCOM), regarding joint cyberspace requirements prioritization. In this capacity, SECAF:

(1) Conducts solutions analyses and acquisition activities.

(2) Identifies joint cyberspace capability gaps.

(3) Advocates for efficient allocation of resources.

(4) Optimizes investment.

(5) Synchronizes the delivery of non-materiel and materiel solutions to deliver integrated system for UP and JCC2 capabilities.

b. Executes, in coordination with the USD(A&S), Combatant Commanders, Secretaries of the Military Departments, Chief, National Guard Bureau, and Defense Agency and DoD Field Activities (CC/S/As), memorandums of understanding, memorandums of agreement, or other instruments necessary to effect a coordinated, DoD-wide cyberspace capability development and delivery effort.

c. Conducts requirements analyses; course of action analyses or similar business case analyses; acquisition and capability development; and fielding for an integrated suite of joint UP and JCC2 related cyberspace solutions. Develops cost estimates to support these efforts and submits them for three-star program review.

d. Coordinates, de-conflicts, and rationalizes CC/S/A requirements generation, acquisition, and Planning, Programming, Budgeting, and Execution activities of critical cyberspace capabilities to effect a joint DoD-wide effort.

e. Undertakes such capabilities-based assessments, joint capability technology demonstrations, rapid prototyping, and other experiments and evaluations as necessary to determine unidentified critical cyberspace capability gaps.

f. Coordinates all JCC2 policies and implementing instructions with regard to capabilities planning, programming, and budgeting recommendations with the DoD Chief Information Officer in accordance with DoDD 3700.01.

g. Implements a coordinated, DoD-wide cyberspace capability comprised of an environment of compatible hardware platforms, software, and network components in an architecture that promotes an interoperable and secure environment for UP and JCC2 purposes.

h. Develops architectures, interfaces, data, and other standards that support validated joint cyberspace operations requirements, consistent with relevant DoD enterprise architectures and standards. Ensures that these architectures and standards, including relevant cyberspace operations reference architectures, are created and updated in accordance with DoD Information Enterprise Architecture standards, as established in DoD Instruction 8310.01.

i. Plans, conducts, and coordinates appropriate UP- and JCC2-related acquisition activities, including materiel solutions analysis, advocating for program(s) of record, technology development, developmental and operational test, technical assurance evaluation, production and deployment, and operations and sustainment. The SECAF will use such coordination to resolve potential conflicts and duplication of effort, and to ensure optimal investment of resources and capability delivery across DoD.

j. Develops UP and JCC2 solutions as necessary to provide the CMF with a seamlessly integrated set of cyberspace capabilities that comprehensively address operational requirements, as appropriate.

k. Generates materiel and non-materiel solutions that, to the extent practical, promote functionally interoperable solutions that address UP and JCC2 capability gaps.

l. Coordinates UP and JCC2 capability development in accordance with Section 392 of Title 10, United States Code, with the Secretary of the Army and the Director, TRMC (for those ranges specified in DoDD 5101.19E), to:

(1) Evaluate emerging training, exercise, and experimentation requirements.

(2) Sponsor and resource future cyberspace training range solutions.

m. Coordinates with the Under Secretary of Defense for Personnel and Readiness and the CDRUSCYBERCOM to advocate synchronization of the UP, JCC2, and Persistent Cyber Training Environment training capabilities.

n. Identifies resource (funding and manpower) requirements for the acquisition and implementation of UP and JCC2 solutions to the USD(A&S) as soon as they are determined to support resourcing and acquisition decisions.

o. Acts as the Secretariat for forums comprising UP and JCC2 governance structure. As the Secretariat, the SECAF:

(1) Provides DoD senior leadership with regular updates on the execution of acquisition efforts pertaining to UP and JCC2 capabilities, through existing Cyber Investment and Management Board and other applicable reporting processes.

(2) Oversees, coordinates, and adjudicates UP and JCC2 issues, working closely with the USD(A&S), the Chairman of the Joint Chiefs of Staff, and CDRUSCYBERCOM. Programmatic issues that cannot be resolved will be deliberated during the annual Program and Budget Review. If necessary, outstanding concerns will be forwarded to the Three-star Programmers in accordance with Chairman of the Joint Chiefs of Staff Instruction 3265.01A; the Deputy's Management Action Group in accordance with DoDD 5105.79; or other senior-level decision-making forums.

(3) Formalizes the multi-tiered governance structure, as described in Section 3, and further delegates DoD EA responsibilities as appropriate. To ensure maximum responsiveness, UP and JCC2 governance bodies will empower decisions at the lowest possible management level.

2.4. SECRETARY OF THE ARMY.

In addition to the responsibilities in Paragraphs 2.5. and 2.6., under the oversight of the Under Secretary of Defense for Personnel and Readiness, and in the capacity as the DoD EA for Cyber Training Ranges in accordance with DoDD 5101.19E, the Secretary of the Army:

a. Coordinates efforts with respect to Deputy Secretary of Defense-designated cyberspace training ranges with the SECAF to consider training solutions that address emerging training and exercise requirements resulting from UP and JCC2 capability development.

b. Coordinates the efforts of the acquisition lead for the Persistent Cyber Training Environment with the SECAF consistent with Paragraph 2.3.a.

2.5. CC/S/As.

The CC/S/As:

a. Coordinate with and submit their cyberspace operations requirements related to UP and JCC2 to U.S. Cyber Command (USCYBERCOM) for review, validation, and prioritization.

b. Coordinate requirements generation; solutions analyses; planning, programming, and budgeting; and acquisition activities relating to UP and JCC2 with the SECAF to establish, promote, and deploy an integrated DoD-wide approach.

c. Designate in writing and provide subject matter experts to support SECAF solutions, analyses, technology development, architecture development and evolution, prototyping, acquisition, and capability development for UP, JCC2, and related activities as determined by the USD(A&S).

d. Ensure that implementation of policy and responsibilities in this issuance, when it involves foreign entities, is conducted in accordance with DoD policies for disclosure of classified military information in DoDD 5230.11, and for international transfers in DoD Instruction 2040.02.

2.6. SECRETARIES OF THE MILITARY DEPARTMENTS, CDRUSCYBERCOM, AND COMMANDER, U.S. SPECIAL OPERATIONS COMMAND.

In addition to the responsibilities in Paragraph 2.5.:

a. The Secretaries of the Military Departments and CDRUSCYBERCOM designate representatives with suitable functional knowledge and expertise to the UP and JCC2 Council of Colonels as described in Section 3.

b. The Secretaries of the Military Departments and the Commander, U.S. Special Operations Command, will retain their responsibility to present trained, equipped, and ready forces for their portion of the CMF, pursuant to Joint requirements and interoperability standards.

2.7. CDRUSCYBERCOM.

In addition to the responsibilities in Paragraphs 2.5. and 2.6., the CDRUSCYBERCOM:

a. Identifies critical cyberspace capability gaps related to UP and JCC2 to the SECAF through:

(1) Continuous collaboration.

(2) Established processes such as joint urgent operational needs, joint emergent operational needs, joint lessons learned, integrated priority lists, and capability gap assessments.

(3) Analysis of interagency cyberspace architectures, standards, and operations.

b. Validates and prioritizes joint cyberspace operations requirements.

c. Develops, in coordination with the DoD EA for UP and JCC2 and the other CC/S/As, operations that are necessary to effect the proper employment of existing and future cyberspace systems.

d. Provides SECAF results and recommendations from prototype development related to gaps in the UP and JCC2 capability package.

e. Coordinates with SECAF regarding CDRUSCYBERCOM's authorities granted pursuant to Section 807 of Public Law 114-92 and Section 167b of Title 10, United States Code, to resolve potential conflicts and duplication of effort, and to ensure optimal investment of resources and capability delivery across DoD.

f. Prescribes, in coordination with the Military Departments, cyberspace operations interoperability and data standards.

SECTION 3: UP AND JCC2 GOVERNANCE STRUCTURE

3.1. GOVERNANCE.

UP and JCC2 will be governed by an Executive Cyber Council, a Steering Board, and two Councils of Colonels as shown in Figure 1. The Executive Cyber Council will endorse Steering Board recommendations and resolve any Steering Board disputes. The Steering Board will resolve Council of Colonels disputes and make policy, process, and strategy recommendations to the Executive Cyber Council.

a. Governance objectives will be to coordinate and integrate the relevant cyber requirements generation, acquisition, and Planning, Programming, Budgeting, and Execution activities of the CC/S/As; identify and resolve issues; and provide DoD senior leadership with a forum for oversight and decision-making.

b. Any subordinate governance structure established by SECAF will be integrated to the maximum extent practical with existing governance bodies and include appropriate representation from the Joint Staff, the Office of the USD(A&S), USCYBERCOM, the DoD Chief Information Officer, the Office of the Under Secretary of Defense for Intelligence, the Defense Information Systems Agency, and other CC/S/As, as appropriate.

3.2. COUNCILS OF COLONELS.

The Councils of Colonels:

a. Act as the solution backlog managers for UP and JCC2 cyber development and operations activities. They:

(1) Maintain, through working groups they establish, continual understanding of CMF needs.

(2) Identify, define, and prioritize the capabilities backlog through the Capabilities Working Groups under the UP and JCC2 Councils of Colonels, led by USCYBERCOM.

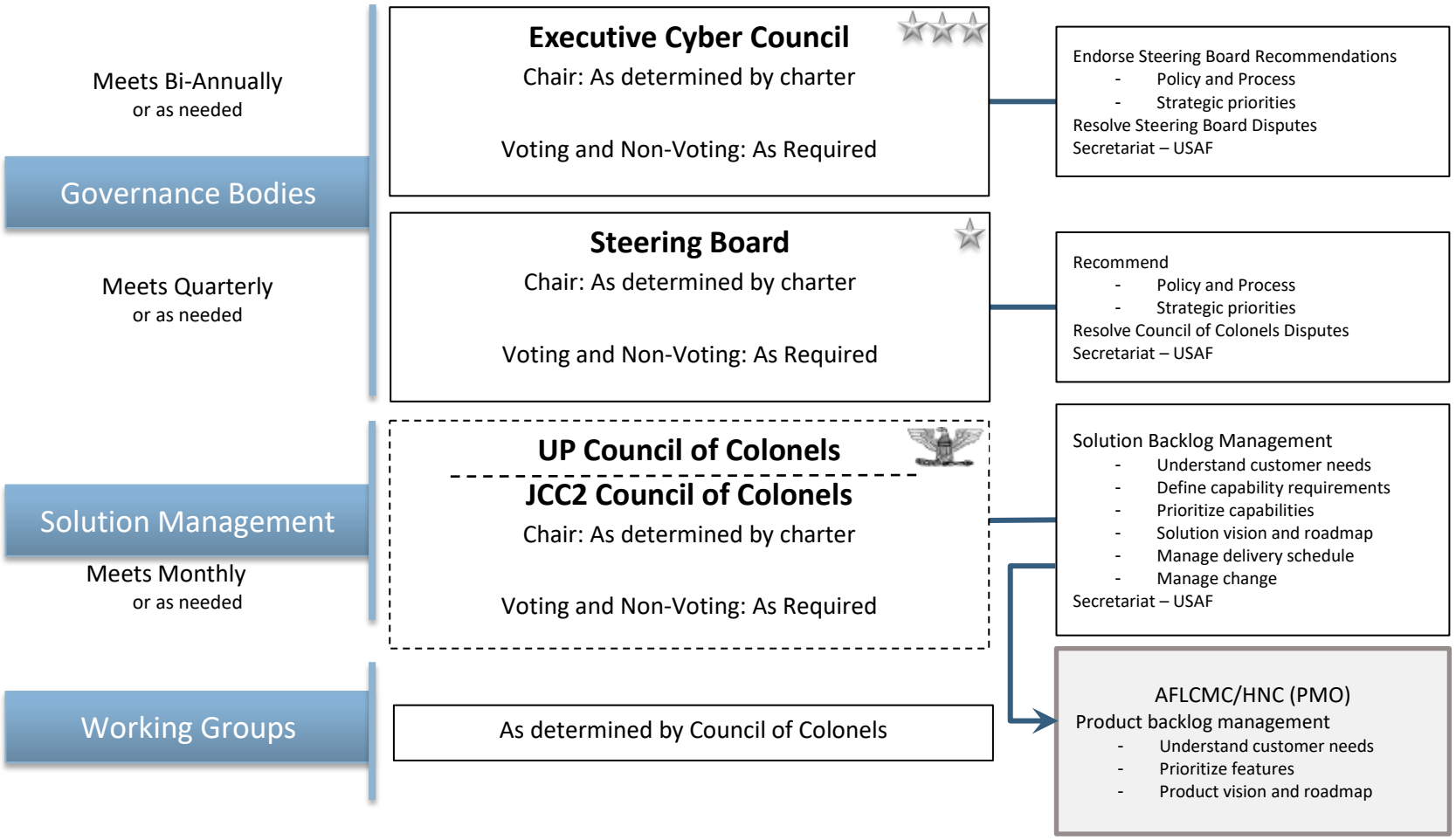
(3) Manage capability delivery schedules.

(4) Direct change management activities.

b. Develop and maintain solution vision and solution roadmaps for all UP and JCC2 cyber development and operations activities.

c. Make recommendations to the Steering Board with respect to the programming and execution of Service-contributed resources in accordance with Paragraph 2.1.c.

Figure 1. Governance Structure



GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AFLCMC/HNC	Air Force Life Cycle Management Center Cryptologic and Cyber Systems Division
CC/S/A	Combatant Commanders, Secretaries of the Military Departments, Chief, National Guard Bureau, and Defense Agency and DoD Field Activities
CDRUSCYBERCOM	Commander, U.S. Cyber Command
CMF	Cyber Mission Force
DoD EA	DoD Executive Agent
DoDD	DoD directive
JCC2	joint cyber command and control
PMO	Program Management Office
SECAF	Secretary of the Air Force
TRMC	Test Resource Management Center
UP	unified platform
USAF	U.S. Air Force
USCYBERCOM	U.S. Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
capabilities backlog	Repositories for all the upcoming work that affects the behavior of the solution. Based on operational mission threads within the scope of the UP and JCC2 Information Systems Initial Capabilities Documents, USCYBERCOM develops strategic and operational viewpoints of the architecture. USCYBERCOM prioritizes the operational capabilities backlog based on threat and mission priority.

TERM	DEFINITION
CMF	Defined in Joint Publication 3-12.
C2	Defined in the DoD Dictionary of Military and Associated Terms.
JCC2 system	A collection of capabilities that provide the battlespace commander the situational and battlespace awareness needed to track and provision the cyber forces, plan and execute missions in cyberspace, develop and distribute operations orders, track the cyber battle through battlespace through visualization, and integrate cyber operations with multi-domain operations. It consists of five capability areas: global force awareness, collaborative planning, orders development and dynamic mission management, timely and effective workflows, and decision support. These capability areas combine through various technologies to provide situational and battlespace awareness in a seamless C2 system for the cyber operator.
Three-Star Programmers	A DoD Functional Oversight Committee. Leads the review of the Program Objectives Memorandum submitted by the DoD components, and screens and develops issues for presentation to the Deputy's Management Action Group. The Chair of the Three-Star Programmers is the Director of Cost Assessment and Program Evaluation.
UP	The primary purpose of UP is to integrate disparate cyber capabilities, systems, infrastructure, and data analytics, allowing the CMF to conduct integrated cyber processing, analysis, exploitation, and dissemination supporting full spectrum cyber operations.

REFERENCES

Chairman of the Joint Chief of Staff Instruction 3265.01A, "Command and Control Governance and Management," October 21, 2013

DoD Directive 3700.01, "DoD Command and Control (C2) Enabling Capabilities," October 22, 2014, as amended

DoD Directive 5101.01, "DoD Executive Agent," September 3, 2002, as amended

DoD Directive 5101.19E, "DoD Executive Agents for the DoD Cyber Test and Cyber Training Ranges," August 24, 2018

DoD Directive 5105.79, "DoD Senior Governance Councils," May 19, 2008

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 8310.01, "Information Technology Standards in the DoD," February 2, 2015, as amended

Joint Publication 3-12, "Cyberspace Operations," June 8, 2018

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Public Law 114-92, Section 807, "National Defense Authorization Act for Fiscal Year 2016," November 25, 2015

10 U.S. Code § 167b. "Unified Combatant Command for Cyber Operations"

United States Code, Title 10, Section 392