JOINT C4 PLANNERS COURSE

RECOMMENDED TRAINING AND READING LIST

Joint Command Control Communication and Computer Planners Course (JC4PC)

US Army Cyber School of Excellence

Fort Gordon, GA. 30905

Recommended Training List for JC4PC

Note: The staff and cadre at the JC4PC have compiled the following list of web-based training to complete prior to attending the course. Being familiar with this material will better suite you for course instruction. This is a list of recommended training and not pre-requisites and not comprehensive.

- **Joint Communications System**. States the objective of the joint communications system; describes key principles and components of the joint communications system; and identifies organizational roles and responsibilities related to the operation of the joint communications system. JP6-0, Joint Communications System.
  http://www.dtic.mil/doctrine/docnet/courses/communications/index.htm

- **Joint Operation Planning**. Key doctrine concepts and principles related to planning for joint operations; joint planning and execution community roles and responsibilities; overview of design as applied to operational art, steps in the joint operation planning process; key joint operation planning inputs, processes, and products (2hrs 40mins). JP5-0, Joint Operation Planning.
  http://www.dtic.mil/doctrine/docnet/courses/planning/jplan.htm

- **Cyberspace Defense**. This interactive web-based training defines cyberspace defense (CD), presenting CD as a subset of cybersecurity. The training describes what DoD Information Networks (DoDIN) and Network Operations (NetOps) are, to include the relationship between them and their functioning within the single security architecture of the Joint Information Environment (JIE). This instruction identifies key cybersecurity requirements for cyberspace defense for the DoD, for each DoD Component, and for local control centers within each DoD Component. The user learns which organizations provide cybersecurity services for the DoD, as well as the requirements these Cybersecurity Service Providers (CSPs) must meet to provide cybersecurity services. This training presents a high-level explanation of the certification and accreditation process for CSPs. The CSP principal services are enumerated; to include system protection services; anti-malware; system scanning tools; Information Operations Conditions (INFOCON) Program support; Information Assurance Vulnerability Management (IAVM) support; vulnerability assessment monitoring, analysis, and detection services; as well as incident response. An explanation of the training and certification requirements for those who work as CSPs is also included. This product is designed for high-level managers who need to acquire a CSP for their organization, cybersecurity professionals who want to transition into a CSP career path, and individuals who desire a general knowledge of cyberspace defense and Cybersecurity Service Provider functions and responsibilities. (2 hrs)
  http://iase.disa.mil/eta/Pages/online-catalog.aspx

- **NetOps**. The NetOps 100 course provides a common understanding of NetOps functions, roles, responsibilities, and benefits. This course is designed to provide an overview of NetOps for all of DoD. (Length - 1 hr 15 min). The NetOps 200 course is a follow-on to NetOps: An Overview (NetOps 100), and is designed to expand upon the "how" of

NetOps by explaining the DoD NetOps policies, methodologies, and enabling technologies that facilitate Net-Centricity, effective situational awareness, and mission mapping. NetOps Applied GIG (DoDIN) Operations (NetOps 200) is technical, and focuses on applying the NetOps concepts within the GIG (DoDIN) operational environment. This course elaborates on key DoD NetOps concepts, capabilities, tools, and models/frameworks to facilitate effective situational awareness and collaborative command and control (C2) of the GIG (DoDIN). (Length - 1.5 hrs)
http://iase.disa.mil/eta/Pages/online-catalog.aspx

- **Risk Management Framework (RMF)**. The purpose of this course is to provider people new to risk management with an overview of a methodology for managing organizational risk – the Risk Management framework (RMF). The RMF was developed to help organizations manage risks to and from Information technology (IT) systems more easily, efficiency and effectively. The course describes, at a high-level, the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step.
http://iase.disa.mil/eta/Pages/online-catalog.aspx

- **Joint Knowledge Online (JKO) Courses**, (MUST HAVE A CAC TO GAIN ACCESS), https://jkodirect.jten.mil/Atlas2/faces/page/login/Login.seam
    a. **Introduction to Mission Partnership Environment, J3OP-US1277**. The Mission Partner Environment (MPE) courses are designed to provide students with an understanding that the MPE capability is comprised of existing information technology tools that allow the Joint Force Commander to visualize, describe, and direct action in a timely and trusted fashion with mission partners involving a U.S. Military cultural change to the art of Command and Control. At its core, MPE is an operational design that moves US military operations off the SIPRNet into a single classification environment that allows mission partners to share information. The Introduction to Mission Partner Environment is a prerequisite for the MPE Planning Course. The purpose of the MPE Introduction course is to provide students with an overview of the Mission Partner Environment (MPE) to include it origin, purpose, and capability framework. Additionally, the introduction will include an understanding of MPE governance, terms and definitions, system configuration, Joining Membership Exiting Instructions (JMEI), and basic core services.
    b. **Mission Partnership Environment Planning, J3OP-US1278**. The purpose of the MPE Planning course is to provide students, possessing a basic understanding of MPE gained through the introductory course, the basic steps and considerations necessary to plan a US led, Joint Interagency, Intergovernmental and Multinational (JIIM) operation with an MPE command and control (C2) construct with any and all mission partners for any one of three missions (Combat OPS, Stability OPS, and Defense Support of Civil Authorities (DSCA) and humanitarian assistance/disaster relief (HA/DR) in any geographic combatant command (GCC).

c. **Lifecycle of the JTF, APC 006-14**. The purpose of this course is to provide an overview of the lifecycle of the Joint Task Force (JTF). It examines the six different phases of. the lifecycle; planning; forming; deploying; employing; transitioning; and redeploying. It also explores the responsibilities of the combatant command and the JTF staff, and how both the combatant command and JTF execute the different phases in support of theater operations. The lesson also describes the instructional methodology used for the follow-on lesson for the lifecycle of the JTF. The overall classification of this course is UNCLASSIFIED.

d. **Introduction to Joint Fundamentals, J3OP-US1141**. To enhance operational effectiveness of joint forces, it is important to have an understanding of the fundamental principles that guide the employment of U.S. military forces in coordinated and, where and when appropriate, integrated action toward a common objective.

e. **Joint Operational Planning, APC 002-14**. The purpose of this course is to examine joint operation planning in detail, extending the broader general discussion of the joint planning overview lesson. Joint operation planning combines two complementary processes; the Joint Operation Planning Process, or JOPP, and the use of Operational Art and Operational Design. Recent doctrinal changes have provided greater emphasis on Operational Art and Design and how the combatant commander arrives at the Operational Approach for a mission. Several graphical charts provide a notional display of the adaptive planning process and its' relationship to JOPP. The overall classification of this course is UNCLASSIFIED.

f. **Joint Staff Officer Cyberspace Operations Awareness Course, J3OP-US1101**. The Joint Staff Officer Cyberspace Operations Awareness Course is intended to provide students an awareness of various facets of cyberspace operations and how these capabilities will impact personnel assigned to joint billets. The course provides a basic introduction to common lexicon, current draft guidance, policy and legal authorities and operational roles and responsibilities associated with cyberspace operations. This course also conveys some of the challenges confronted with integrating cyberspace operations into overall operations. This course has been designed for those who have had limited or no training in cyberspace operations.

g. **Establishing a Cyberspace Situational Awareness (CSA) Capability Course, J3ST-US1221**. The purpose of this course is to help develop, refine, and validate solutions geared towards improving our ability to gain and maintain situational awareness of the cyber domain from a cyber defense perspective. This course presents a resilience methodology, a cyber defense information sharing framework, legal considerations for operating within the cyber domain, CSA enabling technologies, and a set of required CSA capabilities; the purpose of which is to offer the operational community assistance and information to aid ongoing efforts to improve cybersecurity.

Recommended Reading List for JC4PC

Note: The staff and cadre at the JC4PC have compiled the following list of material to read prior to attending the course. Being familiar with this material will better suite you for course instruction. This is a list of recommended reading and not pre-requisites and not a comprehensive list.

- **JP 6-0. Joint Communications System, June 10, 2015**. This publication is the keystone document for the communications system series of publications. It provides the doctrinal foundation for communications system support to joint operations and provides a comprehensive approach to the support of joint force command and control through the integration of joint communications and information systems across the range of military operations. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf

- **Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D. Defense Information Systems Network (DISN) Responsibilities, 24 Jan. 2012** (Current as of 4 Aug. 2015). This instruction establishes policy and responsibilities for the connection of information systems (ISs) (e.g., applications, enclaves, or outsourced processes) and unified capabilities (UC) products to the DISN provided transport (including data, voice, and video) and access to information services transmitted over the DISN (including data, voice, video, and cross domain (CD)).
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf

- **Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231.01E. Manual for Employing Joint Tactical Communications.** The manual serves as the umbrella document that sets the framework and guidance for developing tactics, techniques, and procedures (TTPs) necessary to support integration of communications networks and Internet Protocol (IP)-based net-centric capabilities required to support a Joint or Coalition Task Force (J/CTF), Joint Special Operations Task Force (JSOTF), or other military operations. It identifies the communications concepts, provides guidance for planning and employing joint tactical communications equipment, and serves as guidance for lesson plan development associated with the Joint C4 Planners Course (JC4PC). https://ca.dtic.mil/cjcs_directives/cdata/limited/m623101.pdf (USE EMAIL CERTIFICATE).
The document lists a URL for the online collaboration website, the updated URL is: https://disa.deps.mil/ext/cop/ns-extranet/NS1/NS11/NS112/JTTP/default.aspx

- **Chairman of the Joint Chiefs of Staff (CJCSM) 3130.03. Adaptive Planning and Execution (APEX) Planning Formats and Guidance, 18 October 2012, (Annex K)**. This manual sets forth administrative instructions for joint operational plans and planning products (ANNEX K) which will conform to the guidance, standardized formats, and content herein.
(USE EMAIL CERTIFICATE).
https://ca.dtic.mil/cjcs_directives/cdata/limited/m313003.pdf

- **Department of Defense (DoD) Unified Capabilities (UC) Master Plan (UCMP), Oct 2011.** The purpose of the DoD UCMP is to define the implementation strategy to converged, net-centric, IP-based enterprise UC as required by DoD Instruction (DoDI) 8100.04, "DoD Unified Capabilities." The UCMP serves as a guideline to the DoD Components in the preparation of implementation and acquisition plans for phasing in voice and video over IP services, and other UC that shall operate in converged voice, video, and/or data networks. The UC MP addresses synchronization of life-cycle activities, from acquisition to operations to sustainment until retirement, for DoD networks that provide UC. The UCMP provides guidance for DoD Component Program Objective Memorandum submissions.
  http://www.disa.mil/~/media/Files/DISA/Services/UCCO/APL-Process/Unified_Capabilities_Master_Plan.pdf

- **Department of Defense (DoD) Unified Capabilities Requirements 2013 (UCR 2013) Change 1, June 2015.** The DoD Unified Capabilities Requirements (UCR) 2013 specifies the technical requirements for certification of approved products to be used in DoD networks to provide end-to-end Unified Capabilities (UC). The UCR 2013 specifies the functional requirements, performance objectives, and technical specifications for products that support UC, and shall be used to support test, certification, acquisition, connection, and operation of these devices. It may be used also for UC product assessments and/or operational tests for emerging UC technology. The Defense Information Systems Agency (DISA) translates DoD Component functional requirements into engineering specifications for inclusion into the UCR, which identify the minimum requirements and features for UC applicable to the overall DoD community. The UCR also defines interoperability, Information Assurance (IA), and interface requirements among products that provide UC.
  http://disa.mil/ucco-files/UCR-2013-Change1-Main.pdf

- **Department of Defense (DoD) Unified Capabilities Framework 2013 (UC Framework 2013), Jan 2013.** The DoD Unified Capabilities Framework 2013 describes the technical framework for DoD networks that provide end-to-end (E2E) Unified Capabilities (UC). The UC Framework is one of the documents that make up the UCR Family of documents.
  http://www.disa.mil/~/media/Files/DISA/Services/UCCO/UCR2013/UC_Framework_2013_Combined.pdf

- **Unified Capabilities Approved Products List (UC APL) Process Guide, Version 2.3, December 2014**. The DoD Unified Capabilities (UC) Approved Products List (APL) process is developed in accordance with DoD Instruction (DoDI) 8100.04. The UC APL process is managed by the Defense Information Systems Agency (DISA) – Network Services (NS) Unified Capabilities Certification Office (UCCO) under the DISN Program Office (NSP). The UC APL is to be the single approving authority for all Military Departments (MILDEPs) and DoD agencies in the acquisition of communications equipment that is to be connected to the Defense Information Systems Network (DISN) as defined by the Unified Capabilities Requirements (UCR). In accordance with CJCSI 6211.02D, DISN Responsibilities, 24 January 2012, Enclosure B. Policy. Para 1.c. (4):

"CC/S/As shall procure or operate UC products listed on the DoD UC Approved Products List (APL), as applicable, unless granted an exception to policy IAW DoDI 8100.04." The UC APL process provides for an increased level of confidence through Information Assurance (IA) and Interoperability (IO) certification.
https://aplits.disa.mil/docs/aplprocessguide.pdf
http://www.disa.mil/network-services/ucco/policies-and-procedures

- **Joint Information Environment (JIE) Operations Concept of Operations (JIE Operations CONOPS), version 2.0.** (USE EMAIL CERTIFICATE). Increasingly DoD mission success depends on the ability of military commanders and civilian leaders to act quickly and effectively based on the most accurate and timely data available. In today's national security environment, it is imperative that DoD resolve barriers to trusted information sharing and collaboration, within the Department and with DOD's mission partners, to provide better access to information, and to enhance the nation's effectiveness to defend against cyber threats and vulnerabilities. The current DoD Information Technology (IT) environment is a complex layering of multiple networks with overlapping, duplicative roles and responsibilities. As stated by the Commander of CYBERCOM, the current network is "not defendable." For this reason, the DoD must move to an environment that will enable the Department's vision and strategy for United States military forces as they execute their assigned missions in all operational environments. The JIE effort will realign, restructure, and modernize how the DoD IT networks and systems are constructed, operated, and defended.
https://disa.deps.mil/ext/cop/ns-extranet/NS1/NS11/NS112/JIE/_layouts/WordViewer.aspx?id=/ext/cop/ns-extranet/NS1/NS11/NS112/JIE/Shared%20Documents/JIE%20Ops%20CONOPS%20v2-35.docx&DefaultItemOpen=1

- **Satellite Communications (SATCOM) Gateway Technical Architecture Description (TAD) for the Joint Information Environment (JIE) Version 3.0, Aug 13, 2015**. (Use email certificate). This Joint Information Environment (JIE) Satellite Communications (SATCOM) Gateway (J-SG) Technical Architecture Description (TAD) describes the functional architecture needed to deliver the necessary capabilities to Department of Defense (DOD), other government organizations, and authorized coalition partners worldwide. It serves as a follow on to the J-SG Element Description (ED) and a more detailed view of the elements making up the J-SG. In the larger JIE framework, a J-SG qualifies as a specific type of Joint Communications Node- Fixed (JCN-F). All J-SG sites are a JCN-F, but not all JCN-F sites are a J-SG.
https://disa.deps.mil/ext/cop/ns-extranet/NS1/NS11/NS112/JIE/_layouts/WordViewer.aspx?id=/ext/cop/ns-extranet/NS1/NS11/NS112/JIE/Shared%20Documents/JIE-SG%20TAD/Approved%20V3.0%20documents%20and%20DoDAF%20artifacts/(U)JIE_NNT_SATCOM_GW_TAD_Report_V3-0(U_FOUO).docx&DefaultItemOpen=1

- **The Department of Defense (DoD) Cyber Strategy, April 2015**. The May 2011 DoD Strategy for Operating in Cyberspace guided the Defense Department's cyber activities and operations in support of U.S. national interests over the last four years. This new strategy sets prioritized strategic goals and objectives for DoD's cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans. This strategy builds on previous decisions regarding DoD's Cyber Mission Force and cyber workforce development and provides new and specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf