CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

MANAGEMENT OF JOINT COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER (C4)/CYBER EDUCATION AND TRAINING PROGRAMS
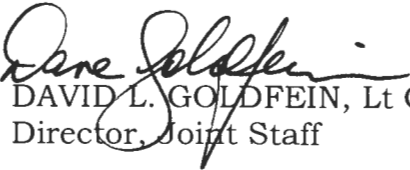
References: See Enclosure C.

1. <u>Purpose</u>. To publish policy for the management of Joint C4/cyber Education and Training programs. The Chairman of the Joint Chiefs of Staff authority is derived from title 10, United States Code (U.S.C.), section 153(a)(5)(C).

2. <u>Superseded/Cancellation</u>. CJCSI 6245.01, dated 28 May 2008, is hereby superseded.

3. <u>Applicability</u>. This instruction applies to the Joint Staff, Combatant Commands, Services, Defense agencies, National Defense University (NDU), Naval Postgraduate School (NPS) and the U.S. Army Signal Center of Excellence at Fort Gordon, GA.

4. <u>Policy</u>. See Enclosure A.

5. <u>Definitions</u>. See Glossary.

6. <u>Responsibilities</u>. See Enclosure B.

7. <u>Summary of Changes</u>. This instruction updates and institutionalizes policy, procedures, and guidance for joint C4/cyber education and training management and aligns defensive cyberspace operations (DCO) and the DoD Information Network Operations (DoDIN). This instruction also formalizes Department level decisions previously published in references a, b, c, d, and e as well as details how the J-6 will provide oversight of functional training as specified in reference e.

8. <u>Releasability</u>. This instruction is approved for public release; distribution is unlimited. DoD Components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page-- http://www.dtic.mil/cjcs_directives. Joint Staff activities may also access or obtain copies of this directive from the SIPRNET Directives Electronic Library.

9. <u>Effective Date</u>. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

DAVID L. GOLDFEIN, Lt Gen, USAF
Director, Joint Staff

Enclosures:

    A – Policy and Management
    B – Resources, Administration, Reporting
    C – References
    GL – Glossary

DISTRIBUTION

Distribution A, B, C, and JEL plus the following:

<div align="right">Copies</div>

Secretary of State... 2
Secretary of Defense... 2
Director of Central Intelligence 2
Commandant, U.S. Coast Guard 1
Commander, U.S. Forces Korea... 1
Commander, United States Fleet Forces Command 1
President, National Defense University 1
Commandant, Joint Forces Staff College 1
Commanding General, U.S. Army Signal Center of Excellence 1
Commandant, Naval War College 1
Commander, Air Force Doctrine Development and Education Center............ 1
Commanding General, Marine Corps Combat Development Command 1
Commander, U.S. Army Training and Doctrine Command 1
Chief, National Guard Bureau.. 1
Director, Joint Military Intelligence Training Center 1

OPR for the subject directive has chosen electronic distribution to the above organizations via e-mail. Those organizations with 2 copies listed will receive hard copy distribution. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPR and NIPR Joint Electronic Library Web sites.

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY AND MANAGEMENT

1. Background. Command and control (C2) of joint and multinational operations relies on the capability of the joint information environment (JIE). Within JIE, the DoDIN is the joint force commander's principal tool for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. Increases in combat capability afforded by DoDIN, ensures cyberspace capabilities are delivered through effective planning, employment, and defense by C4/cyber professionals. Management of joint C4/cyber education and training programs is necessary to ensure that C4/cyber professionals receive training that supports joint force objectives in cyberspace.

2. Policy. This directive augments reference f by providing additional guidance and direction for Joint C4/cyber education and training management. The guidance in this document applies to functional Joint C4/Cyber education and training. Professional Military Education and joint training policies are found in references f-m.

   a. Joint C4/cyber education and training curricula will be driven by data-centric principles, be based on relevant joint doctrine, and conform with approved joint concepts.

   b. Joint C4/cyber education and training programs will be structured to professionalize and expand the knowledge of operationally oriented C4/cyber personnel in planning and providing information assurance in joint and multinational operations.

   c. Joint C4/cyber training will emphasize current joint C4 priorities based on the final reports of the Joint Staff J-6 led biennial curriculum reviews or interim guidance published by the Military Communications-Electronics Board (MCEB).

   d. Joint C4/cyber education programs will use joint C4/cyber priorities and guidance published in the final reports of the Joint Staff J-6 led biennial curriculum reviews to create a foundation for graduates to think within the context of C4 and take decisive action in future assignments.

   e. Distributed Learning Content for Joint C4/Cyber Education and Training Programs. Joint C4/cyber distributed learning content for the

training and education programs under the purview of this instruction will comply with DoDIN data strategies, be managed using data-centric principles, and be indexed and advertised to promote visibility to the joint community.

3. Joint C4 Education Program

    a. Joint Command, Control, Communications, Computer, and Intelligence (C4I) Systems Master's Program Naval Postgraduate School (NPS), Monterey, CA. The Joint C4I curriculum is designed to meet broad educational objectives endorsed by the Joint Chiefs of Staff. The overall objective is to provide officers and DoD civilian equivalents, through graduate education, with a comprehensive understanding of the field of C4I systems as applied to joint and combined military operations. The program is designed with the following goals: enable individuals to develop an understanding of the C4I enterprise in the application of military power and the ability to interpret the impact of C4I on an operating philosophy; develop adequate background knowledge in basic C4I technology, human capabilities, and joint and coalition military operations; evaluate and apply these elements to create mission effects; and provide the framework whereby graduates can identify requirements and conduct analysis of current and emerging C4I systems. The requirements for a Master of Science degree are met through the specified educational skill requirements of the curricular program.

4. Joint C4 Training Programs

    a. The Joint Command, Control, Communications, Computer, and Intelligence/Cyber Staff and Operations Course (JC4ICSOC). The JC4ICSOC is hosted at the Joint Forces Staff College (JFSC), Norfolk, VA. The JC4ICSOC provides students with a broad understanding of joint C4I/cyber doctrine and current policy guidance. The program requires the application of joint C4I/cyber concepts, skills, and procedures to prepare the student for duty in joint or service C4I/cyber staff operations and planning assignments. This course provides a broad overview of Service C4I/cyber capabilities and trains students from varied functional backgrounds to function in a joint environment. Emphasis is balanced between the operational procedures associated with the C2 process and the management and operation of current joint C4I/cyber systems. The program covers the wide spectrum of C4I/cyber that extends from the national and strategic levels to the theater and tactical levels in support of the President, Secretary of Defense, and commanders who control military forces. The JC4ICSOC is for individuals from the defense establishment who are or will be assigned to positions requiring an understanding of C4I/cyber capabilities. The course exposes students to intelligence, operations, and communications capabilities of a joint staff. Individuals from varied backgrounds including officers, warrant officers, senior noncommissioned officers, DoD civilians, and cyber operators are educated to the perspectives represented by these various disciplines. Finally, the

JC4ICSOC students attending the TOP SECRET/Sensitive Compartmented Information-level course are afforded a National Capital Region orientation, which includes senior level engagement with the Joint Staff J-6, DISA, U.S.. Cyber Command, National Security Agency, National Relocation Office, Secret Service, National Military Command Center, and State Department Bureau of Intelligence and Research to gain insight into these agencies unique C4I/cyber capabilities and current issues. Specifically, the course focuses on the following learning areas in accordance with policy, guidance and doctrine specified in references n-v:

      (1) Joint Policy, Doctrine, and Strategy

      (2) Fundamentals to include: Legal, Intelligence, Space Operations, Spectrum, Electronic Warfare, Information Operations, and Cyberspace Operations.

      (3) Systems and Networks

      (4) C4I/Cyber Initiatives

      (5) National, Joint and Service Command and Control

      (6) Planning

      (7) Practical Exercise/Application

   b. <u>Joint Command, Control, Communications and Computer (C4) Planners Course (JC4PC)</u>. The JC4PC is hosted at the U.S. Army Signal Center of Excellence (USASCoE), Fort Gordon, GA. The JC4PC focuses on the technical planning and system engineering aspects of C4/Cyber in support of the crisis action planning process in a joint task force J-6 (communications) staff. The JC4PC maximizes use of standard joint C4 planning tools to prepare students to plan operations in the joint environment within a joint task force J-6. Instruction will ensure students have a strong foundation in joint C4/cyber fundamentals and an orientation to other joining planning fundamentals, such as the Joint Operational Planning Process (JOPP). The course culminates with the development of the required JOPP documents (Annex K, Architectural Diagrams) and other critical C4/cyber planning documents (COMSEC Callout, Joint Restricted Frequency List, Satellite Access Request/Gateway Access Request) necessary to plan a joint communications network in support of joint operations. In a scenario-based environment, students are taught to plan and manage the integration and interconnection of diverse types of joint and multi-national DoDIN capabilities into and interoperable joint information environment supporting joint and combined tactical operations. Students also learn techniques to design and engineer the overall network architecture to support battlefield user requirements, exercise network control, and conduct

recurring network analysis as well as the ability to employ sound techniques for operating in a joint information environment supporting cyberspace objectives. Emphasis is placed on the practical application of systems engineering principles to plan and manage joint information networks using fielded and future military and commercial off-the-shelf systems.

5. <u>Management Structure</u>. The Joint Staff J-6 will ensure that biennial curriculum reviews are conducted by a committee consisting of appropriate representatives from the Joint Staff, Services, Combatant Commands, and Defense agencies. Additionally, representatives from the Department of Defense, Chief Information Officer's (DoD CIO) staff, and NDU will be invited to participate. The final report will be submitted to the MCEB for ratification for each joint C4/cyber education and training course reviewed. The purpose of the joint C4/cyber curriculum review is to provide a forum to assist the course faculty and school administration with their mission; validate course requirements to ensure the course is relevant and in accordance with joint doctrine, emerging priorities, Combatant Command needs and CJCS priorities; and expose gaps and achieve balance in overall joint C4/cyber training and education.

ENCLOSURE B

RESOURCES, ADMINISTRATION, REPORTING

1. <u>Office of the Secretary of Defense</u>. In accordance with reference w, the Secretary of Defense funds professional development education operations of all components of the NDU, including the JFSC.

2. <u>Chairman of the Joint Chiefs of Staff</u>. In accordance with reference x, the Chairman is responsible for formulating policies for coordinating the military education and training of members of the Armed Forces.

3. <u>Joint Staff</u>. Assisting the Chairman, the Joint Staff is responsible for the following:[1]

    a. Assist Combatant Commands with review and coding of joint billets to be filled by joint C4/cyber education and training program graduates. (Joint Staff J-1; J-6)

    b. Function in an oversight capacity to ensure the joint C4/cyber education and training goals set by the Chairman are accomplished. (Joint Staff J-6 lead; J-7 support)

    c. Monitor all joint C4/cyber education and training programs to ensure they are consistent with current and evolving joint doctrine, procedures, and objectives. (Joint Staff J-6 lead; J-7 support)

    d. Ensure that biennial curriculum reviews are conducted for the JC4ICSOC, JC4PC, and JC4I Master's Program by representatives from the Joint Staff, Services, Combatant Commands, and Defense agencies. DoD CIO personnel and representatives from each school shall be invited to participate. The Joint Staff J-6 will chair the review committee. (Joint Staff J-6 lead; J-7 support)

    e. Joint C4/cyber training not reviewed in one of the formal curriculum reviews will be reviewed by participation in course boards, committees, or program of instruction reviews of those courses (e.g., spectrum training, Joint Multi-Tactical Data Link School courses). (Joint Staff J-6 lead; J-7 support)

---

[1] J-6 as the office of primary responsibility for joint C4/cyber is the lead for formulating vision, learning requirements, review processes, and assessment procedures of specific concern to the Joint C4 community. J-7 supports J-6 by assisting with the delivery of Joint C4 education to the joint community through the Military Education Coordination Council (MECC) and associated processes.

f. Review joint C4/cyber distributed learning content with the objective of ensuring that it is consistent with subparagraph 2.e., Enclosure A of this document. (Joint Staff J-6 lead; J-7 support)

4. Combatant Commands

    a. Review Combatant Command needs and schedule individual joint C4/cyber education and training as required. Ensure requisitions and billet coding specifies training en route.

    b. Review requirements for joint billets coded to be filled by joint C4/cyber education and training program graduates and ensure identified billets are annotated with the appropriate criteria.

    c. Ensure joint C4/cyber training for all training levels is included in joint training plans.

    d. Provide individuals with current joint C4/cyber experience to serve on curriculum training review committees.

    e. In accordance with reference y, Combatant Commands review their respective joint training programs and ensure joint C4/cyber education and training is incorporated to meet joint requirements.

5. Services

    a. Review Service joint training programs to ensure the National Guard/U.S. Coast Guard needs and schedule individual joint C4/cyber education and training as required. Services should ensure individuals assigned to joint duty receive appropriate joint training en route to joint assignment.

    b. Review requirements for billets coded or annotated to be filled by joint C4/cyber education and training program graduates.

    c. Provide individuals with current joint C4/cyber experience to serve on curriculum and training review committees.

    d. Ensure that information or school codes for joint course completion are recorded in individual training records.

    e. Consider Joint C4/cyber training and education incorporation in Service training and education.

6. Defense Agencies

    a. Review Defense agency needs and schedule individual joint C4/cyber education and training as required.

    b. Review requirements for billets coded or annotated to be filled by joint C4/cyber education and training program graduates.

    c. Provide individuals with expertise in technical matters and current joint C4/cyber experience to serve on curriculum and training review committees.

7. President, NPS

    a. Maintain a curriculum for respective courses consistent with Enclosure A of this directive.

    b. Schedule and market courses to ensure visibility of educational opportunities to potential students.

    c. Provide C4/cyber expertise and research for Combatant Commanders and Defense agencies as applicable.

    d. Ensure that joint school graduate information is provided to Services for recording in individual training records.

    e. Provide individuals with current joint C4/cyber experience to serve on curriculum and training review committees.

8. President, NDU and Commanding General, USASCoE

    a. Maintain a curriculum for respective courses consistent with Enclosure A of this directive.

    b. Schedule and market courses to ensure visibility of training opportunities to potential students.

    c. Conduct, where feasible, mobile training to joint forces.

    d. Provide C4/cyber expertise to deployed forces as applicable.

    e. Ensure that joint school graduate information is provided to Services for recording in student training records.

    f. Provide individuals with current joint C4/cyber experience to serve on curriculum and training review committees.

9. Administration, Personnel, and Finance

   a. Faculty. In order to ensure proper administration and instruction is conducted, the Services will continue to provide the commissioned officers, warrant officers, and enlisted personnel augmented by civilian personnel or contractor support where warranted, for the staff and faculty of the NPS, JC4ICSOC and the JC4PC.

      (1) Joint C4I Program, NPS

         (a) The joint C4 curricular officer is designated an Air Force lieutenant colonel billet. This officer ensures the graduate program is conducted in a manner consistent with joint objectives and incorporates current joint doctrine and practice.

         (b) The NPS shall assign two faculty members, one Army and one Air Force (preferably O-5s with C4 experience) to the Joint C4I Program. The Air Force faculty member will be in addition to the curricular officer.

      (2) JC4ICSOC, NDU (JFSC)

         (a) U.S. Navy

            1 Course Director

               a Rank/Grade: O-5 (Minimum O-5)

               b Designator: 1050

               c Subspecialty: 620X

               d AQD: JS8 (JPME Ph 1 & 2)

               e NOBC: 3265 (Adv C&S School Instructor)

            2 Course Instructor

               a Rank/Grade: O-4/O-5 (Minimum O-4)

               b Designator: 1020 (Recommend 1820)

               c Subspecialty: None

               d AQD: JS8 (JPME Ph 1 & 2)

<u>e</u> NOBC: 3265 (Adv C&S School Instructor)

(b) U.S. Army

<u>1</u> Instructor, Strategic and Tactical Communications Systems

<u>a</u> Rank/Grade: O-4/O-5

<u>b</u> Designator: code 25A, 26, 27

<u>2</u> Instructor, Information Systems

<u>a</u> Rank/Grade: O-4/O-5

<u>b</u> Designator: code 53A

(c) U.S. Air Force

<u>1</u> Instructor, Warning and Intelligence Systems

<u>a</u> Rank/Grade: O -4/ O -5

<u>b</u> AFSC: 12S, 13S, 14N, or 17D (preferred 13S). May be rated or nonrated.

<u>2</u> Instructor, Tactical Command and Control Systems

<u>a</u> Rank/Grade: O-4/O-5

<u>b</u> AFSCs: 11B, 11F, 12S, 13B, 13S, or 17D (preferred 17D) May be rated or non-rated. Qualifications: Previous duty in a Tactical Air Control System is highly desired; duty in joint tactical C4 activities is desirable.

(3) JC4PC: Manning in accordance with references c and d.

b. The temporary duty expenses for students attending the Joint C4I Program NPS, JC4ICSOC, or JC4PC will be borne by the individual's parent Service or sponsoring Defense organization.

c. The pay, allowance, subsistence, and permanent change of station costs for students, faculty, and staff will be borne by the individual's parent Service or sponsoring Defense agency.

d. The Navy, as executive agent, is responsible for programming, budgeting, and financing the Joint C4I Systems Master's Program at the NPS.

e. In accordance with references g and i, the Secretary of Defense provides funds for the JC4ICSOC through NDU.

f. In accordance with reference c, the Services will fair share split the funding for the JC4PC.

10. Selection and Assignment

a. Military Services are to stress the importance of joint C4/cyber education and training through the support of joint C4/cyber education and training programs for middle- and senior-grade personnel.

b. Personnel attending the JC4ICSOC should be assigned to or be en route to a joint C4/cyber billet or in a billet requiring knowledge of joint C4/cyber capabilities. Graduates of the JC4ICSOC will be identified in their appropriate Service training system as having completed the JC4ICSOC.

c. Graduates of the NPS curriculum will be identified by their appropriate Service training system as joint C4/cyber-qualified asset. Assignment of the graduate to a joint C4/cyber billet is highly recommended. However, if not possible, subsequent assignment to a Service C4/cyber billet is an acceptable alternative.

d. Graduates of the JC4PC will be identified in their appropriate Service training system as being certified joint C4 planners.

e. Combatant Commands will designate billets as needed which require assignment of joint C4 planner qualified personnel, graduates of the JC4PC, JC4ICSOC, and the NPS.

f. Services should consider recoding or annotating Service billets which, because of their potential to be called upon to make up a joint task force, would benefit from assignment of joint C4/cyber planner qualified personnel, graduates of the JC4PC, JC4ICSOC, and the NPS.

ENCLOSURE C

REFERENCES

a. MJCS 77-83, 8 November 1983, "Management of Joint Command, Control, and Communications Education and Training Programs"

b. MJCS 83-78, 23 March 1978, "Joint Command, Control, and Communications Staff and Operations Course"

c. JROCM 237-05, 1 November 2005, "Joint C4 Planners Course DOTMLPF Change Recommendation"

d. JROCM 023-08, 25 January 2008, "Joint C4 Planners Course DOTMLPF Change Instructor Manning Status"

e. CJCSI 3500.01 Series, "Joint Training Policy and Guidance for the Armed Forces of the United States"

f. CJCSI 1801.01 Series, "National Defense University Education Policy"

g. National Defense Authorization Act For Fiscal Year 2002, Section 527, Professional Development Education

h. CJCSM 3500.04 Series, "Universal Joint Task Manual"

i. CJCSI 1800.01 Series, "Officer Professional Military Education Policy (OPMEP)"

j. CJCSI 1805.01 Series, "Enlisted Professional Military Education Policy"

k. CJCSM 3500.03 Series, "Joint Training Manual for the Armed Forces of the United States"

l. CJCSI 5120.02 Series, "Joint Doctrine Development System"

m. CJCSI 6240.01 Series, "Responsibilities for the Joint Tactical Air Operations Interface Training Program"

n. CJCSM 3122.05 Series, "Joint Operation Planning and Execution System (JOPES) Information Systems Governance"

o. CJCSI 3320.03 Series, "Joint Communications Electronics Operating Instructions"

p. JP 2-0, Joint Intelligence

q. JP 3-0, Joint Operations

r. JP 3-12, Cyberspace Operations

s. JP 3-13, Information Operations

t. JP 3-16, Multinational Operations

u. JP 6-0, Joint Communications System

v. Unified Command Plan

w. Title 10, United States Code, section 2165

x. Title 10, United States Code, section 153

y. CJCSM 3150.07 Series, "Joint Reporting Structure Cyber Operating Status"

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

C2	command and control
C4	command, control, communications, and computer
C4I	command, control, communications, computer, and intelligence
COMSEC	communications security
DISA	Defense Information Systems Agency
DoD CIO	Department of Defense Chief Information Officer
J-1	Manpower and Personnel Directorate, Joint Staff
J-6	C4/Cyber Systems Directorate, Joint Staff
J-7	Joint Force Development Directorate, Joint Staff
JC4ICSOC	Joint C4I/Cyber Staff and Operations Course
JC4PC	Joint Command, Control, Communications, and Computer Planners Course
JFSC	Joint Forces Staff College
JIE	joint information environment
JOPP	Joint Operational Planning Process
MCEB	Military Communications/Electronics Board
MJCS	Memorandum Joint Chiefs of Staff
NDU	National Defense University
NPS	Naval Postgraduate School
NSA	National Security Agency
OSD	Office of the Secretary of Defense
USASCoE	U.S. Army Signal Center of Excellence

PART II – TERMS AND DEFINITIONS

cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructure and associated data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12, Cyberspace Operations)

defensive cyberspace operations. Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called DCO. (JP 3-12)

Department of Defense Information Networks. The globally, interconnected, end-to-end set of information capabilities, associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel including owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services, and national security systems. Also called DoDIN. (JP 3-12)

Department of Defense information networks operations. Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense network to create and preserve information assurance on the Department of Defense information network. (JP 3-12)

education. Education conveys general bodies of knowledge and develops habits of mind applicable to a broad spectrum of endeavors.

individual joint training. Training that prepares individuals to perform duties in joint organizations (e.g., specific staff positions or functions) or to operate uniquely joint systems. Individual staff training ensures that individuals know, are proficient in, and have the joint competencies and skills to apply joint doctrine and procedures necessary to function as staff members.

interagency. U.S. government agencies and departments, including the Department of Defense. (JP 3-08)

interagency coordination. Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged U.S. government agencies for the purpose of achieving an objective. (JP 3-0)

interagency training. Training of individuals, units, and staffs considered necessary to execute their assigned or anticipated missions in support of interagency operations.

joint information environment. JIE is a secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures or TTPs.

joint training. Training, including mission rehearsals, of individuals, units, and staffs using joint doctrine or joint tactics, techniques, and procedures to prepare joint forces or joint staffs to respond to strategic, operational, or tactical requirements considered necessary by the Combatant Commanders to execute their assigned or anticipated missions.

multinational training. Training of individuals, units, and staffs considered necessary to execute their assigned or anticipated missions in support of multinational operations, including coalition operations.

Service training. Military training based on Service policy and doctrine to prepare individuals and interoperable units to execute their assigned or anticipated missions. Service training includes basic, technical, operational, and interoperability training in response to operational requirements deemed necessary by the Combatant Commands to execute assigned missions.

training. Instruction and applied exercises for acquiring and retaining skills, knowledge and attributes required to complete specific tasks. The focus of training is on the instruction of personnel to enhance their capacity to perform specific functions and tasks.

(INTENTIONALLY BLANK)