~~SECRET~~

USCYBERCOM

CONTINUITY OF OPERATIONS (COOP) PLAN (U)

DATE: 1 March 2017

USCYBERCOM
9800 SAVAGE ROAD
FORT GEORGE G. MEADE, MD 20755

Classified By: (b)(3)
Derived From: USCYBERCOM Classificaton Guide
Dated: 20150415
Declassify On: 20400416

~~SECRET~~

(INTENTIONALLY BLANK)

USCYBERCOM
9800 Savage Road
Fort George G. Meade, MD 20755

Reply ZIP Code: 20755 1 March 2017

MEMORANDUM FOR: Distribution List

SUBJECT: USCYBERCOM CONTINUITY OPERATIONS (COOP) PLAN for USCYBERCOM (S)

1. (U) This USCYBERCOM Continuity of Operations Plan provides the details for USCYBERCOM efforts to satisfy the DOD 3020.26 "Department of Defense Continuity Programs" requirement for all DOD Components (USCYBERCOM) to develop, coordinate, and maintain continuity plans.

2. (U) The USCYBERCOM COOP Plan is effective for planning purposes upon receipt and for expansion into an Operations Order (OPORD) when directed.

3. (U) The USCYBERCOM COOP Plan was coordinated with USCYBERCOM Components, USSTRATCOM Headquarters staff, and the Joint Staff.

4. (U) Forward any recommended changes to USCYBERCOM J3, 9800 Savage Road, Fort George G. Meade, MD 20755.

FOR THE COMMANDER

STEPHEN G. FOGARTY
Major General, USA
Chief of Staff

Encl
USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (S)
USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN ANNEX C (S)

(INTENTIONALLY BLANK)

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX
RECORD OF CHANGES

In the event the issuing authority distributes changes to this plan, ensure the changes are made and recorded in the table below.

Change Number/ Message DTG	Posted Date	Effective Date	Printed Name/ Signature of Change Verifier

(INTENTIONALLY BLANK)

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (U)
SECURITY INSTRUCTIONS

1. (U) The long title of this plan is "Continuity of Operations Plan for United States Cyber Command (U)." The short title is "USCYBERCOM COOP Plan (U)." Both titles are UNCLASSIFIED.

2. (U) The overall classification of this document is SECRET. Pages are classified SECRET to protect information classified at that level or the compilation of sensitive (but not necessarily classified) individual entries which, when aggregated, may convey information of a classified nature.

3. (U) Reproducing, extracting, and/or paraphrasing in whole or in part is authorized only when necessary to satisfy military requirements, provided the original classification of the affected portion is maintained. The distribution of this plan, or portions thereof, is restricted to those agencies and personnel whose duties specifically require knowledge of the contents.

4. (U) This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, United States Code, sections 793 and 794. The law prohibits the transmission or revelation of information contained within the document to unauthorized personnel.

(INTENTIONALLY BLANK)

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (U)

TABLE OF CONTENTS

CONTENTS PAGE

FIGURES PAGE

TABLES PAGE

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX
SUMMARY (U)

1. (U) PURPOSE. The USCYBERCOM COOP Plan provides the Commander of USCYBERCOM the means to continue USCYBERCOM Mission Essential Functions (MEFs) during national security emergencies or when normal operations conditions have been impaired or made impossible. This plan fulfills the requirement provided by National Security Presidential Directive (NSPD)-51 and DODD 3020.26 which stipulate the requirements for both a comprehensive continuity program and plan development, respectively. This plan will update perishable information as needed.

a. (U) Support National and DOD policy directives.

b. (U) Implement Secretary of Defense (SecDef) and Chairman of the Joint Chiefs of Staff (CJCS) directives.

c. (U) Detail the concept of operations.

d. (U) Define the decision authority for execution.

e. (U) Describe conditions for implementation.

f. (U) Identify execution criteria.

g. (U) Identify primary COOP functions, procedures, and capabilities required to execute those functions.

h. (U) Define a minimum level of readiness.

i. (U) Assign responsibilities to the USCYBERCOM Staff, and USCYBERCOM Military Service and Functional Components.

j. (U) Provide planning capabilities necessary to perform MEFs during national security emergencies or other emergencies that affect the ability to execute the USCYBERCOM mission.

k. (U) Provide guidance to reconstitute the positions of CDRUSCYBERCOM and personnel assigned to USCYBERCOM, to include active duty military, DOD civilian, and contractors as appropriate .

2. (U) APPLICABILITY. This plan is effective upon receipt and applies to all personnel assigned to USCYBERCOM.

3. (U) POLICY. USCYBERCOM will ensure continuous operations of USCYBERCOM's Mission Essential Functions (MEFs) according to National and DOD Policy referring to Continuity of Operations.

a. (U) An identifiable command authority.

b. (U) A surviving USCYBERCOM staff, able to accomplish USCYBERCOM MEFs and adequate to task and manage MEFs accomplishment.

c. (U) A secure, survivable, and redundant operational communications system with access (receive and transmit) to all appropriate data and voice communication systems.

d. (U) MISSION. On order, CDRUSCYBERCOM and designated elements of the Command relocate as part of a USG-wide continuity of operations (COOP) program in order to ensure the Command maintains the ability to perform all Unified Command Plan-directed missions and responsibilities in times of peace, crisis, or conflict.

e. ~~(C)~~ Commander's Intent. USCYBERCOM will be prepared to conduct COOP to ensure continuous operations of USCYBERCOM's MEFs, with or without warning, in a manner that insures seamless C2 of global cyberspace operations and uninterrupted support to Combatant Commands, Services and Agencies in accordance with the standards specified in this plan for a (b)(1) Sec 1.4(a) This will be accomplished through the Command Relocation Group (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(1) (U//~~FOUO~~) Purpose. USCYBERCOM remains able to accomplish MEFs in the event that relocation from the (b)(1) Sec 1.7(e) is ordered, anticipated, or necessary.

(2) (U//~~FOUO~~) Method. Alert and deploy Command Relocation Group personnel to select COOP site(s). Personnel will stand up selected USCYBERCOM COOP sites and commence cyberspace operations in support of USCYBERCOM MEFs.

(3) (U//~~FOUO~~) End State. USCYBERCOM maintain continuous operations at the USCYBERCOM COOP site(s) until operations resume in the (b)(1) Sec 1.7(e) or a follow-on plan has been approved by the Commander.

4. (U) MISSION ESSENTIAL FUNCTIONS (MEFs). Certain USCYBERCOM functions have been identified as Mission Essential Functions for the purpose of this plan. Interruption or loss of these functions will have serious impact within days of interruption. MEFs are the most critical tasks associated with the success of USCYBERCOM's operational mission. See APPENDIX XX to

ANNEX C, "OPERATIONS."

5. (U) ESSENTIAL ELEMENTS OF INFORMATION (EEI). The USCYBERCOM COOP Plan execution is based on an assessment of the potential magnitude of the threat, duration of the threat or attack, potential for facility loss, and readiness concerns.

a. (U) Is there a credible threat to continuous operations or key personnel?

b. (U) How specific and/or imminent is the threat? How much available warning time exists to execute COOP plans and relocate operations?

c. (U) How grave are the potential consequences of the threat?

d. ~~(S)~~ Is there a (b)(1) Sec 1.4(a) at USCYBERCOM HQ?

e. ~~(S)~~ Given the threat, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) remain in place or relocate to another location?

f. ~~(S)~~ Is clandestine (b)(1) Sec 1.4(a)

6. (U) CONCEPT OF OPERATIONS.

a. ~~(S)~~ Purpose. This plan is designed to increase the survivability of essential USCYBERCOM personnel and provide flexible MEFs execution during the pre-, trans-, and post-event phases of a COOP contingency. Survivability and continuity are accomplished (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) IAW the DODD 3020.26.

b. (U) The Concept of Operation supports:

(1) ~~(S)~~ The continuous tailoring of the Command Relocation Group (b)(1) Sec 1.4(a) to meet existing threat conditions.

(2) ~~(S)~~ The relocation of Command Relocation Group (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to the USCYBERCOM COOP sites commensurate with the size, skills, and ranks necessary to support the USCYBERCOM Staff and provide support to the MEFs restoration operations.

(3) ~~(C)~~ USCYBERCOM's COOP plan for devolment (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) is currently being coordinated (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) for COOP space so that mission essential personnel (b)(1) Sec 1.4(a)

(4) (U) Phase 3 Post-Event (Reconstitution). The USCYBERCOM Staff reconstitutes, using surviving USCYBERCOM personnel and, if required, personnel from the Military Services, and USCYBERCOM Subordinate Component Commands. Should the USCYBERCOM HQ (b)(7)(e) (b)(7)(e) not be functional, the USCYBERCOM Staff will reconstitute at a location designated by the acting CDRUSCYBERCOM. See APPENDIX XX, "STAFF RECONSTITUTION," to ANNEX C, "OPERATIONS."

7. (U) CONDITIONS FOR EXECUTION. A decision to execute any portion of the USCYBERCOM COOP may occur during duty and non-duty hours, with little or no warning. COOP execution is explained in detail in ANNEX C Paragraph 3.

8. ~~(S)~~ EXECUTION AUTHORITY. Execution of aspects of this plan requires consultation with and approval by the Commander, USCYBERCOM, his representative, or higher authority. The Director of Operations (USCYBERCOM (b)(1) Sec 1.4(a)

9. (U) TIME TO COMMENCE EFFECTIVE OPERATIONS. See "BASE PLAN," Paragraph 3 Execution, "PLANNING FACTORS."

10. (U) KEY ASSUMPTION AND THREATS.

a. ~~(S)~~ Threats to operations of the USCYBERCOM (b)(1) Sec 1.4(a) facilities range from natural disasters and infrastructure failures to terrorist attacks and attacks during times of war. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) highly visible symbols of the United States, to include government facilities such as USCYBERCOM (b)(1) Sec 1.4(a) Possible threats to USCYBERCOM (b)(1) Sec 1.4(a) operations include, but are not limited to:

(1) (U) Natural disaster (e.g. earthquake, hurricane)

(2) (U) Manmade disaster or emergency (e.g. accidental disruption, and/or cyber attack)

(3) (U) Technological emergency (e.g. Power failure, fire)

(4) (U) Acts of terrorism involving attacks utilizing conventional, nuclear,

biological, and chemical materials weapons, as well as conventional or cyber attacks on (b)(7)(e)

b. (U) Unconventional. Coordinated military attack on the United States involving conventional, nuclear, biological, chemical materials and/or weapons.

11. (U) OPERATIONAL CONSTRAINTS.

a. ~~(S)~~ The overall number of personnel relocating (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) the relocation site.

b. ~~(S)~~ The command must retain the ability (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) during all phases of the plan execution.

c. ~~(C)~~ Nuclear, biological, or chemical attack directed at USCYBERCOM (b)(1) Sec 1.4(a)

d. ~~(C)~~ (b)(1) Sec 1.4(a) relocation and/or reconstitution efforts.

e. ~~(C)~~ During relocation, the group may encounter (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to the designated relocation points.

f. (U) The relocation and reconstitution of designated personnel may not be (b)(7)(e) (b)(7)(e) to perform the MEFs functions.

12. (U) COMMAND RELATIONSHIPS. Command relationships remain the same as prior to plan implementation. Successions of command lines for command of USCYBERCOM are outlined in ANNEX J. USCYBERCOM may elect to reconstitute at any location possessing the capability to support requirements.

13. (U) TASKS. See USCYBERCOM COOP BASE Plan, "COORDINATING INSTRUCTIONS".

14. (U) COMMUNICATION APPRAISAL. See ANNEX K, "COMMUNICATIONS AND INFORMATION."

15. (U) LOGISTICS APPRAISAL. The logistics appraisal of this plan focuses on the three essential elements of logistical assessments: feasibility; supportability; and sustainability. The assessment analysis considers core capabilities in terms of critical items, limitations, logistics, outsourcing, and threats to logistic capabilities prior to and during a COOP event. The

assessment also highlights deficiencies or gaps and any associated risks; it proposes mitigation strategies to reduce or contain identified risks. COOP support is dependent upon the determination of alternate locations/sites and flexibility for the delivery of services and support. See ANNEX D, "LOGISTICS AND SUSTAINMENT" for execution procedures for logistics support to COOP.

16. (U) PERSONNEL APPRAISAL.

a. (U) There are currently enough USCYBERCOM personnel to meet requirements. There is the potential that an event could occur where a significant number of personnel (b)(7)(e) (b)(7)(e)

b. ~~(S)~~ Personnel requirements and processes to achieve rapid reconstitution of USCYBERCOM (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c. ~~(S)~~ Personnel assigned to the Command Relocation Group (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) shall be trained, qualified, certified, and exercised to ensure readiness to execute assigned MEFs, to include operations supporting USCYBERCOM, under all conditions.

OFFICIAL

<F. M. LNAME>
RANK, SERVICE
POSITION, J-3

(INTENTIONALLY BLANK)

USCYBERCOM CONTINUITY OF OPERATIONS (COOP) PLAN 20XX (U)
BASE PLAN (U)

(U) REFERENCES.

a. (U) National Security Presidential Directive 51 (NSPD 51) / Homeland Security Presidential Directive 20 (HSPD 20), National Continuity Policy, 9 May 07 (U)

b. (U) Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Programs and Requirements, Oct 12 (U)

c. (U) Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Function and Primary Mission Essential Function and Identification and Submission Process, Feb 08 (U)

d. (U) DOD Directive 3020.26, Department of Defense Continuity Programs, 9 Jan 09 (U)

e. (U) DOD Directive 3020.26P, Secretary of Defense Continuity of Operations Plan, 21 Mar 07 (S)

f. (U) DOD Instruction 3020.42, Defense Continuity Plan Development, 27 Apr 11 (U)

g. (U) Chairman of the Joint Chiefs of Staff Operation Order 3-12, Continuity of Operations (COOP) for the Chairman of the Joint Chiefs of Staff, 30 Nov 12 (S)

h. (U) National Continuity Policy Implementation Plan, 27 Sep 07 (U)

i. (U) Department of Defense Implementation of National Continuity Policy, 18 Jan 12 (TS)

j. (U) Department of Defense Directive 7730.65, Defense Readiness Reporting System (DRRS), 11 May 15 (U)

k. (U) National Terrorist Advisory System Public Guide, DHS website (U)

l. (U) USSTRATCOM Continuity of Operation (COOP), 1 August 2014 (S)

1. (U) Situation.

a. (U) General. Crises may occur that negatively affect or prevent

operations from continuing in USCYBERCOM facilities. The USCYBERCOM Continuity of Operations Plan (USCYBERCOM COOP Plan) describes the processes and steps in order to continue Mission Essential Functions (MEFs) without unacceptable interruption during a national security emergency. National security emergencies are any occurrence of disruptive conditions that seriously degrade or threaten the national security of the United States. In addition, the USCYBERCOM COOP Plan provides for the timely and orderly devolvement, relocation and/or reconstitution of key staff during an emergency or other event affecting the ability to execute the USCYBERCOM mission from current facilities. Consideration is given to executing relocation of MEFs as a precautionary measure. This will be performed by the Command Relocation Group: (b)(7)(e) as determined by the situation.

b. (U) Enemy. See ANNEX B, "THREATS AND INTELLIGENCE," and current intelligence reports as appropriate.

(1) (U//~~FOUO~~) Threat. Threats to operations of the USCYBERCOM range from natural disasters to terrorist attacks and attacks during times of war. The following threats to USCYBERCOM will meet the threshold for executing COOP.

(a) (U//~~FOUO~~) Natural Disaster

(b) (U//~~FOUO~~) Manmade disaster or emergency

(c) (U//~~FOUO~~) Technological emergency

(d) (U//~~FOUO~~) Acts of terrorism involving Chemical, Biological, Radiological, Nuclear, or High-yield Explosive (CBRNE) materials

(e) (U//~~FOUO~~) Coordinated military attack on the UNITED States involving conventional, nuclear, biological, or chemical materials or weapons.

(2) (U//~~FOUO~~) Intelligence Operations. USCYBERCOM J2 will be responsible for providing and/or coordinating all intelligence required by the commander, staff judge advocate, staff planners, operators to plan and execute all assigned missions. It is the details of the assigned cyberspace operations mission that drive the details of the J2 organization and processes, which are briefly explained below.

c. (U) Friendly. U.S. forces and other components identified by current operations report.

d. (U) Facts.

(1) ~~(C)~~ USCYBERCOM Headquarters Facility, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) variety of threats that may interrupt essential operations and functions.

(2) (U) Enemy forces are capable of launching attacks against Fort Meade, MD and other major US military facilities with little or no advanced warning.

(3) (U) This COOP Plan is executable with or without warning, during duty or non-duty hours.

(4) Emergency funding will be made available to facilitate COOP.

(5) There will be situational event-driven disruption to normal operations.

e. (U) Assumptions.

(1) ~~(C)~~ USCYBERCOM may receive (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) ~~(C)~~ (b)(1) Sec 1.4(a) to and from local COOP sites.

(3) ~~(C)~~ (b)(1) Sec 1.4(a) COOP sites will be available.

(4) ~~(C)~~ (b)(1) Sec 1.4(a) can be modified as required if (b)(1) Sec 1.4(a) determined to be mission essential and subject to COOP.

(5) ~~(C)~~ Command Relocation Group: (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) capable of performing the functions of the USCYBERCOM MEFs.

(6) ~~(C)~~ The COOP site(s) (b)(1) Sec 1.4(a) support and logistics for the Command Relocation Group.

(7) ~~(C)~~ The COOP site(s) (b)(1) Sec 1.4(a) supporting the Command Relocation Group in its performance of the USCYBERCOM MEFs.

(8) ~~(C)~~ USCYBERCOM (b)(1) Sec 1.4(a) will function during COOP and will be accessible by USCYBERCOM from the COOP site(s).

(9) ~~(C)~~ USCYBERCOM remains in communication with higher headquarters, (b)(1) Sec 1.4(a) Combatant Commands (CCMDs), Services, and Agencies at the COOP site(s).

(10) (~~C~~) All designated USCYBERCOM personnel (b)(1) Sec 1.4(a) site(s).

(11) (~~C~~) Non-COOP personnel (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) planned and directed.

(12) (~~C~~) The (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) full range of natural and/or man made disasters and may require devolvement and/or relocation to alternate facilities to perform the USCYBERCOM MEFs.

(13) (~~C~~) The Commander USCYBERCOM (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as long as possible.

(14) (~~C~~) USCYBERCOM will retain (b)(1) Sec 1.4(a) authorities.

f. (U) Planning Factors.

(1) (U) Purpose. This plan is executable in both a "with warning" and "no-warning" scenario, during duty or non-duty hours. For the USCYBERCOM COOP Plan, duty hours are considered to be (b)(7)(e) hours Eastern Time, Monday–Friday except federal holidays.

(2) (U) Staffing Considerations. The rank, skill sets, and number of personnel assigned to the Command Relocation Group are determined by space limitations and MEFs to be performed. Due to these space limitations, the Command Relocation Group by necessity represents a fraction of the full USCYBERCOM staff. To meet these staffing limitations and in order to support the MEFs, the USCYBERCOM directorates will prioritize their directorate functions and select the most knowledgeable and experienced personnel for assignment to the Command Relocation Group. The assignments for USCYBERCOM directorates are provided in APPENDIX 1, "COMMAND RELOCATION GROUP ORGANIZATION," to ANNEX A, "TASK ORGANIZATION."

(3) (U) Essential Elements of Information. USCYBERCOM COOP Plan execution is contingent on an assessment of the potential magnitude of the threat, duration of the threat or attack, potential for facility loss, and readiness concerns.

(a) (U) Is there a credible threat to continuous operations or key personnel?

(b) (U) How specific and/or imminent is the threat? How much available warning time exists to execute COOP plans and relocate operations?

(c) (U) How grave are the potential consequences of the threat?

(d) (~~S~~) Is (b)(1) Sec 1.4(a) USCYBERCOM HQ?

(e) (~~S~~) Given the threat, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) relocate to another location?

(f) (~~S~~) (b)(1) Sec 1.4(a) not to cause additional unrest within the community?

2. (~~S~~) Mission. On order, CDRUSCYBERCOM and designated elements of the Command (b)(1) Sec 1.4(a) program in order to ensure the Command maintains the ability to perform all Unified Command Plan-directed missions and responsibilities in times of peace, crisis, or conflict.

a. (U) MEFs. The MEFs and tasks are discussed in APPENDIX XX "MISSION ESSENTIAL FUNCTIONS," to ANNEX C, "OPERATIONS."

3. (U) Execution. This plan is designed to increase the survivability of essential USCYBERCOM personnel to enable flexible MEF execution during the pre-, trans-, and post-event phases of a COOP contingency. Survivability and continuity are accomplished (b)(7)(e) (b)(7)(e) while maintaining the ability to perform succession.

a. (~~S~~) COOP Concept of Operations. Personnel will relocate to one of the USCYBERCOM COOP locations (Command Relocation Group: (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as determined by the situation. Alternate or additional sites may be used if available at implementation. USCYBERCOM COOP execution (b)(1) Sec 1.4(a)

b. (U) Execution Authority. Execution aspects of this plan requires consultation with, and approval by, the Commander, USCYBERCOM, his representative, or higher authority. The Director of Operations (USCYBERCOM J3) is responsible for the execution of this plan.

c. (U) Conditions for Execution. The following conditions may cause execution of USCYBERCOM COOP. This plan is designed to support continuity of operations given war, terrorist attack, natural or technological disaster, or at the direction of the President or Secretary of Defense. These conditions may occur during duty and non-duty hours, with or without warning, and may cause disruptions to normal USCYBERCOM operations.

(1) (U) War conditions. Conditions may exist when the United States is engaged in hostilities against another country. The hostilities may or may not be conducted under a formal declaration.

(2) (U) Terrorist Attacks. Attacks may be executed by a foreign national

or U.S. citizen and are characterized by a deliberate, planned effort to attack key infrastructure USCYBERCOM relies on.

(3) (U) Natural and Technological Disasters. Any number of events may require a partial or total administrative and operational relocation to an alternate site. Factors for initiating relocation include, but are not limited to: hurricanes, fire, toxic emissions, earthquake, hazardous nuclear power plant emissions, sewer or power failures, contamination of water sources, health hazards, structural instability, or other disruptions to operations during which USCYBERCOM or USCYBERCOM facilities, are rendered unusable for normal operations.

(4) (U) By Direction. Commander, USCYBERCOM or his designated representative will activate all or specific portion(s) of this plan.

d. (U) Operations to be conducted.

(1) (U) COOP Phases. Since the exact nature, timing, or extent of a crisis cannot be precisely determined in advance, this directive outlines flexible options that can be adapted to any crisis situation. COOP planning and execution span four phases: Phase 0 – Pre-event, Phase 1 – Trans-event, Phase 2 – Continuity Operations, and Phase 3 – Post-event.

(a) ~~(S)~~ Phase 0 - Pre-Event Phase (Readiness and Preparedness). This phase consists of all tasks accomplished prior to execution of COOP plans. Actions are taken to decide, prepare, coordinate, and train to readiness standards. Plans and actions are coordinated, reviewed and staffed. In addition, timely alert, notification, coordination, and decision-making exercises are conducted to prepare personnel for a COOP event. USCYBERCOM J3 is the catalyst for pre-event activities. During this phase, consideration is given to phasing the relocation of personnel and resources to a USCYBERCOM COOP site. To reduce the vulnerability of the staff to a surprise attack or terrorist activity, the decision to relocate (b)(1) Sec 1.4(a) personnel significantly minimizes the (b)(1) Sec 1.4(a) of a (b)(1) Sec 1.4(a) This phase ends with (b)(1) Sec 1.4(a) event requiring COOP to be activated.

(b) ~~(S)~~ Phase 1 - Trans-Event Phase (Activation and Relocation) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This phase commences with identification of a threat or event that may require a COOP response (b)(1) Sec 1.4(a) Actions are taken to decide, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) are critical during this phase. Notification of senior leaders is completed, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Succession to command decisions (b)(1) Sec 1.4(a) if necessary, the temporary

(b)(1) Sec 1.4(a) Actions in this phase enable (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This phase ends upon (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (~~S~~) Phase 2 – Continuity Operations. During this phase, the (b)(1) Sec 1.4(a) for a (b)(1) Sec 1.4(a) leadership, directorate, and / or component leads will assist in coordinating and sustaining deployed staff requirements. During this phase, decision-makers will assess the impact of the event and determine the duration of operations from an alternate site(s). Actions include managing communications, logistics, transportation, personnel augmentation and rotation, as well as site and / or platform activities. This phase ends when planning is completed for the return (recovery) of deployed personnel, their functions, and C2 to a permanent site, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (~~S~~) Phase 3 - Post-Event (Reconstitution). During this phase, plans may be implemented for the return (recovery) of the MEFs, their functions, and C2 to a permanent operating location, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Decision-makers will continue to assess the impact of the event and any emerging threats and determine the duration of conducting operations from alternate operating facilities. This concept of operations recognizes the need to function for a (b)(1) Sec 1.4(a) During this (b)(1) Sec 1.4(a) reconstitution actions will interlace with the operational performance of the MEFs. An estimate of the level and duration of the incident that required COOP plan implementation will be based on, but not limited to, the type and continued existence of threats, the severity of the damage, the ability to reconstitute the full staff, and the reliability of communications. If facilities are not available, they will, in turn contact other local bases, federal facilities, or begin searching for other real estate options to support the Command (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Depending on the amount of HQ Staff affected, CDRUSCYBERCOM or his designated representative can select directorates/special staff to relocate based on a given priority for the situation. While Phase 1 and 2 activities may be of short duration, Phase 3 activities may continue for an extended period of time. This phase ends when the USCYBERCOM Commander or his/her designated representative determines whether to reconstitute at the HQs facility (if conditions permit) or at an alternate site.

(2) (U) COOP Tiers. COOP implementation and mission offset revolve around a five-tiered concept of response based on the magnitude of the threat or impact of an actual event. While specific responses are associated with each of these five tiers for planning purposes, this is not intended to restrict the Commander's flexibility to respond to an actual situation using the best available means. The nature and scope of the emergency will dictate the appropriate response to any situation.

(a) ~~(S)~~ Tier 1 USCYBERCOM HQs Impaired. USCYBERCOM HQs in the (b)(1) Sec 1.4(a) has sustained some damage and parts are unusable such as localized flooding, fire, or structural damage (example: Virginia Earth Quake 2012). Individual directorates may be affected, but the HQs is still usable in some areas. The command will relocate and use unaffected areas within the HQs. In addition, personnel and functions may relocate to local COOP facilities in accordance with (IAW) directorate / component plans or as directed by the command. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) may have to execute their COOP Plan. Some personnel may be directed to go home and wait for further instructions.

(b) ~~(S)~~ Tier 2 HQs Unusable. Event renders USCYBERCOM HQ - (b)(1) Sec 1.4(a) completely unusable (example: Hurricane, Fire or Terrorist Attack). If USCYBERCOM is not able to perform MEFs and supporting tasks then CDR USCYBERCOM or his designed representative will determine if a devolment and/or transition of MEFs and supporting tasks to subordinate commands with augmentation considered. Sites will be determined based on the extent of damage and/or the impact resulting from events. This will also determine the decision for COOP. Affected personnel will relocate to COOP facilities IAW COOP or command guidance.

(c) ~~(S)~~ Tier 3 Installation Inaccessible. The threat or event renders USCYBERCOM - (b)(1) Sec 1.4(a) inaccessible and unusable (example: Chlorine release or Hurricane damage). All MEFs, and supporting tasks will be transitioned to alternate and / or COOP operating facilities. The transition of MEFs, and supporting tasks to subordinate commands with the level of augmentation considered. Sites will be coordinated with COOP plan development IOT achieve a successful relocation of selected missions, operations and personnel. Affected personnel will relocate to designated COOP facilities IAW directorate guidance or as directed by the command.

(d) ~~(S)~~ Tier 4 USCYBERCOM area (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) The MEFs, and supporting tasks will be

transitioned and performed as appropriate at the designated COOP facilities. The transition of MEFs, and support tasks to subordinate commands with augmentation will be considered. Sites will be determined based on the extent of damage and impact resulting from events requiring COOP. Affected personnel will relocate to COOP facilities IAW directorate guidance or as directed by the command.

(e) ~~(S)~~ Tier 5 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The MEFs will be transitioned as appropriate to the COOP site(s) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The transfer of MEFs and supporting tasks to subordinate commands with augmentation will be considered. (b)(1) Sec 1.4(a) and coordinated (b)(1) Sec 1.4(a) IAW directorate or as directed by the command.

e. (U) Tasks.

(1) (U) All Directorates and Subordinate Commands.

(a) (U) Support USCYBERCOM J3 efforts to revise and maintain COOP Plan IAW DOD guidelines.

(b) (U) Participate in COOP Working Group (CWG) meetings.

(c) (U) With or without notice, be prepared to (BPT) execute the command COOP in order to be operational (b)(7)(e) or as specified in each individual MEF, after disruption by any event across the spectrum of (b)(7)(e) Units geographically separated from USCYBERCOM Headquarters (b)(7)(e) will independently execute COOP plans, as required, in response to events in their respective geographic locations.

(d) (U) BPT maintain contact with all personnel not included in the COOP for follow on orders and accountability.

(e) (U) Conduct biennial reviews:

1. (U) This Plan and respective Annex's, Appendixes, Tabs, and Exhibits.

2. (U) Coordinate or validate MOUs and/or MOAs with relocation facility hosts. This includes internal coordination with J3 approval for use of a distant relocation facility.

(f) (U) Annually provide COOP training to personnel, and within the first (b)(7)(e) new employee's arrival. Training will include (but not be limited to) the following:

1. (U) Emergency evacuation procedures.

2. (U) Directorate specific COOP responsibilities and actions.

3. (U) Recall procedures; update recall rosters as needed.

(g) (U) (b)(7)(e) (or more frequently, as required), update and maintain MEFs.

(h) (U) Advise all MEF Personnel to develop/review/update family plans and emergency data forms. Continue to maintain / update MEF Personnel Rosters as needed.

(i) (U) Participate in Exercise COOP events (b)(7)(e) as directed in order to:

1. (U) Validate current COOP actions and procedures.

2. (U) Verify required IT and communications capability, connectivity, accesses and collaboration tools at alternate locations.

3. (U) Train and exercise personnel on COOP actions, procedures and capabilities at the relocation sites.

(j) (U) Assign and maintain COOP POCs IAW the COOP Working Group (CWG) Charter.

(k) ~~(S)~~ Test COOP (b)(1) Sec 1.4(a) procedures.

(2) (U) USCYBERCOM Directorates.

(a) (U) The USCYBERCOM Chief of Staff will: BPT stand-up the (b)(7)(e)

(b) (U) Director USCYBERCOM J1 will: Provide required personnel, establish programs, and support the execution of this plan. Additional information is provided in Annex E.

(c) (U) Director USCYBERCOM J2 will: Provide CDRUSCYBERCOM and the Joint Operations Center (JOC) with COOP planning related intelligence situational awareness to include strategic and tactical indications and warning of threats to continuous USCYBERCOM operations.

(d) (U) Director USCYBERCOM J3 will:

1. (U) Be (Office of Primary Responsibility (OPR) for the USCYBERCOM COOP program.

2. (U) Maintain and update this plan as required.

3. (U) Provide all command personnel with an annual COOP awareness briefing.

4. (U) Ensure execution of J3 MEF's during COOP execution as described in ANNEX C.

(e) (U) Director USCYBERCOM J4 will:

1. (U) BPT Support the redeployment/movement of personnel to and from distributive locations.

2. (U) BPT to initiate 24 hour operations as needed.

3. (U) Provide logistics support in accordance with Annex D.

(f) (U) Director USCYBERCOM J5 will: BPT execute applicable parts of the COOP.

(g) (U) Director USCYBERCOM Capabilities Development Group (CDG) will:

1. ~~(S)~~ Develop and maintain a plan (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2. (U) BPT execute directorate COOP.

3. ~~(S)~~ Provide updates on (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) survivability and redundancy.

(h) (U) Director USCYBERCOM J7 will:

1. (U) Ensure COOP events and activities are incorporated into USCYBERCOM and other Combatant Command Tier 1 exercises and training events.

(i) (U) Director USCYBERCOM J8 will:

1. (U) Coordinate with appropriate organization to ensure emergency contracting and purchasing support.

2. (U) Identify deploying personnel to maintain COOP Government Purchasing Card (GPC) capability.

3. (U) Identify deploying personnel that can engage with appropriate contract authority on behalf of USCYBERCOM.

4. (U) Provide Headquarters contracting guidance and fund-site information upon COOP activation. Subordinate Command funding will be provided by their funding organization.

(3) (U) All USCYBERCOM Subordinate Commands, JFHQ-Cs, Service Components, and Task Forces.

(a) (U) Develop and maintain COOP plans. Completed plans will be provided to HQ USCYBERCOM J3 (b)(7)(e) of headquarters plan approval dates and subsequent revision approval dates.

(b) ~~(S)~~ BPT accept the transfer of those HQ USCYBERCOM MEFs that have been (b)(1) Sec 1.4(a) to a Sub-unified, JFCC, Component, or Task Force.

(c) ~~(S)~~ BPT to provide operational facilities and support to ensure COOP for HQ USCYBERCOM (b)(1) Sec 1.4(a) as needed.

4. (U) Administration and Logistics.

a. (U) Concept of Support. See Concept of Operations in Annex C.

b. (U) Logistics

(1) (U) No-Warning Relocation. This situation could occur when an attack or incident is imminent, in progress, or there is a contingency precluding continued use of the USCYBERCOM facilities.

(2) (U) With Warning Relocation. Decision to relocate may be contingent on the same trigger event that drives an increase in tensions and Defense Readiness Condition (DEFCON), Force Protection Condition (FPCON), Information Operations Condition (INFOCON), Continuity of Government Readiness Conditions (COGCON), and/or Homeland Security National Terrorism Advisory System (NTAS) Alerts.

(3) ~~(S)~~ Personnel designated to relocate as part of this plan during a COOP contingency (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
Personnel relocation may be conducted all at once or in phases as relocation options are implemented.

(4) (U) As relocation options are implemented and movements directed by senior leadership, the specific transportation requirements (b)(7)(e)
(b)(7)(e) will be forwarded by their directorate to USCYBERCOM J4 for coordination. These requirements will be presented in writing from the proper approval authority. If an individual directorate is

unable to contact J4, then that organization will coordinate their own transportation (b)(7)(e) .

(5) (U) Where possible, applicable memorandums of understanding and/or agreements should attempt to have host facilities provide all logistics support to implement this plan, to include housekeeping, facilities maintenance, billeting (where applicable), messing facilities, local transportation, medical, chemical warfare defense, security, services, and civil engineering support. J4 will coordinate an update to the Command Arrangement Agreement (CAA) with USTRANSCOM to address short-notice transportation and other mission support requirements.

(6) (U) Transportation plans are executable during duty and non-duty hours, with or without warning. Emergency short-notice relocation of key personnel may be directed by the CDRUSCYBERCOM at any time in order to enhance survivability of key personnel.

c. (U) Personnel. Many annex's and MEF documents establish essential personnel and administrative functions designed to meet USCYBERCOM needs in the event of a large-scale relocation or staff reconstitution.

d. (U) Public Affairs. The Office of Public Affairs (J0) is USCYBERCOM's office with primary responsibility for all Public Affairs (PA) actions that support CDRUSCYBERCOM and will provide information and recommendations on answers to the press on significant PA matters for COOP.

(1) (U) PA will work closely with the DOD, Joint Staff, and other agencies to provide PA planning for continuation of operations; develop contingency public statements and response to media queries, with supporting questions and answers, provide support for media briefings, establish a combined media center or a Joint Information Bureau as required, and develop internal information products and strategies to inform USCYBERCOM personnel and family members of COOP.

(2) (U) All queries received from the public, media organizations, or other organizations involved in gathering and disseminating information will be referred without comment to USCYBERCOM Public Affairs.

(3) (U) Command members shall not give information to the public even if material is unclassified or cleared through security and policy review and operational security channels unless the Commander, through PA, approves the release. This process avoids the release of potentially sensitive information or releases out of context, which could mislead the public.

e. ~~(S)~~ Medical. Medical support will be provided through local public First Aid Station/Clinics located near alternate facilities. Personnel are highly

encouraged to maintain a copy of their medical record, as access to the medical records on short notice may be difficult. Fly-away and MEF personnel will ensure they maintain an adequate quantity of prescription medicines on hand (b)(1) Sec 1.4(a)

5. (U) Command and Control.

a. (U) Command.

(1) (U) Command Relationships. For planning purposes, it is assumed that the current command organizational structure, including all command relationships, will not change. Each annex or appendix will identify all command arrangement agreements, Memorandums of Agreement (MOA) and memorandums of understanding (MOUs) used and those that require development.

(a) ~~(S)~~ Additional Measure: If relocating to a pre-planned location, the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) different locations depending on the event.

(2) (U) Succession to Command. The order of succession, the individuals responsible for assuming command will follow already established USCYBERCOM regulations and procedures and guidance. For positions other than the Commander, date of rank or position within that organization will determine who is in charge.

(a) (U) Orders of succession. Organizations and agencies are responsible for establishing, promulgating, and maintaining orders of succession to key positions. Such orders of succession are an essential part of an agency's COOP plan. Orders should be of sufficient depth to ensure the agency's ability to perform essential functions while remaining a viable part of the Federal Government through any emergency.

(b) (U) Command, Control, Communications, and Computer (C4) Systems. C4 systems play a critical role in the accomplishment of COOP activities. In general, we can assume that there has been significant disruption in C4 and that only basic C4 systems are functional. Each annex and appendix will cover what specific C4 requirements are needed to accomplish their MEFs.

b. (U) USCYBERCOM Support to Other Federal COOP Plans. USCYBERCOM could be required to provide support to other select government COOP plans during a COOP contingency. Support required by USCYBERCOM will be addressed in separately staffed agreements.

c. (U) Coordinating Instructions.

(1) (U) All tasked directorates and agencies will develop, coordinate, and forward to J3 procedures in the form of Annexes to support the USCYBERCOM COOP within 90-120 days of publication approval.

(2) (U) See ANNEXES for additional coordinating instructions and responsibilities.

(3) (U) Universal Coordinated Time (ZULU) will be used.

OFFICIAL

<F. M. LNAME>
RANK, SERVICE
POSITION, J-3