Department of the Army
Pamphlet 500–30

Emergency Employment of Army and Other Resources

U.S. Army Continuity of Operations Program and Planning Procedures

Headquarters
Department of the Army
Washington, DC
2 July 2021

UNCLASSIFIED

SUMMARY

DA PAM 500–30
U.S. Army Continuity of Operations Program and Planning Procedures

This new Department of the Army pamphlet, dated 2 July 2021—

- Provides information about the requirement to coordinate and synchronize the organization continuity of operations plan, mission essential function priorities, and information systems priorities with Chief Information Officer, Deputy Chief of Staff, G–6 and service providers who produce the supporting information technology contingency plans (para 3–3*e* and app B).

- Incorporates cyber resilience as an integral part of information technology contingency plans in support of the organization's continuity of operations plan (para 3–6*g* and throughout).

- Provides information about recommended training for continuity of operations program managers and points of contact (chap 4).

- Provides information about the relationship of organization continuity of operations plans with supporting information technology contingency plans (app B).

- Provides procedures in accordance with AR 25–30 for policies established in AR 500–3 (throughout).

- Synchronizes U.S. Army Continuity of Operations Program procedures with the Army Protection Program in accordance with AR 525–2 (throughout).

Headquarters
Department of the Army
Washington, DC
2 July 2021

Department of the Army Pamphlet 500–30

Emergency Employment of Army and Other Resources

U.S. Army Continuity of Operations Program and Planning Procedures

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet provides guidance and procedures in accordance with AR 500–3 to implement the U.S. Army Continuity of Operations Program to ensure continuity of essential functions under all circumstances across the spectrum of threats. It describes program and planning requirements for the Army Continuity of Operations Program, as well as requirements for continuity of operations program planning and tests, training, and exercises to validate continuity of operations plans and improve preparedness.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Proponent and exception authority. The proponent agency for this pamphlet is the Deputy Chief of Staff, G–3/5/7. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–3/5/7 (DAMO–OD), 400 Army Pentagon, Washington, DC 20310–0400.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References and forms • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Records management (recordkeeping) requirements • 1–4, *page 1*

Chapter 2
Program Management, Plans, and Procedures, *page 1*
General • 2–1, *page 1*
Continuity program management cycle • 2–2, *page 1*
Program management and implementation oversight • 2–3, *page 2*

Chapter 3
Continuity of Operations Planning Guidance, *page 8*

Section I
Development of Plans and Procedures, page 8
Executable plan focused on operations • 3–1, *page 8*
Continuity operations phases and implementation • 3–2, *page 8*

Section II
Continuity Capability Planning Requirements, page 10
Mission essential functions • 3–3, *page 10*
Order of succession • 3–4, *page 11*
Delegations of authority • 3–5, *page 12*
Continuity communications, information systems, and information technology services • 3–6, *page 12*
Essential records • 3–7, *page 13*
Continuity facilities • 3–8, *page 14*
Human resources and emergency relocation group • 3–9, *page 15*
Devolution • 3–10, *page 17*
Reconstitution • 3–11, *page 18*
Continuity of operations test, training, and exercises • 3–12, *page 19*

Section III
Continuity Planning and Plans Requirements, page 20
Additional planning requirements • 3–13, *page 20*
Continuity of operations plan format • 3–14, *page 20*

Chapter 4
Army Continuity of Operations Program Manager and Continuity of Operations Point of Contact Training, *page 21*
Overview • 4–1, *page 21*
Professional continuity training for Army continuity of operations program managers and points of contact • 4–2, *page 21*

Appendixes

A. References, *page 22*

B. Organization Continuity of Operations Plans, Mission Essential Functions, and Supporting Information Technology Contingency Plans, *page 25*

C. Security Classification Guidance, *page 29*

D. Sample Assessment Checklist, *page 30*

Table List

Table 4–1: Professional continuity training for continuity of operations program managers and continuity of operations points of contact, *page 21*

Figure List

Figure 2–1: Continuity program management cycle, *page 2*
Figure 2–2: Sample continuity of operations program manager appointment memorandum, *page 3*
Figure 2–3: Sample continuity of operations point of contact appointment memorandum, *page 4*
Figure 2–4: Determining whether a continuity of operations plan is required, *page 7*
Figure 3–1: Continuity operations phases and implementation, *page 10*
Figure 3–2: Sample emergency relocation group appointment memorandum, *page 17*
Figure B–1: Organization continuity of operations plan and supporting information technology contingency plans, *page 26*
Figure B–2: Example organization continuity of operations plan and mission essential function analysis data, *page 27*
Figure B–3: Example organization continuity of operations plan and mission essential function analysis relationship to information technology contingency plans, *page 28*

Glossary

Chapter 1
Introduction

1–1. Purpose
This pamphlet provides procedures for policies established in AR 500–3. It contains program and planning requirements, instructions, processes, formats, reporting, and guidelines used to carry out the U.S. Army Continuity of Operations (COOP) Program to ensure resilience and continued performance of mission essential functions (MEFs) under all conditions. The Army COOP Program is a functional element of the Army Protection Program (see AR 525–2).

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

Chapter 2
Program Management, Plans, and Procedures

2–1. General
The Army COOP program assures the capability to continue MEFs under all circumstances. COOP programs and plans are mission operations centric by necessity. Establishing a continuity program with planning objectives and procedural requirements is key to sustaining essential functions during a continuity event. Allocating resources to program requirements, plans, procedures, and capabilities is critical to ensure execution and sustain essential functions through all phases of continuity operations. Applying risk management principles can conserve and allocate resources based on assessments and the probability of occurrence for catastrophic emergencies and related consequences. The development, preparation, and execution of the continuity capabilities and elements indicated in this pamphlet are fundamental to successful continuity programs and plans.

2–2. Continuity program management cycle
a. Army COOP programs incorporate a continuity program management cycle depicted in figure 2–1.

b. The cycle facilitates development, implementation, and improvement of resilient continuity programs and consists of:

(1) Developing and implementing COOP plans and procedures.

(2) Testing, training, and exercising.

(3) Evaluating after-action reports, lessons learned, and assessments.

(4) Developing corrective action plans and implementing corrective actions to improve continuity programs, plans, procedures, and capabilities.

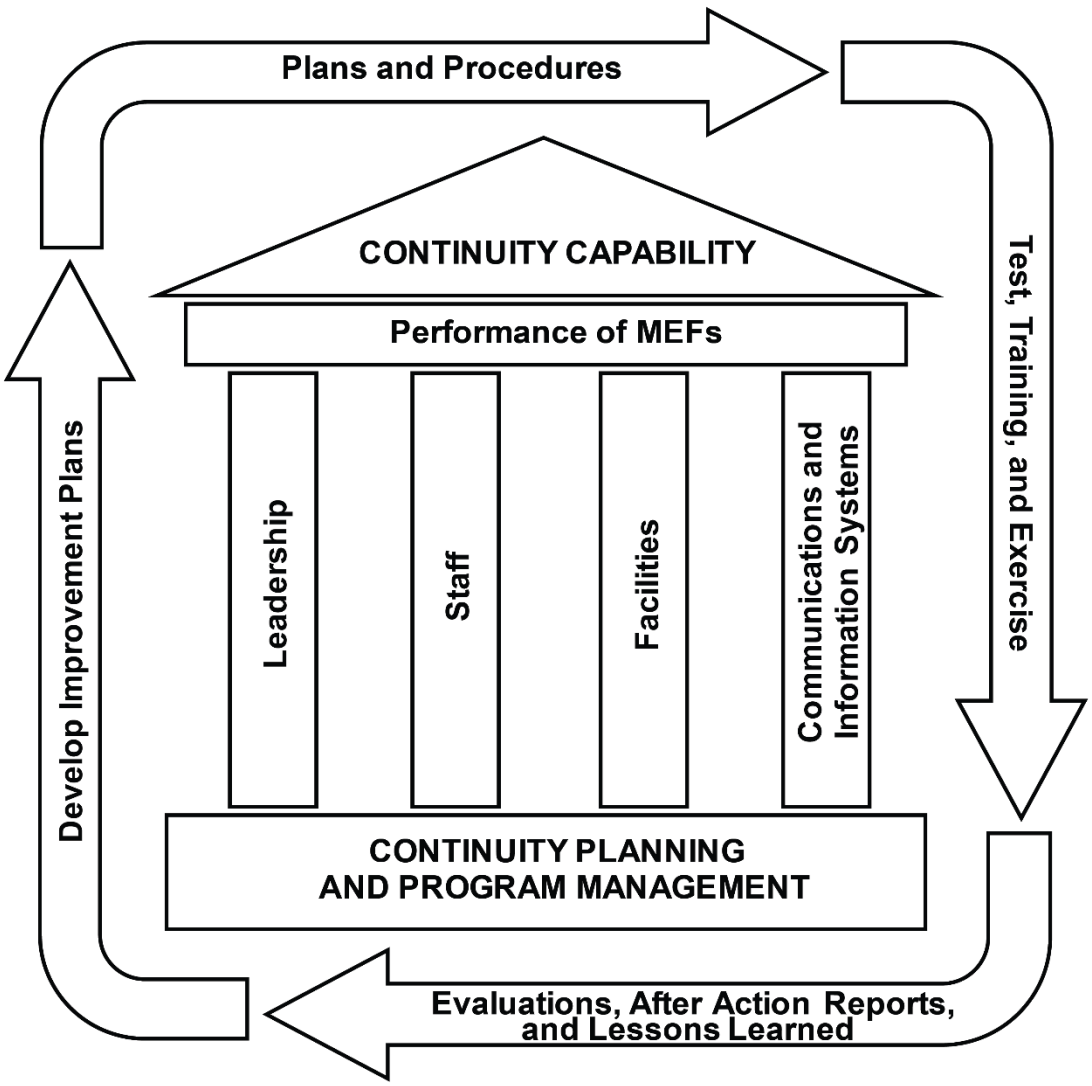

Figure 2–1. Continuity program management cycle

2–3. Program management and implementation oversight

COOP program implementation, management, and oversight activities include but are not limited to the following:

a. Designate points of contact. Designate the continuity of operations point of contact (CPOC) (for Headquarters, Department of the Army (HQDA) staff agencies) or program manager (PM) (for Army commands (ACOMs), Army service component commands (ASCCs), direct reporting units (DRUs), Army National Guard (ARNG), U.S. Army Reserve (USAR), and field operating agencies (FOAs)). Designations are in writing by commanders/senior Army officials responsible or the delegated immediate deputy/chief of staff, but not a lower echelon or subordinate. Designate a primary and alternate CPOC (for HQDA staff agencies) or a primary and alternate PM (for ACOMs, ASCCs, DRUs, ARNG, USAR, and FOAs), as appropriate, responsible to the organization's senior official for management oversight of the organization's COOP program and planning. Refer to AR 500–3 for additional requirements. See sample memoranda for appointment as a COOP PM in figure 2–2 and as a CPOC in figure 2–3.



DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

[Office Symbol] [Date]

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Appointment as Continuity of Operations Program Manager

1. Effective [DATE], [NAME] is appointed as [PRIMARY or ALTERNATE] Continuity of Operations Program Manager (COOP PM) for the [COMMAND or ORGANIZATION].

2. Authority: AR 500-3.

3. Purpose: To serve as the [PRIMARY or ALTERNATE] COOP PM for the command's COOP program, policy, and planning in accordance with AR 500-3 and other applicable directives and as indicated herein.

4. Period: Until reassigned or officially released or relieved from duty appointment or assignment.

5. Special Instructions: [ENTER RESPONSIBILITIES AND INSTRUCTION AS APPLICABLE].

FOR THE COMMANDER

[SIGNATURE BLOCK]

Distribution:

Figure 2–2. Sample continuity of operations program manager appointment memorandum



DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

[Office Symbol] [Date]

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Continuity of Operations Point of Contact Appointment

1. Effective [DATE], [NAME] is appointed as [PRIMARY or ALTERNATE] Continuity of Operations Point of Contact (CPOC) for the [COMMAND or ORGANIZATION].

2. Authority: AR 500-3.

3. Purpose: To serve as the [PRIMARY or ALTERNATE] POC for the organization's COOP program, policy, and planning in accordance with AR 500-3 and other applicable directives and as indicated herein.

4. Period: Until officially released from this appointment.

5. Special Instructions: [ENTER RESPONSIBILITIES AND INSTRUCTION AS APPLICABLE].

FOR THE COMMANDER

[SIGNATURE BLOCK]

Distribution:

Figure 2–3. Sample continuity of operations point of contact appointment memorandum

(1) Encourage the CPOC/COOP PM to complete the recommended training courses identified in chap 4.

(2) Provide primary and alternate CPOCs/PMs with individually assigned, dedicated secure internet protocol router network (SIPRNET) access/connectivity vice using a general use office SIPRNET; to the extent possible ensure

agency emergency relocation group (ERG) members have Army Knowledge Online (AKO) and AKO–S accounts on nonsecure internet protocol network (NIPRNET) and SIPRNET, depending upon the organization's mission.

(3) Maintain the agency's COOP ERG member roster/COOP alert and notification (A&N) roster. Due to the requirement to provide immediate alert or notification to execute the COOP operations plan (OPLAN), ensure all ERG members (primary and alternate) provide their personal contact information, including after-duty hours contact information as appropriate (for example, personal cellular phone numbers or landline phone numbers), email addresses, and so forth, and enter into the COOP ERG roster/system. Review the rosters at least monthly and update as changes occur. Ensure these updated rosters are provided to the agency's operations center, watch, and all personnel who require the rosters. Electronic dissemination is recommended. Adhere to classification, Privacy Act, and operations security (OPSEC) considerations.

(4) Ensure the capability and procedures exist to alert and notify the ERG members when the agency COOP OPLAN is activated.

(5) Identify, update, and oversee the agency's ERG positions required to perform the MEFs, personnel (primary and alternate) to fill the ERG positions, and the supporting essential databases, files, and other resources.

(6) Disseminate COOP program information to the agency's ERG members and expectations for non-ERG personnel, as applicable.

(7) Ensure PMs chair and CPOCs attend the Continuity of Operations Working Group (CWG) which may be integrated into the Protection Working Group (PWG) in accordance with AR 525–2.

(8) Keep the commander/senior Army official responsible for the organization and/or the ACOM, ASCC, DRU, ARNG, USAR, and FOA commander/director informed of COOP related issues and the status of the organization's COOP program either privately or by briefing COOP at senior level staff meetings such as a Protection Executive Committee (PEC). Refer to AR 525–2 for more about a PEC.

(9) Oversee the COOP program's use and implementation of the Government Emergency Telecommunications Service (GETS) cards and Wireless Priority Service (WPS) for COOP personnel. The requirement for use of GETS cards and WPS and the scope of their issue to COOP personnel at the headquarters and subordinate organizations of each ACOM, ASCC, DRU, ARNG, USAR, and FOA is determined by the commander/director/senior Army official responsible or the delegated immediate deputy/chief of staff, but not a lower echelon or subordinate.

(10) Ensure ERG members exercise the communications, networks, information systems, applications, and websites required to perform the organization's MEFs while at continuity facilities (CFs).

(11) Ensure the ERG and other continuity personnel who may carry classified information outside of their normal place of duty are issued and possess current courier cards upon designation to fill an ERG position.

(12) Ensure procedures for telework or work-at-home agreements which support execution of unclassified MEFs and the COOP plan are approved and implemented in accordance with established policy and procedures.

(13) Ensure the agency's contracting requirements and agreements to support COOP are identified and in place in advance of COOP events.

(14) Prepare and maintain the agency's COOP plan and oversee development and maintenance and its subordinate agencies' COOP plans.

(15) Ensure ERG members and agency principals are knowledgeable and informed of ERG member COOP OPLAN responsibilities and procedures.

(16) Develop COOP exercises, lessons learned, tracking, and resolution of corrective actions.

(17) Establish a "COOP" or "Continuity of Operations" link with all nonpublicly accessible unclassified and classified websites. Provide a link from the home page of the organization website to access COOP related information on a need to know basis.

(18) Maintain a paper file or a loose leaf binder containing a copy of the CPOC or PM appointment letters, memorandums, or orders, at a minimum.

b. Conduct risk management. Army COOP program management will incorporate risk management considerations and factors in accordance with Army Protection Program implementation in AR 525–2.

c. Perform budgeting and acquisition of resources. Identify, prioritize, and justify requirements to plan, program, and budget resources to develop, maintain, exercise, and validate the organization's continuity capabilities. The budget includes, but is not limited to, acquisition of the resources necessary to deploy personnel; develop and maintain CFs; conduct a realistic COOP test, training, and exercise (TT&E) program; and resource CFs including communications and information technology (IT) systems to sustain MEF execution for a minimum of 30 days or until normal operations are resumed. Work with headquarters and other agencies to plan and budget for continuity program requirements in accordance with the command budget process and the Planning, Programming, Budgeting, and Execution System, as appropriate. Maintain documentation of the organization's COOP budget requests and funding status. Resources for implementing risk management must be identified and allocated as part of the budgeting process.

d. Conduct strategic planning. Develop and implement a multiyear strategy and program management plan (MYSPMP) that provides for the development, maintenance, and annual review of continuity capabilities to ensure critical activities and resources are acquired to sustain program support and continuous improvement efforts. The MYSPMP provides for as a minimum:

(1) Short- and long-term planning goals and objectives.

(2) Potential program implementation issues, concerns, and obstacles and a strategy to address each.

(3) Planning, training, and exercise milestones and activities.

e. Provide supplemental guidance. Headquarters organizations provide oversight and issue procedures and planning guidance to ensure the continuity capability and readiness in accordance with AR 500–3.

f. Establish a Continuity of Operations Working Group. Charter and establish a CWG to meet at least quarterly. The charter designates membership as determined by the organization. The CWG is the body of COOP PMs, CPOCs, action officers, service providers, partners, and others, as applicable, for sharing continuity information within and among organizations. The CWG facilitates development, maintenance, and improvement of planning; TT&E events; assessments; and preparedness for resilience and continuity capabilities. CWG format, presentation, and documentation will be determined by the senior Army official responsible for the organization. The PM or CPOC facilitating the CWG maintains documentation showing at a minimum the CWG was conducted including date, time, place, agenda, and attendees. The agenda may include, as applicable, items such as program budget and funding review, readiness status of the capability to execute the COOP OPLAN, training status, alternate facility readiness and status, emergent issues affecting the COOP program/plan, TT&E outcomes, lessons, after-action reports, review and tracking of open actions pending resolution, and dissemination of COOP related information. Procedurally, the CWG may be integrated into the PWG in accordance with AR 525–2. The CWG's meeting program content, including slides, reports, meeting notes, and attendance by name and organization is documented and maintained for at least the previous 24 months.

g. Review continuity of operations readiness. COOP managers capture data, track, analyze, and review COOP program readiness metrics and report the status of the organization's readiness to execute its COOP OPLAN to the CWG and leadership. This includes, but is not limited to, status of ERG personnel manning and training, status of annual exercise when ERG members operated from the CF, training status of MEF exercised, status of CFs' capability to support ERG personnel and to execute and sustain MEFs for 30 days, and status of facility communications, information systems, IT services, and access to essential records/data.

h. Approve the continuity of operations operation plan. The organization's COOP OPLAN is approved and signed in accordance with AR 500–3. The organization's COOP OPLAN is validated, updated, approved, and reissued at least every 2 years, or more often as changes warrant. The COOP OPLAN contains the organization's prioritized MEFs approved in accordance with AR 500–3 as the basis for the COOP OPLAN, related continuity planning, preparation, and plan execution. The COOP OPLAN must be capable of being activated with or without warning during duty hours and nonduty hours. A COOP plan is required for organizations that have MEFs that must be continued throughout, or resumed rapidly after a continuity event as determined by a MEF analysis and review. Figure 2–4 provides information to determine whether an organization needs a COOP plan.

DETERMINING WHETHER A CONTINUITY OF OPERATIONS PLAN IS REQUIRED

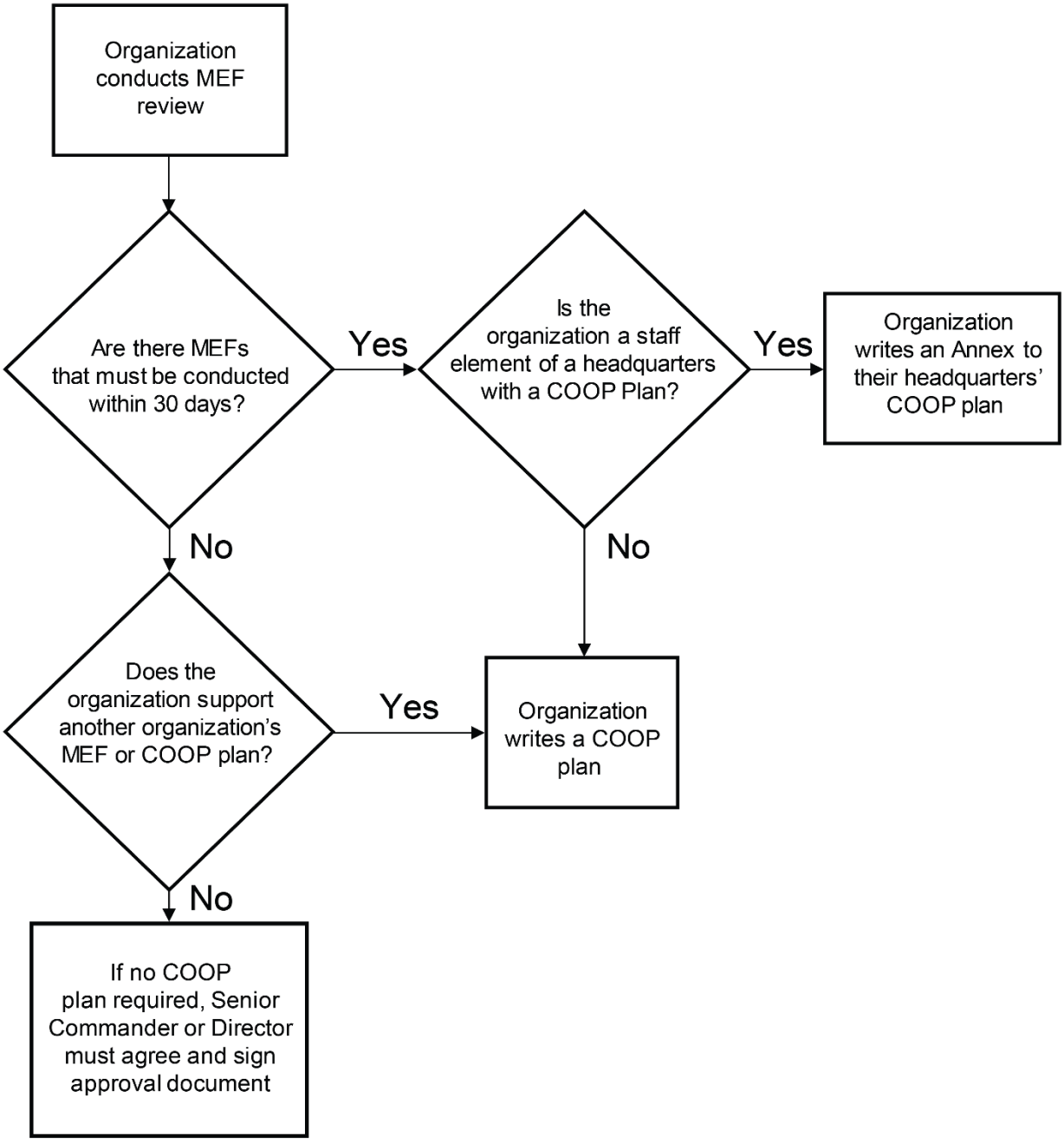

Figure 2–4. Determining whether a continuity of operations plan is required

Chapter 3
Continuity of Operations Planning Guidance

Section I

Development of Plans and Procedures

3–1. Executable plan focused on operations

Army COOP OPLANs will be designed to conduct operations in response to continuity contingencies across the spectrum of threats. The organization's COOP OPLAN must be executable, trained to, tested, and exercised. Continuity planning applies to execution of the organization's mission. COOP OPLANs focus on the organization's operations and capabilities to continue its MEFs during and after an emergency event. Army COOP OPLANs will be event neutral and consider procedures that provide Army organizations and leadership with the ability to ensure MEFs continue in all-hazards environments with minimum disruption through the event until normal operations are resumed. Minor interruptions such as a short duration power failure, for example, that do not substantially disrupt an organization's MEFs potentially will not be considered by the organization's leadership as a declared COOP event based on the situation. In addition to AR 500–3, the requirements of this pamphlet apply.

3–2. Continuity operations phases and implementation

Army COOP plans will incorporate the following four phases of continuity operations planning and implementation. Executing a COOP plan is intended to continue or rapidly resume MEFs following a disruption of normal operating conditions. The continuous performance of MEFs is critical to an organization's resilience. Four phases are used to build continuity plans, procedures, and processes; to establish goals and objectives; and to support the performance of organizational MEFs during a catastrophic emergency. See figure 3–1.

a. Phase I: Readiness and Preparedness. Readiness is the ability of an organization to respond to a continuity threat or event. Readiness is a function of planning and training and is ultimately the responsibility of leadership. Leadership must ensure its organization can perform continuity operations, including the performance of essential functions before, during, and after all-hazards emergencies. This phase includes all continuity readiness and preparedness activities, such as development, review, and revision of continuity plans to include planning for devolution and reconstitution; A&N procedures, roster maintenance, orders of succession, and delegations of authority; resourcing and equipping CFs with communications and information systems and applications; conducting TT&E activities to maintain readiness; and risk management.

b. Phase II: Activation (0 – 12 hours). This phase includes the activation of plans, procedures, and activities to continue MEFs. ERG members must be fully operational at the alternate facility as soon as possible but no later than 12 hours after continuity activation. The activation phase includes the following activities:

(1) Occurrence of an event or the threat of an event.

(2) Review, analysis, and decision to activate COOP OPLAN and/or devolution plans.

(3) Activation of A&N procedures, systems, and capabilities to notify the ERG.

(4) Initiation of prioritized recovery actions required to return an organization's essential functions, systems, processes, and support functions to initial operational stability following an interruption or disaster. Recovery actions include execution of supporting IT operations disaster recovery plans (DRPs) and related information system contingency plans (ISCPs).

(5) Relocation of ERG members to alternate sites.

(6) In-processing, reception, and accountability of ERG members at alternate sites.

(7) Accounting for primary ERG members no later than 12 hours after activation. The capability to account for alternate ERG members no later than 12 hours after activation exists.

(8) Devolution of control and direction and the responsibility for execution of the organization's MEFs to devolution sites, if necessary, should the organization be unable to execute them.

(9) Identification of available organizational leadership.

(10) Situation and status reporting in accordance with plans and procedures.

c. Phase III: Continuity Operations. This phase includes the following activities to continue MEFs:

(1) Accountability of all personnel in the affected area after activation of an organization's COOP plan.

(2) Performing and sustaining MEFs.

(3) Establishing communications with supporting organizations, supported organizations, and other stakeholders.

(4) Preparing for the organization's reconstitution.

d. Phase IV: Reconstitution. The process of reconstitution generally starts immediately after an event concludes. Some of the activities involved with reconstitution include:

(1) Assessing the need to rebuild the organization's staff with personnel due to casualties or other losses.

(2) Assessing the status of the affected facility or facilities.

(3) Assessing the status of supporting infrastructure, communications, IT networks, information systems, applications, and capabilities required to resume normal operations at a new or the restored primary operating facility.

(4) Determining how much time is needed to repair the affected facility and/or to acquire and equip a new facility.

(5) Supervising facility repairs.

(6) Notifying decision makers of the status of repairs, including estimates of when the repairs will be completed.

(7) Implementing a priority-based, phased approach to reconstitution.

(8) Coordinating establishment of an emergency family assistance center, as applicable.

(9) Supporting business continuity plans, as applicable, for on-installation businesses which agreed to a role in the recovery organization, including the recovery working group. See DA Pam 525–27 for more details.

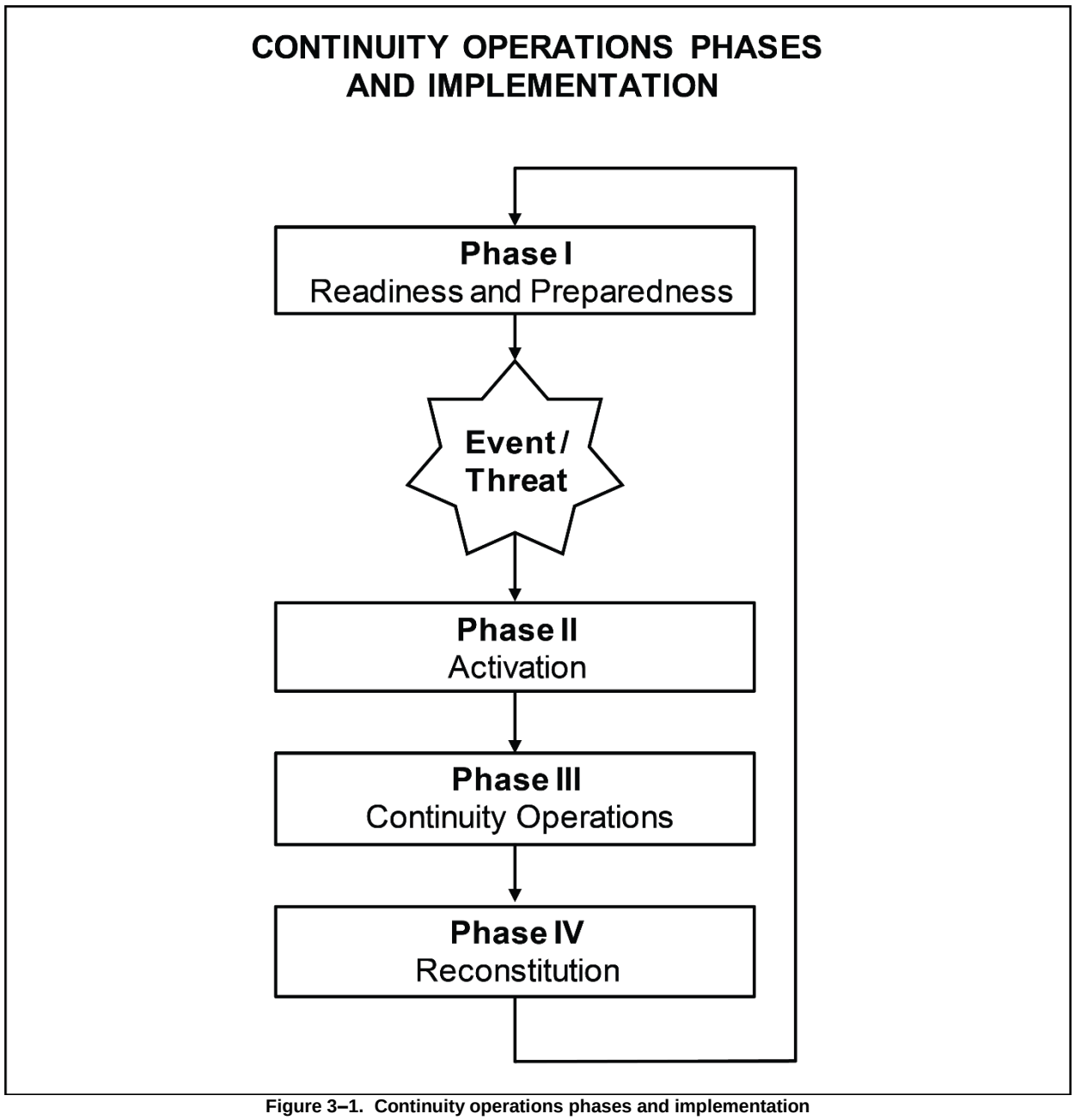

Figure 3–1. Continuity operations phases and implementation

Section II

Continuity Capability Planning Requirements

Army COOP planning activities and plans must include, but are not limited to, the following continuity capability planning elements which are based on DoD guidance derived from national and federal executive branch directives (see app D for a sample assessment checklist).

3–3. Mission essential functions

The COOP OPLAN will identify and prioritize the organization's MEFs. Identification and prioritization of MEFs is the foundation of effective continuity planning and the basis for the plan. MEFs are the limited set of the organization's normal functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities. MEFs are directly related to the organization's unique mission as specified, or implied tasks required to be performed by, or

derived from, statute, executive order, or other appropriate guidance, and those activities that must be performed under all circumstances to achieve organization missions or responsibilities in a continuity threat or event. Common organizational functions are important, however, not every important function or activity is a MEF. The MEFs define the size and composition of the ERG, the requirements for CF capabilities, resources for sustainment of continuity operations, essential records replication and accessibility, and the communications, IT networks, information systems, applications, and services required. Generally, MEFs are unique to each organization. Organization COOP OPLANs will—

a. Identify the organization's MEFs. Review and update MEFs every 2 years prior to and in conjunction with the organization's COOP OPLAN revision. Mission changes and reorganizations within the 2-year period will require an immediate MEF review to determine if the organization's COOP OPLAN will need to be revised. Identification includes organization MEFs performed at the primary operating facilities/locations used by the organization whether owned or leased.

b. Identify the criticality and priority for each MEF.

(1) MEF criticality is determined by analyzing the level of impact (for example, consequences or harm) that would occur for each MEF if it could not be performed and the maximum tolerable downtime (MTD) which is the maximum amount of time the performance of the MEF can be delayed before there is mission impact. The MTD is the maximum time acceptable for a disruption or degradation in the performance of the MEF. The MTD is determined by the owner of the MEF.

(2) MEF priority is based on the criticality assessment and approval by the organization's leadership.

c. Identify the primary and alternate secure and nonsecure communications, IT networks, information systems, applications, databases, and websites required to perform each MEF.

d. Identify partners and interdependencies required to perform each MEF, such as internal and external service providers, as applicable.

e. Coordinate and synchronize the organization's priority for each MEF and the assessment of the level of impact or harm that would result from the consequences of loss of availability of information or information system required to perform the MEF. Coordination is with the information technology contingency plan (ITCP) coordinators/planners, ITCP points of contact (POCs), and service providers, as applicable, for the ITCPs they develop and for the plans to test the ITCPs in accordance with AR 25–2 and DA Pam 25–1–2. ITCPs are coordinated with and support the organization's COOP OPLAN and assure the capability to continue organization MEFs across the full spectrum of emergencies. Appendix B outlines relationships between an organization's COOP OPLAN with MEF and MTD and the supporting ITCPs developed by the IT contingency planner/service provider.

f. Identify the ERG positions required to accomplish each MEF.

g. Based upon the skill sets, tools, data, and systems required to execute each of the organization's MEFs, identify another organization(s) which is most capable of performing each MEF should the organization be unable to communicate or perform its MEFs and need to devolve each MEF.

h. Approve organization MEFs and their priority in accordance with AR 500–3.

i. Resource MEFs which must be continued uninterrupted or resumed rapidly within 12 hours of the event with the robust, redundant, interoperable, survivable communications and information systems, facilities/platforms, and personnel required to ensure that capability.

3–4. Order of succession

The organization's COOP OPLAN will identify the designated successors in order and at least three positions deep for command authorities and other key personnel in accordance with AR 600–20 to ensure an orderly succession of leadership during any emergency. Orders of succession are formal and sequential listings of positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role under specific circumstances. In some cases, organizations may have the latitude to develop orders of succession as they deem appropriate, while in other cases succession is prescribed by statute, order, or directive. Procedures should be in accordance with AR 600–20 and the Vacancies Reform Act of 1998, as amended (5 USC 3345 et seq.), if applicable. Those identified in the orders of succession should be trained annually on responsibilities and will participate in TT&E events. Orders of succession should be reviewed by the organization's General Counsel or equivalent to ensure legal sufficiency, as necessary. Considerations for establishing orders of succession are:

a. Establishing an order of succession to the position of agency head and other key leadership positions.

b. Describing orders of succession by position titles rather than names of individuals.

c. Identifying a minimum of three positions to succeed to the identified leadership position.

d. Outlining a process and criteria to activate procedures for the transition of successors. This includes establishing procedures for notifying appropriate personnel when succession is implemented.

e. Identifying any limitation of authority (for example, statutory, time limits, geographical).

f. Establishing the rules and procedures designated officials are to follow when facing issues of succession and rules for promulgating the changes.

g. Using geographically dispersed successors, where feasible.

h. Ensuring orders of succession are positioned and available at primary and alternate facilities as a part of essential records.

3–5. Delegations of authority

Delegation of authority is an essential part of an organization's continuity plans and should have sufficient depth and breadth to ensure the organization can perform its MEFs during the course of any emergency.

a. The organization's COOP plan will identify and delineate preplanned delegations of authority needed to assure execution of the organization's COOP plan and performance of its MEFs during a continuity event until normal operations are resumed. Clearly established delegations of authority ensure continuity personnel have the appropriate legal authority to make key decisions and take actions during catastrophic emergencies. Delegations of authority are activated when normal operational conditions are disrupted, and are deactivated once the organization determines that the disruption has ended and normal operations can be resumed. Pre-established delegations of authority ensure orderly transition of responsibilities within an organization during continuity activation for key individuals (military or Department of the Army Civilian (DAC)) within the organization.

b. A written delegation of authority provides the succeeding individual with the legal authorization to act on behalf of the incumbent for specified purposes and to carry out specific duties. Delegations of authority will generally specify a particular function that an individual is authorized to perform and includes restrictions and limitations associated with the authority. Organizations should identify the individuals to whom authorities are delegated by position title and not by name. Delegations of authority are frequently tied to specific positions, but since many delegations require specific training, qualifications, and certification, organizations must also associate some delegations of authority with specific individuals (for example, delegations for committing funds, contracting, technical direction, and classification authority).

c. Delegations of authority outline conditions under which delegated authority takes effect and the termination process for when authorities are reestablished. Organizations must include written delegations of authority as an essential record and ensure they are available at all alternate locations. If the command determines from analysis it does not need any preplanned delegations of authority to assure performance of any of its MEFs, the plan will state such including the date of the legal/commander's determination, and a copy of the analysis will be maintained and available in essential records.

d. Development and revision of delegations of authority must be coordinated with the organization's General Counsel or equivalent to ensure legal sufficiency.

3–6. Continuity communications, information systems, and information technology services

COOP programs and plans operations depend on the availability and accessibility of critical secure and nonsecure communications and IT systems with sufficient resilience and IT contingency planning necessary to perform MEFs at primary and alternate facilities. These systems and services must be interoperable and provide connectivity between and among key leaders, internal elements, other organizations, and external partners under all conditions. These technologies must be robust, reliable, redundant, and resilient. The primary and alternate communications and information systems that support each MEF must be identified during the MEF review in order to plan and provide for the availability and accessibility of those systems. The capability to maintain availability and accessibility is assured by IT contingency planning and programs, generally led by the Deputy Chief of Staff (DCS), G–6 and service providers, which ensure compliance with Federal Information Security Management Act information security requirements and leverage guidelines contained in the U.S. Department of Commerce NIST SP 800–34 Rev. 1 and NIST SP 800–53 Rev. 4 to inform the standards and measures for system evaluations. The IT contingency planning is often unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level. These programs and processes directly support the resilience of an organization's MEFs. Organization COOP planners coordinate the MEF prioritization and the required systems for each MEF derived from their MEF review with the applicable ITCP planners/coordinators, ITCP POCs, and service providers in order to integrate with and inform communications and information systems contingency planning and resilience efforts. The organization's COOP OPLAN will—

a. Identify the organization's priority for each MEF to inform and coordinate with the IT partners and service providers to ensure MEF prioritization is integrated with ITCP coordinators' efforts to produce communications and ISCPs and resilience planning through the IT Risk Management Framework. Risk acceptance levels and/or mitigation

strategies must be reconciled with user requirements and integrated into the overall plan for continuation of MEFs the system enables.

b. Identify the secure and nonsecure communications, IT networks, information systems, applications, websites, and IT services required to perform the organization's MEFs at its primary operating location and at its alternate facilities and devolution locations. Communication capabilities will include mobile in-transit communications capabilities for senior leadership, as required, to ensure the continuation of the organization's MEFs. Organizations must plan and resource accordingly if a MEF requires uninterrupted communications and IT support.

c. Prioritize the communications, networks, information systems, and applications required to perform the organization's MEFs, and coordinate with applicable DCS, G–6 staff and service provider agencies for integration into communications and ISCPs and resilience planning efforts supporting the organization's MEFs.

d. Identify alternate methods to respond to cyber degradation. Methods should not be dependent on internet protocol-based information systems to continue MEF and the appropriate classification level. Consider non-IT based methods and alternate business strategies to execute organizational MEFs.

e. Verify the levels of support and resilience necessary for specific information systems are coordinated in service level agreements with each communications and IT system service provider.

f. Identify the applicable emergency communications systems used by key leaders and other select continuity personnel while they are in transit and at the alternate sites, including:

(1) GETS cards for both primary and alternate continuity personnel and prepositioned GETS cards for emergency use at the alternate site.

(2) Government-issued cellular telephones with WPS for continuity personnel members that qualify in accordance with Department of Homeland Security Office of Emergency Communication WPS eligibility criteria (https://www.dhs.gov/cisa/wps-eligibility).

(3) Primary and alternate site circuits supporting continuity communications are included in the Telecommunications Service Priority Program.

(4) Residential and mobile secure communications (for example, DoD mobility classified capability device) for headquarters senior leadership and continuity staffs to collaborate, develop policy recommendations, and direct execution of essential functions from headquarters or alternate locations under all circumstances, as required by Office of Science and Technology Policy/Office of Management and Budget Directive D–16–1, Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities, December 2016.

g. Incorporate cyber resilience. COOP programs and plans are dependent on the availability of robust communications. Command, control, communications, computers, and intelligence (C4I) systems are critical enablers of effective communication and execution of MEFs. The organization's COOP OPLAN will—

(1) Identify and prioritize the communications, IT networks, information systems, applications, and websites required to perform the organization's MEFs. Coordinate the prioritized MEFs and systems with applicable DCS, G–6 staff, ITCP coordinators, and service providers for integration into communications, ISCPs, and resilience planning activities which support the organization's MEFs. See appendix B.

(2) Integrate cyber resilience into the plan to maintain performance of MEFs in the event of network disruption and degradation. Exercise the plans to be ready to operate in a degraded cyber environment where access to networks and data is uncertain.

3–7. Essential records

Effective continuity programs include comprehensive processes for identification, protection, and accessibility of electronic and hardcopy essential records at primary operating facilities, alternate facilities, and devolution locations. Essential records are those records the organization needs to perform its MEFs under any emergency condition and to support its reconstitution during and after a COOP activation (that is, emergency operating records) or to carry out the organization's essential legal and financial functions vital to the protection of the legal and financial rights of individuals who are directly affected by the organization's activities (that is, legal and financial rights records). Essential records may include documents, references, personnel records, and electronic information systems. Redundant data management software applications and equipment should be standardized throughout the organization and must provide the appropriate level of access and cybersecurity to protect classified, sensitive, and personally identifiable information.

a. The organization's COOP OPLAN will identify essential records and procedures to ensure essential information systems and applications, electronic and hardcopy documents, references, databases, and records, to include classified or sensitive data, needed to perform MEFs during a continuity event are safeguarded, available, and accessible to support continuity operations at alternate facilities and devolution locations.

b. The organization's CPOCs/COOP planners coordinate replication and availability requirements with the IT community's ITCP coordinators, ITCP POCs, or service providers in order to integrate with and inform the IT community's communications and information systems contingency planning, resilience planning, and service level agreements.

c. MEF owners identify alternate means to access web-based essential documents, references, databases, and records at CFs should web access be unavailable; such as electronic records stored at CFs or hardcopy documents.

3–8. Continuity facilities

The organization's COOP OPLAN will identify its CFs. CFs will have the capability to perform MEFs as soon as possible, but not later than 12 hours after notification, and the capability to sustain continuity operations for a minimum of 30 days or until normal operations are resumed. The term "continuity facilities" is comprehensive, referring to alternate locations, alternate headquarters, alternate facilities, alternate sites, and devolution sites, as well as work arrangements such as telework.

a. The OPLAN will—

(1) Indicate the organization's designated nickname (for example, Site Kilo) for each of its CFs to provide for OPSEC considerations and security classification in accordance with DoD continuity program security classification guidance.

(2) Identify one or more CFs that could be used based upon varying degrees of risk and severity of threat to ensure performance of MEFs under all circumstances. An organization may select an alternate site in the immediate geographic location as its primary operating location for use in the event of a burst pipe or a fire in the main building. Organizations maintain an alternate site or sites located far enough away from the primary facility that it would not be impacted by the same events, such as a hurricane, flooding, tornados, earthquake, explosive detonation, and resulting extended utility outages for electric power, communications, and water for life support for the ERG.

(3) Describe the verified and tested transportation plans, methods, and procedures for movement of ERG personnel with warning and without warning to alternate sites and provide directions to each alternate facility.

(4) Provide procedures to enable access to the alternate facility/headquarters and the host organization/installation, as applicable, during elevated security conditions at the alternate location.

(5) Describe the A&N process, procedures, and systems used to activate alternate sites.

b. Planning considerations for the identification and preparation of CFs will include:

(1) Selection of CFs including an all-hazard risk assessment (in accordance with AR 525–27). This analysis should include identification of all natural hazards that may affect the facility; the potential for the facility to be impacted by technological accidents such as release of hazardous materials from nearby fixed-facility and lines of transportation; technological failures such the electrical grid; degradation of the cyber environment; the ability to secure the facility against crime, sabotage, terrorist attacks, or military attack; and the capabilities of on-site and/or local first responders. Organization alternate locations/facilities/headquarters should be located in an area where disruption to the organization's ability to perform and maintain MEFs is minimized. Use existing local or geographically separated electric power, communications, and water infrastructures when possible.

(2) Sufficient space, infrastructure, power, life support, communications, and IT connectivity to accommodate the organization ERG and equipment required to perform MEFs. Consider geographic dispersion of designated MEFs, if possible.

(3) Physical security including perimeter, access, and internal functions commensurate with the performance of essential functions.

(4) The distance from the threat area to any other vulnerable facilities/locations (for example, hazardous materials/nuclear power plants, or areas subject to natural disaster) (see UFC 4–010–01).

(5) Access to reliable logistical support and essential resources such as rations, lodging, water, fuel, medical facilities, technical service providers, IT equipment, office supplies, and emergency services (for example, fire and police), as required.

(6) Procedures for maintaining the readiness of alternate sites and options for evacuation and relocation, if necessary.

(7) Prepositioning and maintaining unique equipment required to perform MEFs at alternate sites.

(8) Compliance with the Americans with Disabilities Act. Procedures for routine and emergency ingress and egress must consider handicap assigned and visiting personnel, including during power out conditions.

(9) Emergency power capability. The organization's alternate facilities/sites/headquarters should have the emergency power capability to allow MEFs and continuity operations to continue in any environment.

(10) At least an annual review of its alternate facilities for suitability and functionality.

c. Organizations with alternate facilities that are not owned or leased by the U.S. Government or not owned by the organization will have a current, signed memorandum of agreement (MOA)/memorandum of understanding (MOU) with the owner or occupant of the facility and will review the MOA and/or MOU annually, or following leadership changes. At a minimum, MOAs and/or MOUs will—

(1) Specify requirements to have the facility configured for occupancy to perform MEFs as soon as possible, but not later than 12 hours after notification.

(2) Provide details of the space and services to be provided at the facility.

(3) Provide access control procedures to the allocated space during occupancy.

(4) Document the dates and names of personnel conducting the review.

(5) Complete a legal review.

d. Telework can be a useful option to support unclassified MEFs. If the organization plans to use telework to perform or support any of its MEFs in whole or in part, the COOP plan will identify each MEF and the ERG position or positions that perform the MEF. When using telework as a COOP option, the organization must follow pre-established telework policy and procedures. Telework may not be a viable strategy for continuing MEFs during all events (for example, cyber events, mass power outage, wide spread disaster). Telework may be used to augment continuity, but should not be relied upon as an organization's only continuity option. Organizations will adhere to policy and provide protection of information as well as information systems used during telework operations according to government standards. COOP OPLANs will—

(1) Identify each of the organization's unclassified MEFs that will be completely or partially performed using telework during a continuity event.

(2) Designate, roster, train, exercise, and manage teleworkers performing organization MEFs as members of the ERG. The teleworkers must be established participants in an approved telework program.

(3) Coordinate with the organization's telework managing officer.

3–9. Human resources and emergency relocation group

The organization's COOP program and plan will—

a. Identify ERG positions and identify the positions required to perform the organization's MEFs. Consider the mix of skills, qualifications, experience, rank/grade, and number of persons required to perform and sustain MEFs at alternate facilities including 24/7 operations. The ERG positions and composition are approved in accordance with AR 500–3 by the organization's commander/senior Army official responsible or the delegated immediate deputy/chief of staff, but not a lower echelon or subordinate.

b. Select ERG personnel. Selection will include:

(1) Possession of a security clearance commensurate with the requirements of the MEFs they will be required to perform along with having the security requirements needed for access to specific alternate site(s).

(2) Ability of the ERG member to relocate to a potentially austere environment for up to a 30-day period.

(3) Inform in writing with endorsement by the employee (primary and alternate) designated to fill a position on the COOP ERG at alternate sites of their continuity roles and responsibilities during COOP events and exercises. The signed endorsement acknowledges the person understands and accepts these roles and responsibilities. ERG members can include military, DAC, and contractor personnel. If bargaining unit employees are included as ERG members, organizations must ensure applicable collective bargaining obligations are satisfied. Commanders/senior Army officials responsible or the delegated immediate deputy/chief of staff, but not a lower echelon or subordinate, determine the method used to inform personnel. The method of notification used will be one or more of the following:

(a) A memorandum of appointment including the employee's endorsement signature and date of acknowledgment. See figure 3–2 for a sample ERG appointment memorandum.

(b) The employee's position description.

(c) Applicable orders.

(d) Employee's annual performance appraisal. For DAC, consider inserting an additional performance criteria in the DoD Performance Management and Appraisal Program. This ensures the employee's performance in COOP is being evaluated by the supervisor.

(4) Ensure appropriate language in contracts for contractors who are part of the continuity staff that legally binds and defines the contractor's responsibilities and level of participation during a continuity event. Before designating contractor personnel as an ERG member, coordinate with the responsible contracting officer.

c. Provide information for ERG members (military, DAC, and contractor) to plan and prepare for emergencies, including developing family emergency plans, and to stay informed during a continuity event. Include procedures to contact and account for ERG personnel. Address applicable human resources management issues such as pay, leave, work scheduling, benefits, hiring, authorities, and flexibilities. Guidance on family readiness is available at

https://www.militaryonesource.mil/family-relationships/family-life/preparing-your-family-for-emergencies/creating-a-family-emergency-plan and at www.ready.gov.

d. Designate ERG personnel on the COOP roster. Designate organization personnel (primary and alternate) by name to fill the ERG positions on the COOP roster. This supports A&N of the ERG members. Maintain the COOP roster containing ERG member names as a separate document from the COOP plan with both duty and off-duty contact information for A&N, such as cell phone numbers. Review and update the COOP roster monthly. Describe the procedures for maintaining and publishing up-to-date rosters. Safeguard rosters in accordance with personally identifiable information and other DoD guidelines.

e. Provide a COOP program awareness briefing to all incoming agency personnel during onboarding which provides information, expectations, and procedures for personnel who do not deploy with the ERG to an alternate facility.

f. Establish and maintain the critical capability to account for personnel. Organizations must have the means, process, procedures, and systems in place to contact and account for ERG members and all other employees and communicate this process to all employees.

g. Facilitate coordination among their respective head of human resources, telework managing officer, and CPOC.

h. Address procedures to contact and account for all personnel in the event of a continuity event, including human resources management issues such as pay, leave, work scheduling, benefits, hiring, authorities, and flexibilities.

i. Provide the plan for billeting ERG personnel at or near the CF. Options include billeting within government facilities, as permitted, private or commercial facilities (for example, hotels, motels), and/or use of employee residences if within commuting distance.

j. Address health and medical support available at or in the vicinity of the CF.

k. Provide guidance to ERG personnel concerning the contents and maintenance of individual and office fly-away kits to include clothing, personal items, and prescription medicine. Fly-away kits may also consist of critical office items and records that cannot be prepositioned at alternate sites. Data that is part of a fly-away kit should be backed-up often to minimize data loss in the event of a continuity event.

l. Provide a process and or procedures to communicate the organization's operating status to all staff and stakeholders (for example, 1–800–hotline, website, radio or television broadcast, social media, and email).

m. Incorporate or provide the location or a link to the pandemic influenza–infectious disease plan applicable to the organization which implements mitigation, management, or control measures during a pandemic situation.

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

[Office Symbol] [Date]

MEMORANDUM FOR [NAME OF ERG MEMBER]

FROM: [SUPERVISOR, NAME, OFFICE]

SUBJECT: Appointment as an Emergency Relocation Group Member

1. You have been identified as critical to continuity of agency operations in an emergency situation. By signing below, you are indicating you are able and willing to be appointed as an Emergency Relocation Group (ERG) member for [OFFICE NAME]. ERG members are select personnel assigned to perform mission essential functions (MEFs) when they can no longer be supported from the [PRIMARY/OTHER] facility due to a local, regional, or national change in operating status and the need to operate from an alternate operating facility exists. In a continuity of operations (COOP) plan activation, you shall deploy to your designated alternate location [NICKNAME OF ALTERNATE LOCATION (e.g., Site Tango) (Do not associate with the facility location/address, building name, or host agency)]. Deployment to the alternate location may last for 30 days after an event or until normal operations can be resumed. Additionally, ERG members are required to attend COOP training.

2. Each ERG member is selected by his/her respective department head based upon:

a. The identification of predetermined MEFs that must be performed, regardless of the operational status of the [PRIMARY/OTHER] facility.

b. The employee's knowledge and expertise in performing these MEFs.

3. Designation as a COOP ERG member is a separate process from the identification of essential personnel that must report during government closures. ERG members may be activated during a continuity event or training exercise and do not necessarily support government closures due to lapses in appropriations or weather conditions. More details of the COOP program and plan will be provided during ERG COOP training. If you have questions contact [NAME, CONTACT INFORMATION].

4. I understand and accept my assignment as an ERG member for [OFFICE NAME] as outlined above.

[First, Last Name]_____ [xx-xx-xxxx]_____
Signature of ERG member *Date*

Figure 3–2. Sample emergency relocation group appointment memorandum

3–10. Devolution

Devolution is the capability to transfer statutory authority and responsibility from an organization's primary operating staff and facilities to another designated staff or subordinate organizations and devolution locations to perform and sustain MEFs. A COOP plan's option for devolution describes how an organization will identify and transfer its organizational command and control, as well as responsibility for performing its MEFs to another organization or organizations and personnel at a geographically dispersed location(s) unaffected by the incident. Organizations can activate devolution as a short-term option while ERG members relocate to their alternate location(s). Additionally, organizations can choose to partially devolve by transferring responsibilities for select MEFs or devolve to multiple sites by transferring responsibilities for particular MEFs to various sites. The organization's devolution counterpart (that is, the gaining organization(s) and facilities) must have the capability to perform MEFs as soon as possible but not later than 12 hours after devolution plan activation and must be able to sustain operations for a minimum of 30 days or until normal operations are resumed. When selecting a devolution organization and location, the capabilities of the receiving organization and location must be considered to ensure it has sufficient communications, systems, equipment, and resources prepositioned or available within the accepted timeframe to assume responsibility for performing the MEFs devolving to that devolution site. Personnel assigned devolution responsibilities to perform continuity operations at each gaining organization/site are referred to as the Devolution Emergency Response Group (DERG) and should have the training and skill sets to conduct the specified MEF. The devolving organization and its counterparts must prepare the gaining organization's DERG to conduct continuity operations through the TT&E program. Organizations should also consider the development of support documentation such as training and job aids, standard operating procedures, desk guides, and handbooks. In addition, the organization's COOP OPLAN will—

a. Provide the organization's plan and procedures to devolve organizational control and direction and the responsibility for performing each of its MEFs. Devolution planning addresses the full spectrum of threats and all-hazards emergency events that may render an organization's leadership or staff unavailable to support, or incapable of supporting, the execution of the organization's MEFs from either its primary location or its alternate sites. The organization's devolution plan is a continuity option that can be included in the COOP plan or can be a standalone plan, but it will not be a standalone plan in lieu of a COOP plan. If the devolution plan is a standalone plan, the COOP plan will provide a summary and refer to the devolution plan.

b. Identify for each of the organization's MEFs the counterpart organization which will gain the responsibility to perform that MEF.

c. Coordinate devolution requirements between the devolving organization and the organization or organizations gaining/receiving the responsibility for each devolved MEF. This should include the deliverable or output of each MEF, when it is due and what organization(s) the deliverable/output should be provided, and the contact information for the organizations gaining responsibility for each MEF and the contact information for the organization(s) the deliverable/output should be provided to, including the contract information at their CFs.

d. Identify for each MEF which gaining organization will conduct that MEF if the devolving organization is not available or unable, the contact information for that gaining organization at its primary and alternate facilities, the expected outcome/deliverables for the MEF, and the expected delivery time for the products/deliverables.

3–11. Reconstitution

Reconstitution is the final phase of a continuity event and is the process by which surviving and/or replacement personnel resume normal operations. Reconstitution may occur at any designated location that provides the staff, facilities, and systems necessary to sustain essential functions and activities to resume normal operations. Reconstitution activities re-establish noncritical missions, functions, organizations, resources, and services as they existed prior to the crisis event. Reconstitution is a combination of personnel, facilities, and IT systems and equipment actions taken to rebuild or replace the staff, facilities, and communications and IT capabilities as soon as possible after an event. As an element of continuity, reconstitution concurrently supports sustainment of MEFs while managing the resumption of normal operations. Since reconstitution activities should begin as soon as possible after a continuity event, the organization's COOP OPLAN will identify a reconstitution team by organization and position including the leadership, staff, and resources dedicated and separate from existing continuity support. In most cases, extensive coordination will be necessary to repair or rebuild the original facility or procure a new operating facility, backfill staff, reestablish communications and IT infrastructure, restore essential records, and take other actions to return the organization to normal operations. The organization's COOP OPLAN will—

a. Provide the organization's plan and procedures for reconstitution of staff, facilities, and systems to resume normal operations. Designate the organization's office or position responsible to the senior official to be the lead and POC for reconstitution coordination and activities. Delineate the process, procedures, and responsibilities for initiating and coordinating the organization's reconstitution. Provide information essential to the reconstitution effort including

identification of requirements for facilities, systems, communications, IT, office and conference space, security measures, and other capabilities required to perform all essential functions.

(1) Identify and provide contact information for the internal and external organizations and partners required to conduct and coordinate organization reconstitution of personnel staff (military and DAC), facilities, communications, information systems, and infrastructure.

(2) Identify vendors and contract vehicles to obtain essential services for reconstitution.

b. Focus reconstitution actions on restoration of command staffs, capabilities, and functions. This includes—

(1) Restoring essential C4I. The goals are redundancy and security for communications. Implementation of these goals is determined by the commander/senior Army official responsible for the organization.

(2) Restoring or maintaining communications with higher, lower, and other headquarters and organizations or agencies, as required.

(3) Assessing the organization's remaining capabilities and resources.

(4) Supporting higher headquarters priorities and missions, as applicable.

(5) Allocating resources in support of higher headquarters priority missions, the organization's MEFs, and reconstitution activities.

(6) Restoring all organizational capabilities, functions, and activities to resume normal operations.

3–12. Continuity of operations test, training, and exercises

TT&E events assess and validate continuity plans, policies, procedures, systems, and alternate locations. Initial and recurring training programs inform and familiarize leaders and staff with continuity plans and procedures and their responsibilities. It is critical for organizations to plan and conduct routine, regular internal TT&E events in order to train personnel, evaluate program readiness, and test adequacy and viability of COOP plans, communications, and IT systems. Periodic exercise program events improve the organization's preparedness posture and emphasize the value of integrating continuity functions into daily operations. Corrective actions identified during TT&E events are tracked to completion, ensuring preparedness improvements. An effective corrective action program develops improvement plans which are continually monitored and implemented as part of the larger system of improving preparedness. The organization's COOP program and plan will—

a. Implement its COOP TT&E program strategy and plan to evaluate and validate COOP program capabilities and readiness and train leadership and continuity staff. Test and exercise to assess COOP plans, policies, procedures, communications, information systems, logistics, and facilities. Update and reissue the organization's COOP TT&E program, training plan, and schedule annually.

b. Test and exercise the COOP A&N capability, systems, and procedures to contact the COOP ERG members and provide instructions at a minimum quarterly.

c. Ensure ERG members (primary and alternate) are trained within 90 days of assignment to the ERG. This training will include:

(1) Train ERG members on COOP A&N procedures.

(2) Training on COOP plan execution and procedures and the role and responsibilities of the ERG members.

(3) Onsite training and orientation at the organization's alternate facility(ies) including procedures on arrival, reception, login to information system and accessing essential records, and supporting plans and procedures to perform continuity operations at the alternate facility.

d. Exercise the organization COOP OPLAN at least annually, or more often as directed.

(1) Exercise annually the deliberate and preplanned movement of ERG personnel to an alternate site or sites including the ERG testing of relevant continuity and supporting procedures, communications, and IT systems.

(2) Ensure exercise participants are primary or alternate ERG members. ERG members will complete ERG COOP training before participating in an exercise.

e. Exercise the alternate facilities at least annually including activation, reception, and establishment of continuity operations to test the IT systems that support MEFs and communications to both higher headquarters and subordinate organizations.

f. Assess the OPSEC of COOP execution during exercises.

g. Conduct an after-action review of each exercise and develop an after-action report to capture the lessons learned and items that need to be improved. Maintain the after-action reports for 24 months.

(1) Develop and maintain a corrective action plan. Consolidate items that need to be improved from multiple exercises and training events into the corrective action plan where responsibilities are assigned for making corrections and tracked until the action is complete. Review corrective action plans quarterly by the CWG or PWG and annually by the COOP executive committee or PEC.

(2) Ensure the facility owner, host, contractor, or provider supporting each organization CF conducts an annual assessment and/or test of the CFs' power out emergency circuitry, emergency generators, and power out egress mechanisms during actual power out conditions to determine emergency requirements under simulated disaster conditions. Facility structure, systems design, and operations requirements may affect the assessment and extent of such test.

Section III

Continuity Planning and Plans Requirements

3–13. Additional planning requirements

In addition to the continuity capability planning elements, the organization COOP OPLAN will include—

a. Operations security. The organization's COOP OPLAN will implement effective OPSEC measures to protect the continuity program, plans, facilities, networks, and personnel.

b. Supporting and complementing plans. The organization's COOP OPLAN will identify and reference supporting and complementing emergency management and response plans. Planning includes synchronizing COOP plans and procedures with supporting or complementing emergency response plans such as the Occupant Emergency Plan or building evacuation plan which includes evacuation and shelter-in-place procedures, health protection related pandemic influenza–infectious disease plans, and telework plans.

c. Operations. The COOP OPLAN will—

(1) Describe the COOP concept of operations.

(2) Delineate the executive decision-making process that allows for assessment of a threat, or potential threat situation, and the procedures to execute the plan. Identify execution authority or authorities by position which have the authority to activate the plan. Describe the procedures if plan execution is directed by higher headquarters. Describe the conditions for execution with triggers for executing the plan. Include a decision tree or matrix for plan activation.

(3) Describe the execution process and procedures.

(4) Identify the team and/or procedures for providing critical situational information to the senior leaders (for example, operations center, crisis management cell, crisis action team, and command center).

d. Relocation. The organization's COOP OPLAN will provide the procedures for relocation, reception, in-processing, and startup for the organization's ERG at its CFs. The COOP OPLAN will identify alternate relocation procedures when primary notification or alert systems cannot be implemented.

e. Transportation plan. The COOP OPLAN will describe an executable transportation plan and procedures including primary and alternate means of transportation for movement of ERG members to alternate facilities.

f. Interdependencies. Identify internal and external interdependencies with supporting agencies, ITCP coordinators, and service providers as applicable.

3–14. Continuity of operations plan format

Army organization COOP plans will be operational in design and nature irrespective of the format. Upon COOP execution/activation, a COOP OPLAN automatically becomes an operations order (OPORD).

a. The OPLAN format is recommended. The COOP OPLAN format is a combination of FM 6–0 and the required continuity capability planning elements from DoD guidance derived from national and federal executive branch continuity directives. When not directed by AR 500–3 or requirements in this pamphlet, the commander/senior Army official responsible at each organization is authorized to adjust the OPLAN format to fit mission requirements. See appendix C of this pamphlet for further classification guidance.

b. Recommend using the FM 6–0 five-paragraph format as the basis for the COOP OPLAN and its annexes. The paragraphs are:

(1) Situation.

(2) Mission.

(3) Execution.

(4) Sustainment.

(5) Command and Signal.

c. If an OPLAN format is not used, the COOP plan will be operational in design and execution. The plan will address all requirements of AR 500–3 and this pamphlet as well as applicable subjects normally contained in an executable OPLAN.

Chapter 4
Army Continuity of Operations Program Manager and Continuity of Operations Point of Contact Training

4–1. Overview
Professional continuity training is recommended for Army COOP PMs and CPOCs. This training increases working knowledge of COOP programs and planning and improves effectiveness of the U.S. Army COOP Program. Training consists of Federal Emergency Management Agency (FEMA) material as outlined in table 4–1.

4–2. Professional continuity training for Army continuity of operations program managers and points of contact
a. COOP PMs (ACOMs, ASCCs, DRUs, USAR, and ARNG) are encouraged to obtain the FEMA Level I Professional Continuity Practitioner certification within 2 years of appointment. These courses provide a strategic and tactical perspective of COOP. The FEMA Level I Professional Continuity Practitioner courses are found online at https://www.fema.gov/continuity-excellence-series-professional-and-master-practitioner-continuity-certificate-programs. Organizations should maintain records of personnel that have completed recommended COOP training.

b. HQDA agency CPOCs are encouraged to complete two FEMA courses consisting of the COOP Awareness Course and Introduction to Continuity of Operations.

Table 4–1
Professional continuity training for continuity of operations program managers and continuity of operations points of contact

Training	Time Required (hours)	COOP PM	CPOC
FEMA – Level I Professional Continuity Practitioner	85 – 71 [1]	X	
FEMA COOP Awareness Course, Independent Study 546	1	—	X
FEMA Introduction to Continuity of Operations, Independent Study 547	2	—	X
Total Training Time	—	85 – 71 hours [1]	3 hours

Note:

[1] Time required depends on which classes are selected within the course syllabus.

Appendix A

References

Section I

Required Publications

AR 500–3
U.S. Army Continuity of Operations Program (Cited on title page.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Army publications are available on the Army Publishing Directorate website at https://armypubs.army.mil. DoD publications are available at https://www.esd.whs.mil/dd/.

AGO 2017–07
Designation of the United States Army Cyber Command as an Army Service Component Command, Alignment of the Army's Portion of the Department of Defense Information Network Roles and Responsibilities, Reassignment of United States Army Network Enterprise Technology Command to Army Cyber Command, and Discontinuation of Second Army

AGO 2020–01
Assignment of Functions and Responsibilities within Headquarters, Department of the Army

AR 10–47
U.S. Army Command and Control Support Agency

AR 10–87
Army Commands, Army Service Component Commands, and Direct Reporting Units

AR 11–33
Army Lessons Learned Program

AR 15–1
Department of the Army Federal Advisory Committee Management Program

AR 25–1
Army Information Technology

AR 25–2
Army Cybersecurity

AR 25–30
Army Publishing Program

AR 25–55
The Department of the Army Freedom of Information Act

AR 350–28
Army Exercises

AR 380–5
Army Information Security Program

AR 385–10
The Army Safety Program

AR 525–2
The Army Protection Program

AR 525–26
Infrastructure Risk Management (Army)

AR 525–27
Army Emergency Management Program

AR 530–1
Operations Security

AR 600–20
Army Command Policy

CNSSI 1253
Security Categorization and Control Selection for National Security Systems (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

DA Pam 25–1–1
Army Information Technology Implementation Instructions

DA Pam 25–1–2
Information Technology Contingency Planning

DA Pam 25–403
Guide to Recordkeeping in the Army

DA Pam 385–16
System Safety Management Guide

DA Pam 385–30
Risk Management

DA Pam 525–27
Army Emergency Management Program

DoD Defense Continuity Program (DCP) Security Classification Guide
(Available from Deputy Chief of Staff, G–3/5/7 (DAMO–OD–AOC–COOP), 1E665 Army Pentagon, Washington, DC 20310.)

DoD Dictionary of Military and Associated Terms
(Available at https://www.jcs.mil/doctrine/.)

DoDD 3020.26
DoD Continuity Policy

DoDD 3020.40
Mission Assurance (MA)

DoDD 5100.01
Functions of the Department of Defense and Its Major Components

DoDD 5105.77
National Guard Bureau (NGB)

DoDI 1035.01
Telework Policy

DoDI 3020.42
Defense Continuity Plan Development

DoDI 3020.47
DoD Participation in the National Exercise Program (NEP)

DoDI 6055.17
DoD Emergency Management (EM) Program

DoDI 8440.01
DoD Information Technology (IT) Service Management (ITSM)

DoDI 8500.01
Cybersecurity

DoDI 8510.01
Risk Management Framework (RMF) for DoD Information Technology (IT)

EO 12656
Assignment of Emergency Preparedness Responsibilities (Available at https://www.archives.gov/federal-register/codification/executive-order/12656.html.)

EO 13526
Classified National Security Information (Available at https://www.archives.gov/isoo/policy-documents/cnsi-eo.html.)

Federal Continuity Directive 1
Federal Executive Branch National Continuity Program and Requirements (Available at https://www.fema.gov/media-library/assets/documents/86284.)

Federal Continuity Directive 2
Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process (Available at https://www.fema.gov/media-library/assets/documents/132803.)

FIPS 199
Standards for Security Categorization of Federal Information and Information Systems (Available at https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.)

FM 6–0
Commander and Staff Organization and Operations

NIST SP 800–34 Rev. 1
Contingency Planning Guide for Federal Information Systems (Available at https://csrc.nist.gov/publications/sp.)

NIST SP 800–53 Rev. 4
Security and Privacy Controls for Federal Information Systems and Organizations

UFC 4–010–01
DoD Minimum Antiterrorism Standards for Buildings (Available at https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc.)

36 CFR 1223
Managing Vital Records (Available at https://www.ecfr.gov/.)

44 CFR Chapter 35
Coordination of Federal Information Policy (also known as the Federal Information Security Modernization Act of 2014) (Available at https://www.dhs.gov/cisa/federal-information-security-modernization-act.)

5 USC 3345 et seq.
The Federal Vacancies Reform Act of 1998 (Available at https://uscode.house.gov/.)

10 USC 7013
Secretary of the Army (Available at https://uscode.house.gov/.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil).

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B

Organization Continuity of Operations Plans, Mission Essential Functions, and Supporting Information Technology Contingency Plans

B–1. Organizational continuity of operations plan and service provider information technology contingency plans

a. Continuity planning incorporates cyber resilience. This appendix outlines relationships between the organization COOP plan and IT agency/service provider developed ITCPs which support the COOP plan. See figure B–1. Effective continuity planning requires coordination and synchronization between these plans.

b. Organization continuity of operations plan. The organization COOP plan identifies each MEF, the MTD for each MEF, and the communications, networks, information systems, applications, and websites required to perform each of the organization's MEFs. Organization COOP plans—

(1) Identify the criticality and priority of each organization MEF.

(2) Identify and prioritize the primary and alternate communications and information systems required to perform each MEF.

(3) Coordinate MEF MTD, MEF priority, and system priority with the DCS, G–6 staff, ITCP planner, and service providers who produce the supporting ITCPs.

c. Information technology contingency plans. ITCPs contain applicable system DRPs and ISCPs for the primary and alternate information systems required to perform the MEFs. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency and activates one or more ISCPs for recovery of individual systems. ISCPs provide established procedures for the assessment and recovery of a single system following a system disruption regardless of site or location.

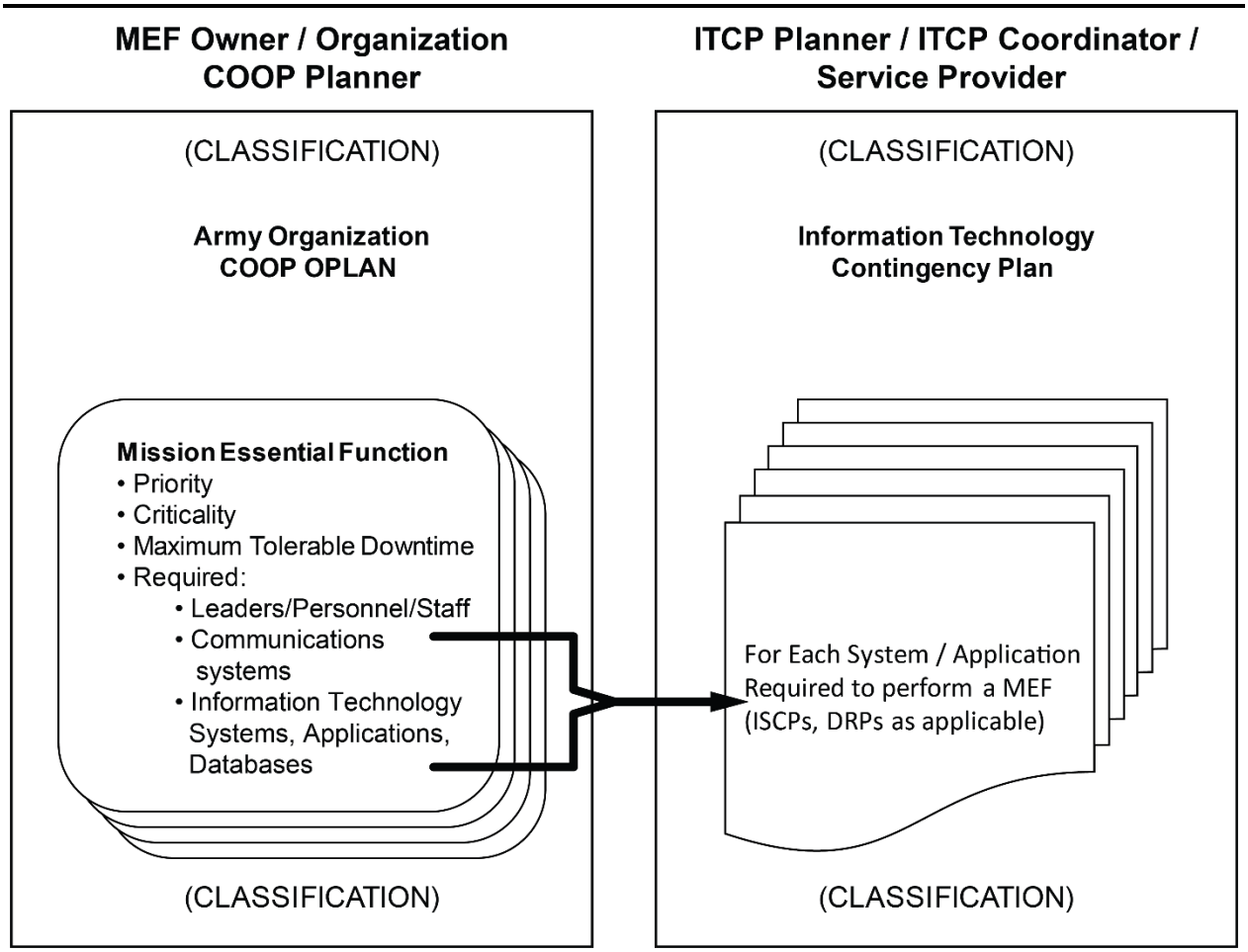

Figure B–1. Organization continuity of operations plan and supporting information technology contingency plans

B–2. Organization continuity of operations planner

a. Mission essential function analyses. Organization COOP planners review the output of the MEF review and any service level agreements to specify and prioritize the communications, records, and information systems required to perform each MEF and associated essential supporting activities.

b. Maximum tolerable downtime. Organizations must analyze and determine acceptable versus unacceptable downtimes for MEFs based on input from the MEF owners and personnel that support those functions and have necessary experience in key areas. The organization's MEF owner determines the MTD for each MEF identified. The MTD is the maximum amount of time acceptable for a disruption to, or degradation of, MEF performance before a mission impact to the organization. When evaluating impacts on each MEF, organizations should also consider whether another organization is able to perform the MEF if they cannot do so within an acceptable timeframe.

c. Coordination. Organization COOP planners coordinate with the ITCP coordinator/ITCP planner to ensure the ITCP for required systems and essential records incorporates elements from the MEF analysis ensuring the recovery time objective (RTO) for each system does not exceed the MTD of the MEF. The example in figure B–2 indicates key information derived from the organization MEF analysis which must be coordinated and synchronized with the ITCP coordinator/ITCP planner/service provider.

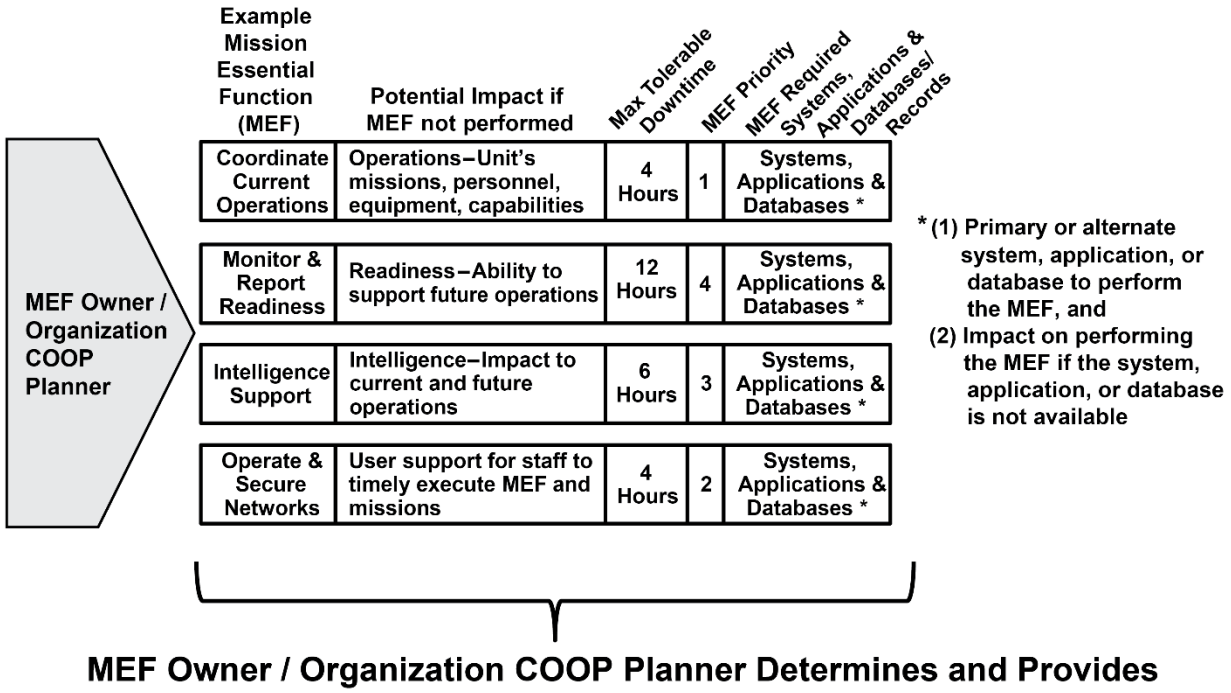

Figure B–2. Example organization continuity of operations plan and mission essential function analysis data

B–3. Relationship of organization continuity of operations plan to information technology contingency plan

Figure B–3 demonstrates an example of the interdependency between an organization COOP plan and the supporting ITCPs for the example MEF titled Monitor and Report Readiness. The figure indicates the framework for cyber resilience.

a. Recovery time objective. The ITCP coordinator/ITCP planner/service provider determines the RTO for each system resource requirement or critical asset identified in the MEF analysis, considering the MTDs for the MEFs it supports. The RTO is a value describing the maximum amount of time that an information system's component, system resource, or a critical asset can be unavailable before it has a failure or unacceptable impact on each of the MEF it supports. The RTO helps to ensure necessary lead time for selecting technologies and resources required to support MEFs within their MTDs.

b. Common terminology. AR 25–2 summarizes the potential impact definitions (low, moderate, and high) for the security objectives confidentiality, integrity, and availability.

(1) *Confidentiality.* Assurance that information is not disclosed to unauthorized entities or processes.

(2) *Integrity.* The degree of protection for data from intentional or unintentional alteration or misuse.

(3) *Availability.* The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

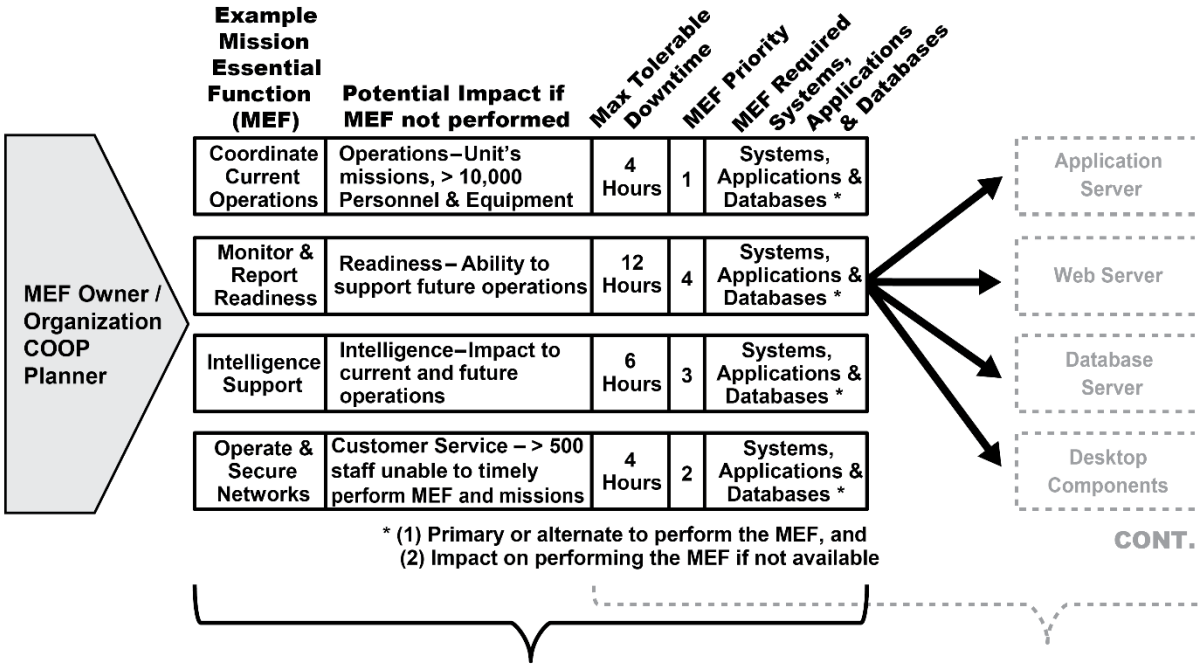

Figure B–3. Example organization continuity of operations plan and mission essential function analysis relationship to information technology contingency plans

Appendix C

Security Classification Guidance

C–1. Security classification

This appendix applies to the HQDA Secretariat and Staff, ACOMs, ASCCs, DRUs, the Regular Army, the ARNG/Army National Guard of the United States, USAR, the U.S. Army Corps of Engineers, FOAs, Army-owned and Army-managed garrisons, facilities, and civil works projects, and Army subordinate commands that support Army COOP activities. General Army security classification guidance is contained in AR 380–5 and this pamphlet. AR 380–5 contains detailed information on marking documents, transmitting procedures, and other classification instructions. For official use only (FOUO) is a designation that is applied to unclassified information which is exempt from mandatory release to the public under the Freedom of Information Act. AR 25–55 contains the definition and policy application of FOUO markings. The DoD Defense Continuity Program Security Classification Guide provides guidance on the classification of information pertaining to defense continuity programs and plans. If there is any conflict in this appendix with AR 380–5, the most recent publication takes precedence. Security classification will be commensurate with the overall content of the document, the DoD Defense Continuity Program Security Classification Guide, and applicable program and organizational mission security classification guidance.

C–2. Recommended changes

Recommended changes to this appendix with appropriate justification should be sent through command or staff channels to Deputy Chief of Staff, G–3/5/7 (DAMO–OD–AOC), 3200 Army Pentagon, Washington, DC 20310–3200.

Appendix D

Sample Assessment Checklist

This notional assessment checklist may be adjusted, as applicable, to the organization and local conditions.

D–1. Program implementation and management

a. Has a CPOC (primary and alternate) been designated in writing within operational channels or an organizational staff best suited to execute the organization's COOP program and OPLAN?

b. Do headquarters organizations' CPOCs maintain a roster of their subordinate echelon (staff sections and commands) primary and alternate CPOCs with contact information (phone numbers)?

c. Do CPOCs oversee their COOP program and interface with their higher headquarters COOP program office?

d. Do primary and alternate CPOCs have individually assigned, dedicated SIPRNET access/connectivity vice using a general use office SIPRNET?

e. Has the ACOM, ASCC, DRU, ARNG, USAR, or agency provided program implementation and planning guidance about organization unique requirements in accordance with supplementation guidance in AR 500–3?

f. Are ERG members (primary and alternate) informed in writing of their continuity roles and responsibilities? Does the organization obtain a signed acceptance of these roles and responsibilities from the DAC ERG member?

g. Do statements of work for contractors with COOP responsibilities reflect clearly that they are emergency essential and/or specify what their nonroutine office duties are (for example, travel, 24-hour on-call duties, 24-hour exercise duties, and so on)?

h. Is a CWG organized and functioning? Is documentation of meeting content, actions, and attendance maintained for the preceding 24 months?

i. Does COOP program management and plans incorporate risk management factors including risk assessment and risk mitigation considerations?

j. Does the COOP program identify, prioritize, and justify requirements to plan, program, and budget resources to develop and maintain the organization's continuity capabilities? Does the budget include acquisition of the resources necessary to deploy personnel; develop, equip, and maintain CFs, systems, and applications; conduct a realistic COOP TT&E program; and obtain and stock supplies to sustain continuity operations at alternate facilities for a minimum of 30 days or until normal operations are resumed? Do COOP managers work with other offices and agencies to plan and budget for continuity program requirements in accordance with the command's budget process? Does the COOP manager maintain documentation of COOP budget requests and funding outcomes?

k. Does the COOP PM/CPOC develop and implement a MYSPMP that provides for the development, maintenance, and annual review of continuity capabilities to ensure critical activities and resources are acquired to sustain program support and continuous improvement efforts? Is the COOP program reviewed internally annually?

l. Do COOP PMs/CPOCs capture data, track, analyze, and review COOP program readiness metrics and report the readiness to execute the organization's COOP OPLAN to the CWG and leadership?

m. Is the COOP OPLAN designed to be activated with or without warning during duty hours and nonduty hours?

n. Is the COOP OPLAN executable, trained to, tested, and exercised?

D–2. Mission essential functions

a. Does the COOP OPLAN contain the organization's identified, prioritized MEFs?

b. Are the MEFs reviewed and updated at least every 2 years in conjunction with the organization's COOP OPLAN revision? If the organization had a significant mission change or reorganization, was a MEF review conducted?

c. Are the organization's MEFs validated and approved by the commander/senior Army official responsible or the delegated immediate deputy/chief of staff, but not a lower echelon or subordinate?

d. Does MEF identification determine those directed by applicable laws, presidential directives, executive orders, and other policies or directives?

e. Does MEF identification determine functions that directly support an essential function performed by another organization?

f. Does MEF identification determine functions that need to be continued, uninterrupted, or resumed as soon as possible but not later than 12 hours for up to a minimum of 30 days following a change in normal operations?

g. Do the organization's COOP program and COOP OPLAN develop, maintain, identify, and prioritize MEFs in accordance with guidance contained within AR 500–3 and this pamphlet?

h. Has the organization identified the criticality and priority of each of its MEFs and coordinated such with DCS, G–6 staff, ITCP coordinators, and service providers who produce the supporting ITCP?

i. Does MEF review and analysis identify the communications, networks, information systems, applications, and websites required to perform each of the organization's MEFs? Is this coordinated with service providers developing supporting ITCPs?

j. Are the primary and alternate secure and nonsecure communications, IT networks, information systems, applications, and websites required to perform each MEF identified?

k. Do subordinate organizations or activities with MEFs develop and maintain their own supporting COOP OPLANs and procedures?

l. Are procedures established for the improvisation or emergency acquisition of resources necessary to execute MEFs?

m. Are the organization's capabilities and procedures needed to relocate ERG personnel to CFs to support MEFs identified and defined?

n. Are other organization(s) identified to receive each devolving MEF if the primary organization is unable to perform its MEF?

o. Are the capabilities to execute MEFs at the CFs available for a minimum of 30 days or until normal operations are resumed?

D–3. Order of succession

a. Does the organization's COOP OPLAN identify the order of succession at least three positions deep for the position of organization head and key positions?

b. Does the organization's COOP OPLAN describe the process and procedures governing succession to office?

c. Do orders of succession comply with AR 600–20 and the Vacancies Reform Act of 1998, as amended (see 5 USC 3345 et seq.), if applicable?

D–4. Delegations of authority

a. Does the organization's COOP OPLAN identify and delineate preplanned delegations of authority needed to assure execution of the organization's COOP plan and sustain performance of MEFs during a continuity event?

b. Does the organization establish and document, in writing, for the legal delegation of authorities?

c. Does the delegation of authority document outline explicitly the authority, including any exceptions to that authority, of an official so designated to exercise organizational direction?

d. Does the delegation of authority delineate the limits of authority and accountability?

e. Does the delegation of authority outline the authority of officials to redelegate functions and activities, as appropriate?

f. Does the delegation of authority define the circumstances under which delegation of authorities would take effect and would be terminated?

g. Does the delegation of authority incorporate the conditions under which the delegations would take place, the method of notification, the duration the delegations may last, conditions when the delegation may be terminated, and any temporal, geographical, or organizational limitations to the authorities granted by the delegation of authority(ies), including the ability to redelegate authorities?

h. Does the organization inform the officials listed within the delegations of authority in writing who might be expected to assume authorities in a continuity activation?

i. Does the organization establish procedures for notifying appropriate personnel upon implementation of the delegation of authority?

j. Does the organization coordinate development and revision of delegations of authority with General Counsel to ensure legal sufficiency?

k. Does the organization's delegations of authority include authorities that are required to support devolution of MEFs to the commands or organizations gaining/receiving the MEFs?

D–5. Continuity communications, information systems, and information technology services

a. Does the organization's COOP OPLAN identify the primary and alternate communications and information systems that support each MEF?

b. Does the organization's COOP OPLAN identify the applications, websites, and networks required to perform each of its MEFs? Does the organization coordinate the criticality and priority of each of its MEFs with G–6, ITCP coordinators/planners, and service provider agencies for integration into communications and ITCPs and resilience planning efforts supporting the organization's COOP plan?

c. Does the organization's COOP OPLAN incorporate cyber resilience in order to maintain performance of MEFs in the event of network disruption and degradation?

d. Does the organization's COOP plan provide for communications capabilities, their maintenance, and are continuity personnel trained in their use?

e. Are communications capabilities provided to support the organization's senior leadership while they are in transit to alternate locations?

f. If the organization shares an alternate location and communications capabilities with other organizations, is there a signed agreement with the system owner to ensure each has adequate access to communications resources?

g. Does the organization's COOP OPLAN indicate the MTD for each MEF?

h. Are WPS on cellular phones issued to continuity personnel who perform MEFs and/or other continuity team personnel, as determined by the organization?

i. Are GETS cards issued to continuity personnel as determined by the organization and its mission?

j. Are GETS cards prepositioned for emergency use at all primary and CF locations as determined by the organization and its mission?

k. Are primary and alternate locations involved in the performance of MEFs and/or other sites designated by the organization enrolled in the Telecommunications Service Priority Restoration Program, as applicable?

l. Are organizational, command, and national continuity communications plans (as appropriate) reviewed annually for accuracy to ensure they are capable of supporting MEFs?

D–6. Essential records

a. Does the organization COOP OPLAN identify essential records required to perform the organization's MEFs and support reconstitution of normal operations?

b. Does the organization's COOP plan identify essential records and procedures including information systems and applications, electronic and hardcopy documents, references, databases, and records, to include classified or sensitive data needed to perform MEFs? Are essential records safeguarded, available, and accessible to support continuity operations at alternate facilities and devolution locations?

c. Does the organization COOP OPLAN provide for ERG personnel to have appropriate access at alternate locations to required media (for example, paper, photographic film, microform, and/or electronic forms), equipment, and instructions for retrieval of essential records including, but not limited to, records stored in cloud-based applications and accessed via the internet or a virtual private network?

d. Does the organization's CPOC/COOP planner coordinate essential records replication and availability requirements with the IT community's ITCP coordinators, ITCP planners, or service providers, in order to integrate with and inform the IT community's development of communications and information systems contingency planning, resilience planning, and service level agreements?

D–7. Continuity facilities

a. Does the COOP OPLAN identify the organization's CFs used to perform its MEFs?

b. Does the COOP program/plan identify policy and guidance for storing, protecting, replicating, and accessing essential records, materials, and databases required to execute MEFs at CFs?

c. Do MEF owners have alternate means at CFs to access web-based essential documents, references, databases, and records should web access be unavailable, such as electronic records stored at CFs or hardcopy documents?

d. Does the organization's COOP OPLAN identify one or more CFs to be used during permissive or nonpermissive environments when the primary operating location is threatened or becomes unusable?

e. Does the organization's COOP OPLAN identify at least one CF located in an area separated from the primary facility geographically so that it would not be impacted by the most likely hazard events, such as a hurricane, flooding, tornados, earthquake, and resulting extended utility outages for electric power, communications, and water for life support for the ERG?

f. Have assigning, training, and equipping augmentation organizations to facilitate evacuation, shelter-in-place, and other COOP related requirements, as deemed necessary, been considered by leadership?

g. Do CFs comply with the Americans with Disabilities Act and are they accessible and designed for handicapped personnel?

h. Are CFs capable of permitting ingress and egress during power out conditions? Procedures for routine and emergency ingress and egress must consider assigned and visiting able-bodied and handicap personnel, including during power out conditions.

i. Does the organization with alternate locations that are not owned or leased by the U.S. Government have a current, signed MOA/MOU with the owner or occupant of the facility? Is the MOA/MOU reviewed in conjunction with the COOP OPLAN review and following leadership changes?

j. Does the MOA/MOU specify requirements to have the CF configured for occupancy to perform MEFs as soon as possible, but not later than 12 hours after notification and the capability to sustain continuity operations for a minimum of 30 days or until normal operations are resumed?

k. Does the MOA/MOU provide details of the space and services to be provided at the CF?

l. Does the MOA/MOU provide access control procedures to the allocated space during occupancy?

m. Does the organization's COOP OPLAN identify the capabilities and procedures needed to relocate ERG members to alternate facilities/sites/headquarters to perform MEFs?

n. Does the organization COOP OPLAN establish and maintain alternate locations for relocation of ERG personnel during disruptions to normal operations?

o. Does the organization review its CFs for suitability and functionality annually?

p. Does the organization plan establish and implement procedures for relocation, reception, in-processing, and startup for the organization's ERG at its CFs?

q. Does the organization coordinate with site facility managers to ensure availability of space, connectivity, communications, information systems, IT networks, and services?

r. Does the COOP OPLAN ensure the capabilities required to perform MEFs exist at CFs prior to activation, or become available as soon as possible but not later than 12 hours after activation?

s. Does the CF have the capability to ensure performance of MEFs with minimal disruption of operations for a minimum of 30 days or until normal operations are resumed?

t. Does the COOP OPLAN provide for replication of essential records and capabilities by providing systems and configurations that are used in daily activities?

u. Does the CF have the capability to access and use essential records required to perform MEFs?

v. Does the CF provide interoperable communications, including secure communications if appropriate, with all identified internal and external partners and stakeholders?

w. Does the CF provide computer equipment, software, information systems, and other automated data processing equipment necessary to perform MEFs?

x. Does the CF provide for the availability of essential resources such as food, water, fuel, medical, and municipal services to ensure the health, safety, and security of the facility and personnel?

y. Does the CF provide for emergency/back-up power capability in the event the primary power source is disrupted?

z. Does the COOP OPLAN provide for lodging to support ERG personnel at or near the facility? Options include billeting within the facility, private or commercial facilities (for example, hotels, motels), and/or use of employee residences if within commuting distance.

aa. Does the COOP OPLAN provide a transportation support plan that details transportation to, from, and at the physical alternate location for ERG members?

bb. Does the CF provide sufficient levels of physical and information security to protect against all threats, as identified in the facility's risk assessment and physical security surveys? This includes sufficient personnel to provide perimeter, access, and internal security, as required by organizational policy.

D–8. Human resources

a. Does the organization's COOP OPLAN develop and implement processes to identify, document, and prepare ERG personnel to conduct or support continuity operations?

b. Does the organization's COOP OPLAN define the expectations, roles, and responsibilities of ERG personnel?

c. Does the organization's COOP program/plan provide procedures to inform DAC personnel who are ERG members (primary and alternate) in writing of their continuity roles and responsibilities? Does the organization obtain a signed acceptance of these roles and responsibilities? See a sample ERG appointment memorandum at figure 3–2.

d. Does the organization's COOP program/plan maintain a COOP roster of trained personnel capable of performing COOP operations? Is the roster reviewed monthly and updated as necessary?

e. If bargaining unit employees are included as ERG members, are applicable collective bargaining obligations satisfied?

f. Does the organization's COOP program/plan provide guidance to ERG members on individual preparedness measures they should take to ensure response to a COOP plan activation?

g. Does the organization's COOP plan recommend the content and maintenance of fly-away kits for deploying continuity personnel?

h. Does the organization's COOP program/plan provide or reference related emergency response plans and planning guidance to assist staff in preparing, planning, and staying informed during an emergency, procuring an emergency supply kit, making a family emergency plan, and being informed about the different types of emergencies that could occur and their appropriate responses?

i. Does the organization's COOP program/plan provide the ability to communicate with and coordinate activities with noncontinuity personnel?

j. Does the organization's COOP program or plan provide or reference related guidance on roles and responsibilities of non-ERG personnel during a continuity event? Does the program/plan communicate how, and the extent to which, employees are expected to remain in contact with their organizations during any emergency situation?

k. Does the COOP plan address procedures to contact and account for all personnel in the event of a continuity event during both duty and nonduty hours?

l. Does the COOP plan provide a process and procedures to communicate the organization's operating status to all staff and stakeholders (for example, 1–800–hotline, website, radio or television broadcast, email)?

m. Does the COOP plan address human resources management issues such as pay, leave, work scheduling, benefits, hiring, authorities, and flexibilities?

n. Does the COOP plan provide procedures and the ability to communicate and coordinate activities with all personnel, CFs, support teams, and entities the affected organization interacts with (other organizations, customers, and stakeholders) during and after a continuity event, including alerts and notification?

D–9. Devolution

a. Does the COOP plan establish procedures for the devolution of organization control and direction?

b. Does the COOP plan identify the counterpart gaining organization or organizations for each of its MEFs?

c. Does the devolution plan specify the deliverable or output of each MEF and when it is due?

d. Does the devolution plan specify what organization(s) are to receive the deliverable or output of each MEF?

e. Does the devolution plan specify the contact information for the organizations gaining the responsibility for each MEF? Does it specify the contact information for the organization(s) the deliverable/output should be provided to, including the contact information at their CFs?

f. Does the devolution plan indicate coordination with each gaining organization about how it designates, trains, and activates its DERG?

D–10. Reconstitution

a. Does the COOP plan designate the organization's reconstitution manager/office/position to oversee the reconstitution process? Does the plan identify a reconstitution team with leadership, staff, and resources dedicated and separate from existing continuity support?

b. Does the reconstitution planning provide a plan and procedures to begin recovery from the effects of a disruption of operations and to support the transition back to normal operations once a threat or disruption has passed?

c. Does the reconstitution plan describe how the organization will assess the status of its affected personnel, assets, and facilities?

d. Does the reconstitution plan outline procedures for conducting a smooth transition from the CF back to either the normal primary facility, another temporary facility, or a new permanent facility?

e. Does the reconstitution plan describe how the organization will verify operational capability and availability of systems, communications, essential records, infrastructure, and other required resources?

f. Does the reconstitution plan identify how the organization will determine if any records were affected by the incident to ensure an effective transition or recovery of essential records?

g. Does the reconstitution plan describe how the organization will instruct all personnel on how to resume normal operations?

D–11. Continuity of operations test, training, and exercise program

a. Does the organization test the COOP A&N process, procedures, systems, and capability to contact the organization's ERG members at a minimum quarterly?

b. Does the organization test, assess, and exercise its COOP plan at least annually to provide assurance that MEF can be performed across a spectrum of contingencies, threats, events, and emergencies?

c. Does the organization's COOP TT&E program conduct annual activities to test, exercise, and validate its COOP plan and capabilities?

d. Are the ERG members and other COOP personnel who may carry classified information outside of their normal place of duty issued current courier cards to the extent determined by the COOP PM/CPOC?

e. Does the organization coordinate tests and exercises with planned gaining organizations to prepare its DERG for continuity operations as a result of devolution?

f. Are tests conducted at least annually to assess and/or test the organization's alternate facilities' power out emergency circuitry, emergency generators, and power out ingress and egress mechanisms during actual power out conditions to determine emergency requirements under simulated disaster conditions?

g. Are corrective actions, lessons learned, metrics, tracking mechanisms, formats, and/or procedures reviewed annually by a senior Army official? (See AR 11–33 and AR 350–28 for guidance.)

h. Are corrective action plans reviewed quarterly by the CWG or PWG and annually by the COOP executive committee or PEC?

i. Is OPSEC considered in the planning, conduct, and evaluation of exercises?

j. Does the ACOM, ASCC, DRU, USAR, or ARNG assess subordinate organizations that have a COOP program/plan (that is, have MEFs) and those organizations that are designated to receive and conduct MEFs as a gaining organization during a devolution situation as a part of the command's Organizational Inspection Program in accordance with AR 525–2?

D–12. Additional plan requirements

a. Does the organization's COOP plan identify OPSEC measures to protect the continuity program, plans, facilities, networks, and personnel?

b. Does the organization's COOP plan identify and reference supporting and complementary emergency management and response plans?

c. Does the organization's COOP plan describe operations including the concept of operations, the execution process and procedures, the decision-making process, the execution authorities, and the conditions that trigger execution of the plan?

d. Does the organization's COOP plan identify the team and/or procedures for providing critical situational information to the senior leaders (for example, operations center, crisis management cell, crisis action team, and command center)?

e. Does the organization's COOP plan provide the procedures for relocation, reception, and startup for the organization's ERG at its CFs?

f. Does the organization's COOP plan describe an executable transportation plan and procedures including primary and alternate means of transportation?

g. Does the organization's COOP plan identify interdependencies with partners, supporting agencies, and service providers as applicable?

Glossary

Section I

Abbreviations

A&N
alert and notification

ACOM
Army command

AKO
Army Knowledge Online

AOC
Army Operations Center

AR
Army regulation

ARNG
Army National Guard

ASCC
Army service component command

C4I
command, control, communications, computers, and intelligence

CF
continuity facility

COOP
continuity of operations

CPOC
continuity of operations point of contact

CWG
Continuity of Operations Working Group

DA Form
Department of the Army form

DA Pam
Department of the Army pamphlet

DAC
Department of the Army Civilian

DCS
Deputy Chief of Staff

DERG
Devolution Emergency Response Group

DoD
Department of Defense

DRP
disaster recovery plan

DRU
direct reporting unit

ERG
emergency relocation group

FE
functional exercise

FEMA
Federal Emergency Management Agency

FM
field manual

FOA
field operating agency

FOUO
for official use only

FSE
full-scale exercise

GETS
Government Emergency Telecommunications Service

HQDA
Headquarters, Department of the Army

ISCP
information system contingency plan

IT
information technology

ITCP
information technology contingency plan

MEF
mission essential function

MOA
memorandum of agreement

MOU
memorandum of understanding

MTD
maximum tolerable downtime

MYSPMP
multiyear strategy and program management plan

NIST SP
National Institute of Standards and Technology Special Publication

OPLAN
operations plan

OPSEC
operations security

PEC
Protection Executive Committee

PM
program manager

POC
point of contact

PWG
Protection Working Group

RTO
recovery time objective

SC
senior commander

SIPRNET
secure internet protocol router network

TT&E
test, training, and exercise

TTX
tabletop exercise

UFC
United Facilities criteria

USAR
U.S. Army Reserve

USC
United States Code

WPS
Wireless Priority Service

Section II

Terms

All-hazards
A classification encompassing all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects. Examples include, but are not limited to accidents, technological events, natural disasters, space weather, domestic and foreign-sponsored terrorist attacks, acts of war, weapons of mass destruction, and chemical, biological (including pandemic), radiological, nuclear, or explosive events.

Alternate facility, alternate site, alternate headquarters, or alternate location
See "continuity facility."

Army Protection Program
The overarching leadership framework to integrate, coordinate, synchronize, and prioritize protection policies and resources among the functional elements and their associated enabling functions.

Continuity facility
Facilities, sites, locations, and platforms where essential functions are continued or resumed during a continuity event (for example, alternate facility, alternate headquarters, alternate location, or alternate site). Locations, other than the primary facility, used to carry out MEFs by relocating ERG members following activation of the COOP plan. This includes devolution sites and devolution locations used to carry out essential functions by devolving the organization's MEFs to geographically separated facilities and staffs following activation of the COOP plan's devolution option/plan. These facilities also refer to work arrangements such as telework and mobile work concepts.

Continuity of operations
An internal effort within each agency/organization to ensure essential functions continue to be performed during disruption of normal operations.

Corrective action program
An organized method of documenting, assigning responsibilities for action, and tracking improvement actions until complete for an organization's continuity program.

Delegation of authority
Identification, by position, of the authorities for making policy determinations and decisions at headquarters, regional and field levels, and all other organizational locations. Generally, predetermined delegations of authority will take

effect when normal channels of direction have been disrupted and will lapse when these channels have been reestablished.

Devolution
The transfer of statutory authority and responsibilities for performance of MEFs from an organization's primary operating staff to other employees internal or external to the organization in order to sustain essential functions for an extended period. Devolution is a continuity option used instead of, or in conjunction with, relocation in order to ensure the continued performance of essential functions.

Emergency relocation group
The selected individuals of the organization's staff and leadership prepared to move to designated alternate facility(ies) and perform essential functions in response to emergencies or contingencies that threaten the operations of the organization.

Emergency relocation staff
A subset of the ERG. The collective ERG may be subdivided into emergency relocation staffs that deploy to different alternate sites.

Essential records
Information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity event. The two basic categories of essential records are emergency operating records and rights and interest records. Emergency operating records are essential to the continued functioning or reconstitution of an organization. Rights and interest records are critical to carrying out an organization's essential legal and financial functions and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. The term "vital records" refers to a specific subset of essential records relating to birth, death, and marriage documents.

Essential supporting activities
Functions that support performance of MEFs but do not reach the threshold of MEFs. Essential supporting activities are important facilitating activities performed by most organizations (for example, providing a secure workplace and managing the personnel payroll system); however, the performance of essential supporting activities alone does not directly accomplish an organization's MEFs.

Exercises
Two types of exercises, discussion-based and operations-based, are useful as part of a comprehensive COOP TT&E program depending on the purpose, scope, and objectives.
a. Discussion-based exercises include seminars, workshops, tabletop exercises (TTXs), and games. These types of exercises are used to familiarize players with, or develop new, plans, policies, agreements, and procedures. Discussion-based exercises focus on strategic, policy-oriented issues. A TTX is intended to generate discussion of various issues regarding a hypothetical, simulated continuity event. TTXs are used to improve general awareness, validate plans and procedures, rehearse concepts, and/or assess the types of systems needed to guide the response to a defined continuity event. Generally, TTXs are aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in attitudes.
b. Operations-based exercises include drills, tests, functional exercises (FEs), and full-scale exercises (FSEs). These exercises are used to validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps. Operations-based exercises are characterized by actual reaction to an exercise scenario, such as initiating communications or mobilizing personnel and resources. FEs are designed to validate and evaluate one or more capabilities, functions and/or subfunctions, or interdependent groups of functions. FEs are focused on exercising plans, policies, procedures, a system or systems, infrastructure, and staff members involved in management, direction, command, and control functions. Events and event updates are promulgated through an exercise scenario that drives activity at the management level. An FE is conducted in a realistic, real-time environment; however, movement of personnel and equipment is usually simulated. An FSE is more complex and involves multiple agencies, organizations, commands, and validates many facets of preparedness including supporting procedures, logistics, and agreements. Events are introduced through an exercise scenario with event updates that drive activity at the operational level. FSEs are usually conducted in a real-time, stressful environment that is intended to mirror a real event. Personnel and resources are mobilized and deployed to perform actions as if a real event had occurred. The FSE simulates reality by presenting complex and realistic problems that require critical thinking, problem solving, and responses by trained personnel.

Geographic dispersion
The distribution of personnel, functions, facilities, and other resources in physically different locations from one another.

Information system contingency plan
Provides established procedures for the assessment and recovery of an information system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. An ISCP supports, but is not, an organization COOP plan. Refer to NIST SP 800–34 Rev. 1 for additional information.

Information technology contingency plan
Provides procedures and capabilities for recovering and sustaining an IT system, capability, or application. An ITCP is a part of a continuity planning, but it is not an organization COOP plan. ITCPs support the organization COOP plan. An ITCP can be enacted without enacting a COOP plan. See DA Pam 25–1–2 for additional details.

Maximum tolerable downtime
The maximum amount of time acceptable for a disruption to, or degradation of, MEF performance before a mission impact to the organization. The organization's MEF owner determines the MTD for each MEF identified. When evaluating impacts on each MEF, organizations should also consider whether another organization is able to perform the MEF if they cannot do so within an acceptable timeframe.

Mission assurance
A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains critical to the execution of DoD MEFs in any operating environment or condition.

Mission essential function
Select functions directly related to accomplishing the organization's mission. Failure to perform or sustain these functions would significantly affect the organization's ability to provide vital services or exercise authority, direction, and control. MEFs are the limited set of the organization's normal mission functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

Order of succession
A formal, sequential listing of organization positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role under specific circumstances.

Reconstitution
Actions taken to re-establish an organization or the capabilities of an organization that have been destroyed or severely damaged. Also refers to the period in the post-attack environment when military activities re-establish noncritical missions, functions, organizations, resources, and services as they existed prior to the crisis event. Reconstitution is a combination of personnel, facilities, and IT systems and equipment actions taken to rebuild or replace the staff, facilities, and communications and IT capabilities as soon as possible after an event. Reconstitution may continue for an extended period until normal operations are resumed from the original or replacement primary operating facilities.

Recovery
The implementation of prioritized actions required to return an organization's essential functions, systems, processes, and support functions to operational stability following an interruption or disaster. Recovery may be initiated from any safe operating location. Recovery actions will generally start as soon as possible and can run concurrently with the relocation or reconstitution process. Recovery actions include execution of applicable supporting IT operations DRPs and related ISCPs.

Recovery time objective
A value describing the maximum amount of time that an information system's component, system resource, or a critical asset can be unavailable before it has a failure or unacceptable impact on each of the MEFs it supports. The organization's IT contingency plan coordinators/IT contingency planners determine the RTO for each system resource requirement or critical asset identified in MEF analysis, considering the MTDs for the MEFs it supports. The RTO helps to ensure necessary lead time for selecting technologies and resources required to support MEFs within their MTDs.

Relocation
The movement of the ERG to a CF or facilities for purposes of maintaining command and control and conducting MEFs on a continuous basis.

Resilience
The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

Risk management
a. A continual process or cycle where risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and risk avoidance (see DA Pam 525–27).
b. A continuous process applied across the full spectrum of Army training and operations, individual and collective day-to-day activities and events, and base operations functions to identify and assess hazards/risks, develop and implement controls, make decisions, and evaluate outcomes; blends tactical, threat-based risks with accidental, hazard-based risks (see AR 380–5).

Senior commander
Command of Army installations is exercised by a senior commander (SC). The SC is designated by senior Army leadership. The SC's command authority over the installation derives from the Chief of Staff, Army and the Secretary of the Army's authority over installations. This is a direct delegation of command authority for the installation to the SC. The SC's command authority includes all authorities inherent in command including the authority to ensure the maintenance of good order and discipline for the installation (see AR 600–20 and AR 525–27).

Test, training, and exercises
Activities designed to familiarize, impart skills, and ensure viability of continuity plans. TT&E aids in verifying that an organization's COOP plan is capable and ready to support the continued execution of the organization's essential functions throughout the duration of a continuity event.