A WHITE PAPER

Federal Continuity of Operations

Part 10 of 10: Continuity of Operations (COOP) Plan

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATIONS FEDERAL INFORMATION SYSTEMS

Topic Summary

Smaller federal agencies and programs often do not implement Continuity of Operations (COOP) Plans because such planning does not meet the bar required of a “national essential function.” This impacts national security because:

- Preventable service disruptions can occur, with subsequent loss of availability.
- Disruptions within many smaller programs each year aggregate into significant failure.
- Misunderstanding the interrelationships between smaller and larger programs adds unnecessary risk.

This paper analyzes policy from the commercial, federal, DOD, and Army levels to argue that most (if not all) programs within the public sector should implement cost-efficient COOP Plans. A reference COOP Plan derived from the Federal Emergency Management Agency (FEMA), tailored to a small Army Program use case, provides a valuable strategy and planning asset for the COOP practitioner within the federal space.

Executive Summary

To prepare for the next Big Disaster is Big Business for the federal government and the Department of Defense (DoD). A brief glance at the headlines highlights sobering statistics for the year 2011:

- *Natural disaster costs blow all budgets.*[1] The first six months of 2011 are the costliest on record for property damages, and not only because of the February earthquakes in New Zealand or the March tsunami in Japan. In the United States alone, 98 weather events accounted for over $27 billion of damage. Munich Re (a multinational insurer of insurance companies) pegs losses worldwide at well over $265 billion. In the event of a natural disaster, an organization can lose its primary facility within hours.
- *Cyber-attacks siphon funds from businesses of all sizes.* Federal agencies and businesses of all sizes are lucrative targets for cyber-criminals; a USA Today article finds that cyber-attackers are increasingly targeting even small businesses,[2] while a CNN report highlights that undetected cyber penetrations of businesses are increasing and that the "first three months of 2011 has seen a record number of new malicious software."[3] As the recent Sony debacle shows, corrupted data and systems resulting from such breaches can easily affect an business unit's ability to operate.[4]
- *Terrorists target the U.S. government.* While everyone in the country knows of the 9/11 attacks and the Oklahoma City bombings, it may not be obvious that international criminals continue their misguided and malignant efforts every day. A February 2011 article reports that U.S. government facilities remain of high interest to these enemies of freedom.[5] Such threats pose a clear and present danger to federal programs.

Threats falling within any of these categories can hinder a federal agency's ability to complete its mission. Presidents Bush and Obama have enacted wise provisions to protect the federal government; in particular, Bush's National Continuity Policy seeks to preserve constitutional governance of the United States, regardless of any threat (manmade) or hazard (natural).

This paper, the culmination of a series of ten papers on Continuity of Operations (COOP), builds on this overarching Executive Branch policy to see how it can be practically applied to a small Army Program as a use case. The paper analyzes COOP policy and planning, as well as implementation templates, and closes by applying a sample COOP Plan to the Army Program. A budget and time estimate, along with recommendations, provides the COOP practitioner with a workable and practical COOP Plan reference guide. COOP practitioners throughout the federal space benefit from this reliable and best-practice guide; the nation benefits from the assurance that, with even small programs protected by COOP Plans, large swaths of the federal government and DoD will have the organizational resilience to face disasters and threats securely, reliably, and with confidence.

[1] Miguel Llanos. "2011 already costliest year for natural disasters," *today.msnbc.msn.com*, July 12, 2011. http://today.msnbc.msn.com/id/43727793/ns/world_news-world_environment/ (accessed: July 14, 2011).

[2] Byron Acohido. "New cyberattacks target small businesses," *USATODAY.com*, July 4, 2011. http://www.usatoday.com/tech/news/2011-07-04-small-business-cyber-attackss_n.htm (accessed: July 14, 2011).

[3] Kevin Voigt. "Analysis: The hidden cost of cybercrime," *CNN*, June 7, 2011. http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html (accessed: July 14, 2011).

[4] Greg Thom. "Sony restarts internet services weeks after hacking debacle," *Herald Sun*, May 15, 2011. http://tinyurl.com/sony-debacle (accessed: July 14, 2011). Sony was down for 22 days in 2011 from April 21 to May 15.

[5] "Al-Qaeda and terror groups planning attack on US facilities," *DeccanHerald*, February 13, 2011. http://www.deccanherald.com/content/52422/al-qaeda-terror-groups-planning.html (accessed: July 14, 2011).

Table of Contents

Illustration Index

Tables Index

1.0 Introduction

Continuity of Operations (COOP) within the federal government and the Department of Defense (DoD) serves a fundamentally different purpose than it does in the commercial world. The commercial sector prefers the term Business Continuity Management (BCM), which is best expressed by the British Standard (BS) 25999-1:2006 ("BCM Code of Practice: Part 1"):

> *Commercial BCM: "holistic management process that identifies potential threats to an organization and the impacts to business operations…[and] provides a framework for building organizational resilience that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."*
>
> *BS25999-1:2006, p 7*

The federal government sets a much higher bar for what constitutes continuity. As President Bush eloquently phrased it in the National Security and Homeland Security Presidential Directive (NSPD / HSPD) "National Continuity Policy,"[6] the function of a COOP Program is nothing less than the assurance of the national way of life:

> *Enduring Constitutional Government (ECG) within COOP: "preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions (NEFs) during a catastrophic emergency"."*
>
> *NSPD 51 / HSPD-20, p 1*

The preservation of an individual organization's "value-creating activities" seems to pale in comparison with the preservation of the nation's constitutional form of government. In face, protecting programs and missions "in the large" as NEFs do makes it harder for smaller programs to achieve organizational resilience; this is based upon the perception that such resilience should be reserved only for those Mission Essential Functions (MEFs) that can be shown to support one or more NEFs actively. Such MEFs, because they support an NEF, are called "Primary" Mission Essential Functions (PMEFs).

This section analyzes why this concept is flawed by reviewing problems in the model and showing how COOP planning and implementation can benefit federal and DoD organizations of all sizes. The section then closes with the topics covered by this paper.

1.1 Problems in the Current Model

The Homeland Security Council (HSC) under the Department of Homeland Security (DHS) was tasked with providing the National Continuity Policy Implementation Plan (NCPIP) in 2007 as guidance for the federal

[6] Hereinafter: NSPD51.

government and DoD. This plan defined the eight different NEFs at a high-level:

1) Continue the functioning of the three branches of government;
2) Maintain the trust of the American people;
3) Defend the Constitution against all enemies domestic and foreign;
4) Maintain effective relations with foreign nations;
5) Protect the homeland against threats;
6) Respond rapidly and effectively to attacks against the homeland;
7) Protect and stabilize the nation's economy; and,
8) Support those federal functions that provide critical national health, safety, and welfare within the U.S.

These eight NEFs define the core responsibilities of every agency within the federal government.

1.1.1 Broad Brushstrokes make for ineffective Specific Policy

The roles and responsibilities at the Agency level (to include the DoD) are clearly stated, but only insofar as to require Heads of such organizations to be "responsible for integrating continuity planning as a fundamental part of everything that they do" (p 45). Moreover, individual agencies are responsible for maintaining other big-picture functions; as an example, the Secretary of Defense is charged with ensuring "secure, integrated Continuity of Government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies" (p 48). The General Services Agency (GSA), on the other hand, is made responsible to "provide and maintain a centralized procurement function for all department and agency continuity infrastructure requirements" and to "assist DHS in conducting continuity training and other preparedness activities and assist DHS and the departments and agencies in their recovery and reconstitution" (p 50).

Such approaches do little to address existing Programs of Record (PORs) that must perform their functions despite significant disruption (to include national emergencies). For example, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) is responsible for all DoD acquisition-oriented Web sites and (ultimately) provides guidance to the DoD acquisition community, including the Defense Logistics Agency (DLA).[7] Does this mean that GSA should have a COOP Plan (which it does)[8] but that DoD acquisition (particularly DLA) should not?[9] Certainly not; for COOP to be effective, it must be applied more granularly than

[7] The reader can find out more information on the USD(AT&L) and the programs it supports at http://www.acq.osd.mil/index.html (accessed: July 18, 2011).

[8] See GSA's Web site at http://www.gsa.gov/portal/content/101727 for a list of COOP services provided for other federal agencies.

[9] See page 15 of the "Fiscal Year 2011 Budget Estimates Defense Logistics Agency (DLA)" at http://comptroller.defense.gov/defbudget/fy2011/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PARTS/DLA_FY11.pdf (accessed: July 18, 2011) for a description of DoD's $27.1 million COOP budget request: "The COOP is under the staff cognizance and oversight of the Office of the Secretary of Defense and was transferred to the DLA in FY 1994. In accordance with DoD Directive 5111.1, Defense Continuity & Crisis Management (DCCM) was established to consolidate continuity-related policy and oversight activities within DoD in order to ensure the Secretary of Defense can perform his mission essential functions under all circumstances."

is called for by NSPD 51/HSPD-20 and the NCPIP.

1.1.2 *Less a Question of "If" than "When"…*

The year 2011 provides a prime example of how expensive a series of smaller, regional emergencies can be to government (federal and local). The following examples detail damages only to public buildings (not private households) and constitute a minority of emergency events identified for 2011:[10]

- Massachusetts, June 15, 2011 (Severe Storms and Tornadoes) - $24.7 million
- New York, June 10, 2011 (Severe Storms, Flooding, Tornadoes, and Straightline Winds) - $38.6 million
- Alaska, June 10, 2011 (Ice Jam and Flooding) - $1.3 million
- Minnesota, June 7, 2011 (Severe Storms and Tornadoes) - $16.3 million
- Idaho, May 20, 2011 (Flooding, Landslides, and Mudslides) - $4.6 million
- Oklahoma, May 13, 2011 (Severe Winter Storm and Snowstorm) - $9.4 million
- Tennessee, May 9, 2011 (Severe Storms, Flooding, Tornadoes, and Straightline Winds) - $8.3 million
- Hawaii, April 8, 2011 (Tsunami Waves) - $7.5 million
- California, January 26, 2011 (Severe Winter Storms, Flooding, and Debris and Mud Flows) - $75.4 million

Localized disasters occur throughout the year and all around the country. Individual federal programs and agencies lacking a COOP Plan to handle these events risk failing to perform their missions simply due to their primary facilities being unavailable or inaccessible to their people.

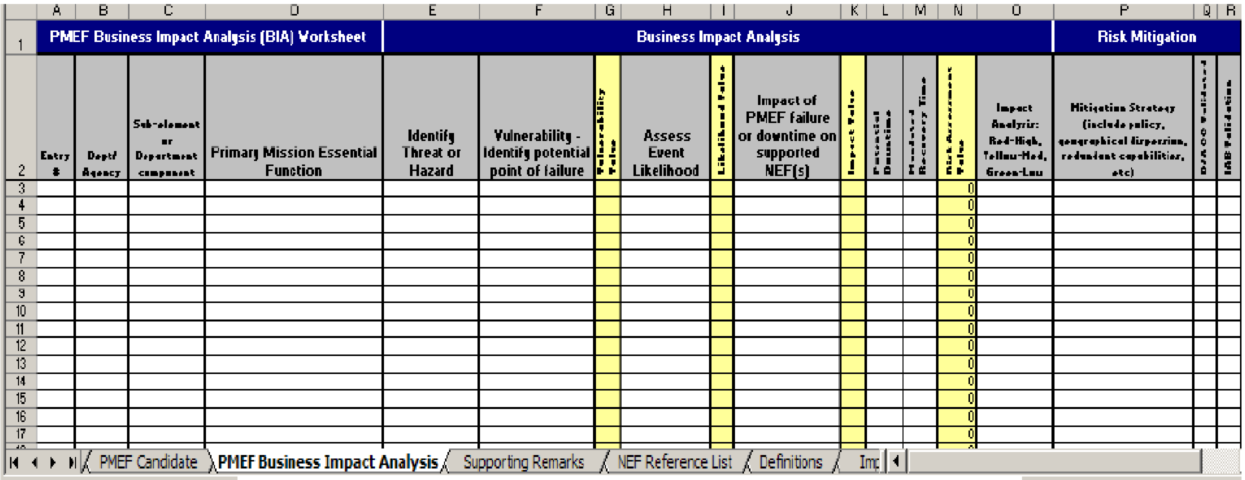
1.2 COOP planning for the Smaller Program

Smaller programs must be capable of accomplishing their missions even in the face of (possibly localized) disasters. This set of papers has looked at how a COOP Plan can be created for a smaller Army Program as a use case, and applies commercial, federal, DoD, and Army guidance to show the similarities and differences between the various continuity methodologies. COOP for a small federal-sector program relies on making the case for COOP, allocating scarce funding dollars wisely, and building in an exercise capability.

1.2.1 *Make the Case for COOP*

As for any other function, small programs must show a need for COOP based on the impact to their mission and to the owning organization. A small program needs first to understand all the areas it affects by using the same DHS guidance as "big programs" use: namely, to leverage Federal Continuity Directive (FCD) 2 ("Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process"). Specifically, smaller programs can use the PMEF Business Impact Analysis (BIA) worksheet as shown in the figure below:

[10] All statistics provided courtesy of FEMA at http://www.fema.gov/news/disasters.fema (accessed: July 18, 2011). Information is current as of this report date, but damage estimates average six weeks behind the emergency declaration.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	PMEF Business Impact Analysis (BIA) Worksheet				Business Impact Analysis											Risk Mitigation		
2	Entry #	Dept/ Agency	Sub-element or Department component	Primary Mission Essential Function	Identify Threat or Hazard	Vulnerability - Identify potential point of failure	Vulnerability Value	Assess Event Likelihood	Likelihood Value	Impact of PMEF failure or downtime on supported NEF(s)	Impact Value	Potential Downtime	Needed Recovery Time	Risk Assessment Value	Impact Analysis: Red-High, Yellow-Med, Green-Low	Mitigation Strategy (include policy, geographical dispersion, redundant capabilities, etc)	DoA COO Validated	IAB Validation
3														0				
4														0				
5														0				
6														0				
7														0				
8														0				
9														0				
10														0				
11														0				
12														0				
13														0				
14														0				
15														0				
16														0				
17														0				

Figure 1: PMEF BIA Worksheet[11]

Even a Program that is not itself a PMEF will glean insight into the interrelationships between itself and its stakeholders (consumers, suppliers, and partners) by completing the BIA worksheet. Once these relationships are understood, it becomes possible to quantify the effect that a loss of service would have on other organizations and on the Program's owner. For the Army Program use case, loss of the primary IT facility would affect the Program's ability to charge for its service.[12] This would be detrimental not only to the Army Program but also to its parent organization, a point which helps make the case for a targeted COOP Plan.

1.2.2 Apply Scarce Funds Wisely

In the federal government today a funding crisis looms over DoD as the "U.S. public overwhelmingly favors cutting defense spending."[13] Outgoing Defense Secretary Gates, in fact, called for $100 billion worth of cuts in Information Technology (IT) expenditures, defense contractors in support roles, and expensive weapons systems.[14] In this environment no Program Management Office (PMO) could make the argument that *every* function within a program can or should be addressed by a COOP Plan. The BIA identifies critical dependencies, allowing for functions to be prioritizend. As military analyst Andrew Faltum wrote for the Center for Homeland Defense and Security (CHDS) in 2009, programs must "[b]alance the need to share against the need to protect,

[11] Source: FCD-2, p 26.

[12] The general reader may be confused by this notion of "charging" in the public sector, but should consider that fee-for-service organizations in the federal government and DoD are common. The "charges" are paid for from other federal / DoD programs with budgeted funds approved by Congress rather than by after-market consumers, but the effect on a fee-for-service organization like the Army Program use case is ultimately quite similar to that of a commercial entity: loss of business service capability translates directly to lost revenue from customers.

[13] Amber Corrin, March 11, 2011. "Fight brewing over DOD budget cut," *defensesystems*. http://defensesystems.com/articles/2011/03/14/homepage-defense-fiscal-2012-budget-cuts.aspx (accessed: July 18, 2011).

[14] Amber Corrin, January 6, 2011. "Gates details DOD budget cuts, consolidations," *defensesystems*. http://defensesystems.com/articles/2011/01/06/gates-updates-dod-budgetary-measures.aspx (accessed: July 18, 2011).

enabling true risk management, *not just risk avoidance or risk acceptance*" (FALTUM, p 2).[15] In short, not every function can be protected within the COOP Program, and PMOs do well to remember that fact.

1.3 Topics for this Paper

Within the context of the small Army Program use case examined by this series of papers, the emphasis has been to detail a full COOP Plan reference implementation approach. This final paper provides an overview of policy guidance from the commercial, federal, DoD, and Army viewpoints and then leads into an overview of different templates available for use. The highlight for this final paper is "Appendix A: Sample COOP Plan," which provides a reference implementation adapted for the selected use case.

This entire series of papers has emphasized cost-effective implementation of COOP planning, honoring the country's urgent need to conserve funds while still ensuring that a Program's mission can be carried out. This results in a series of hard decisions and requires the COOP practitioner to demonstrate strength and resolve in determining which functions should be protected and to what extent. This paper and the reference COOP Plan continue this approach with the goal of providing a practical, goal-based, and enterprise-aligned COOP Program implementation roadmap.

2.0 Policy Guidance

The papers in this series have outlined policy guidance relevant to why COOP planning is important, how to jump-start the COOP planning process, how to understand BIA and Risk Assessment processes as part of the overall COOP planning strategy, and how to handle incidents and emergencies during a COOP Plan activation from a people (safety) and a technology (processes) view. This final paper looks at policies relevant to selecting and writing the COOP Plan.

2.1 Standards and Guidance Overview

Standards are best thought of as general approaches to a problem which form a framework for decision making. Both the commercial and federal sectors lay out a number of standards that can be used by the COOP practitioner. This section provides insight on the COOP Plan guidelines provided by these standards. One must remember that a standard, by itself, does not specify how to implement any one thing in particular; rather, procedures and guidelines that work in support of a standard can be used to solve specific problems. Thus, an Army standard such as Army Regulation (AR) 500-3 ("U.S. Army COOP Program Policy and Planning") provides the practitioner with general guidance on what must be considered within a COOP Plan, while a specific guideline such as Special Publication (SP) 800-34 ("Contingency Planning Guide") published by the National Institute of Standards and Technology (NIST) becomes much more detailed.

[15] Emphasis added.

2.2 Commercial Standards: BS 25999-1:2006 (BCM Part 1)

In the private sector, British Standard (BS) 25999-1:2006 ("Business Continuity Management – Part 1: Code of Practice") is the standard by which most BCM plans are judged. Its influence shows in the COOP policies, standards, and guidelines of DoD and the federal government as a whole.[16]

Within BS 25999, the Commentary within Section 8.6 ("The business continuity plans (BCPs)") highlights the fact that each BCM Plan should be tailored to its organization: "The components and contents of BCPs vary from organization to organization and have a different level of detail based on the scale, environment, culture and technical complexity" (p 39). BS 25999 requires that each BCM Plan incorporate four elements:

- *Plan Invocation.* A set of action plans assign responsibility for invoking the BCM plan and specify the procedures / stakeholders that guide that decision; mobilization of third parties (such as fire or police) and internal response teams; communications pathways; and emergency workarounds upon a failure in any of these high-level invocation support actions.
- *Resource Requirements.* Resources include the people, facilities, technology, supplies, and management capabilities that allow functions to be performed during an emergency, during a recovery, and upon return to normal operations.
- *Responsible Persons.* A *clear line of authority* is drawn to person(s) nominated as *responsible* based on the invocation of the BCM Plan. There must exist a *defined succession policy* so that decision-making can continue even in the absence of the identified responsible person.
- *Forms and Annexes.* These are the locations for the sub-plans (Communications Management Plan, Incident Management Plan, etc.) as well as the area where logs are maintained and relevant internal / external organizational contacts are kept.

As will be seen below, the federal, DoD, and Army COOP models all include these basic elements. Of special interest to the Army Program use case is the fact that BS 25999 acknowledges that BCM Plans can and should be different for each type of organization; this lends credence to this paper's supposition that *all* federal and DoD programs should assure COOP commensurate with their available budget and personnel resources.

2.3 Federal Standards and Guidance

The federal government consists of a vast number of bureaucracies, all operating under the control of the Executive Branch (the U.S. President) and all subject to laws as passed by the Legislative Branch. Within the federal government, the Office of Management and Budget (OMB) has issued circulars in support of Presidential directives, and the Department of Commerce has authorized NIST to set out guidelines to assist federal agencies in remaining compliant to all applicable laws, regulations, and policies. This section analyzes how the federal government uses policies and, standards, and guidelines to ensure that COOP Plans are complete and aligned to enterprise goals.

[16] Robert Giffin, November 1, 2009. "Why is DRI Speaking Out Against Organizational Certification?" *DisasterRecoveryJournal*, http://www.drj.com/view-by-tag/bs-25999/ (accessed: July 19, 2011). The reference notes that "[t]he federal government is developing a voluntary certification program (as mandated in law PS 110-53)," similar to BS 25999.

The following sections focus especially on how COOP Plans should relate to smaller organizations.

2.3.1 HSPD 20 / NSPD 51(“National Continuity Policy”)

From a high-level and big-picture view, a small Program might seem unlikely to merit consideration as part of federal COOP strategy. However, per the Implementation Action from the Policy (p 2), “[c]ontinuity requirements shall be incorporated into daily operations of all executive departments and agencies” and must emphasize “geographic dispersion of leadership, staff, and infrastructure.” Moreover, “appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.” In other words, individual agencies must perform an impact analysis (such as a BIA) with a subsequent risk analysis to ensure that the individual programs and functions required to support *all* government missions can be continued.

The practical ramification of this highest-level policy for the small Army Program use case is that the PMO is obligated to perform COOP planning in order to satisfy the next-higher level owning program or mission. In the Army Program use case, this analysis determines how specific program functions support the mission of the Army Materiel Command (AMC); the larger owning program’s COOP planning would be different but the net effect (the need for an integrated and holistic COOP planning strategy) would be the same.

2.3.2 FPC 65 (“Federal Executive Branch Continuity of Operations”)

Where HSPD 20 / NSPD 51 provides policy, Federal Preparedness Circular (FPC) 65 (“Federal Executive Branch Continuity of Operations”) specifies guidance for creating a COOP Plan. The Circular takes a pragmatic approach to COOP planning as simply a good business practice that all agencies must follow.

BS 25999 explicitly places human safety first (p 36) while FPC 65 just as explicitly places human safety *second*.[17] Furthermore, FPC 65 specifies that the most important element of a COOP Plan is “ensuring the performance of an agency’s essential functions” (p 2). The sobering conclusion to be drawn from this is that even individual initiatives like the Army Program use case must take a hard look at what their functions support and that any COOP Plan must ensure a well-ordered succession can take place.

FPC 65 continues by establishing the elements which any “viable” COOP Plan must contain and these can be applied to the Army Program use case:

- *Plans and Procedures.* Build a management structure that allows COOP planning to occur. This requires that the highest-ranking local official must be briefed and educated on the need for COOP; in the Army Program use case this would be the resident colonel.
- *Essential Functions.* Understand the goals of the parent organization and identify the criticality of individual functions within the program specifically as they align to the parent organization’s goals. AMC’s vision to be the “Army’s premier provider of materiel readiness – technology, acquisition support, materiel development, logistics power projection, and sustainment”[18] requires that technology services be given top priority.
- *Delegation of Authority.* Decision-making authority needs to be assigned prior to an emergency, and

[17] From the Circular: the second objective of COOP is “*reducing* loss of life, minimizing damage and losses” (p 3, emphasis added).

[18] Source: Army Material Command Web site (http://www.amc.army.mil/pa/about.asp, accessed July 19, 2011).

personnel need a clear command path to understand who can give directions during an incident. In the Army Program use case this means that the local Commander must authorize at least one deputy.

- *Succession of Authority.* As in the commercial model, a viable COOP Plan must account for vacancies in the command structure. This is the logical successor to the Delegation of Authority element in that procedures must be in place so that authorized deputies can assume command and control.
- *Alternate Operating Facilities.* Even where a small Program's budgetary concerns do not permit total duplication of the working environment the COOP Plan must identify what relocation would mean in the event of an emergency. For example, if the Army Program use case suffered a flood then the commanding officer needs to be able to present his or her facility needs expeditiously (e.g. "room for 25 employees, 25 government-furnished computers with Army login capabilities, network access to support X amount of bandwidth" and so forth).
- *Interoperable Communications.* The organization must have redundant paths for communicating with its employees. Alternatives such as the Government Emergency Telecommunications Service (GETS) to ensure priority in getting a dial tone during an emergency, cell phones, multiple emails, and even social networking (such as sending Tweets) can all be used as redundant methods of notifying staff of emergency events and activities.
- *Vital Records and Databases.* These include legal and financial records, emergency operating manuals, and any essential database storage mechanisms (such as database servers and supporting network infrastructure). For the Army Program use case, the binding Memoranda of Agreement (MOAs) with data consumers (especially those consumers accessing classified information vital to operational forces) would be prime candidates for inclusion in this category.
- *Human Capital.* This includes the people and the expert capabilities that allow the mission to function. While it is possible to run a program on a skeleton crew of highly trained individuals, simply looking at human capital as "warm bodies" is a grave error. Within the Army Program use case, the key personnel would include those individuals necessary to run the infrastructure and to make decisions for the program.
- *Test, Training, and Exercise*. This includes the concept of continuous improvement through measurement and management. The COOP Plan cannot be a "once-and-done" event but must rather be looked at as an ongoing commitment. The Army Program use case can schedule inexpensive and non-disruptive events from table-top plan walkthroughs, to data center evacuations, to periodic tests that data backups can be restored to meet recovery point objectives (RPOs).[19]
- *Devolution of Control and Direction.* COOP officials need to plan how constitutional government would operate in the complete absence of a program or function. Smaller programs do not need to provide workarounds in this area (as entire agencies need to do) but must instead focus on the question "What other functions would break if we simply ceased to exist?"
- *Reconstitution.* One weakness of BS 25999 compared to FPC 65 is the relative lack of information on how an organization should resume operations after a full disaster. FPC 65 goes to some lengths to identify the ways by which an organization must show that it has a recovery plan; the Army Program

[19] The *recovery point objective* is that point in time to which data must demonstrate integrity; BS 25999 defines it as "[i]n all cases, information needs to be recovered to a point in time that is known and agreed to by management" (p 30).

use case can concentrate less on this aspect of the COOP Plan by ensuring that operational requirements and functional interdependencies are well-understood and documented. Only then should any type of formal reconstitution planning effort be undertaken, and then only if the parent organization concurs.

The COOP practitioner should refer extensively to FPC 65 for guidance on creating and implementing a thorough, well-organized, and viable COOP Plan.

2.3.3 NIST SP 800-34 ("Contingency Planning Guide")

NIST's SP 800-34 ("Contingency Planning Guide") is not a *continuity* guide but rather a *contingency* guide. As such, the NIST publication is geared to ensuring that Information Technology (IT) support infrastructure displays necessary resilience and fault-tolerance in the face of disaster rather than ensuring that the business processes which depend upon that IT infrastructure can continue to operate effectively. This specialized approach makes the NIST guide extremely useful to create the IT Infrastructure plan as a major part of the overall COOP Plan.

The NIST document aims to guide and educate both commercial and federal organizations; thus, NIST includes a specific section on the need to create a Business Continuity Plan that concentrates on "sustaining an organization's mission/business processes during and after a disruption" (p 22), such as payroll processing or customer service. NIST defines COOP as concentrating on "restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations" (p 22). The contents of a COOP Plan as defined by NIST matches exactly to FPC 65 and, for the Army Program use case, implementing a COOP Plan provides sufficient resilience to meet all OMB requirements.

NIST's guidance, with its emphasis on cost-effective security and management controls, assists the COOP practitioner in writing the COOP Plan as highlighted below. Such emphasis was especially pertinent to the recent budget crisis where the specter of a U.S. government default loomed over the national economy:

Table 1: NIST SP 800-34 Cost-Reduction Guidance

Cost-Effective Point	Discussion
Prevent failures and losses.	The old adage "an ounce of prevention…" holds true here, and NIST advocates low-cost methods such as: Use appropriately-sized uninterruptible power supplies (UPS) for short-term outages; Inspect fire / smoke devices routinely (and avoid the use of water-based fire-suppression systems if budget permits); Install a master shutdown switch; Store materials in fire-proof safes.
Ensure spare equipment inventory is on-hand.	Purchasing equipment during a disruption can add significantly to the cost of recovery. A good inventory of current equipment makes high-value items easier to identify.
Do not discount reciprocal agreements.	Reciprocal agreements, while unenforceable, are a low-cost approach to handle redundancy for relocating staff during a disruption. Facilities should be far enough apart to mitigate against regional disasters and data storage agreements must be negotiated well in advance. (Very high uptime requirements preclude this approach.)
Provide alternative	Installation of a separate gigabit switch between floors can help to mitigate the

Cost-Effective Point	Discussion
communications cabling.	risk that a primary network cable is cut without entailing the expense of running multiple cables to individual workstations. While specific to IT infrastructure redundancy, this strategy highlights the need for business continuity planners to consider the implications of a purely local failure.

NIST's approaches and techniques emphasize the proactive nature of a continuity plan. The federal government's high-level focus on ensuring enduring constitutional government actually *requires* smaller programs to plan for COOP in support of higher-level missions.

2.4 DOD Standards and Guidance

According to NSPD 51 / HSPD-20, DoD's primary function during COOP activation is to "provide secure, integrated, Continuity of Government communications" (p 5). This section explores the policy and procedures that COOP practitioners should use when creating COOP Plans within the DoD.

DoD does define neither specific COOP implementation guidelines nor specifications; in fact, each agency and individual program must define its own COOP Plan that conforms to laws, regulations, and policies. This works in favor of smaller programs; DoD's wise avoidance of a monolithic COOP approach allows for flexibility and creates cost-control opportunities within individual implementing programs.

2.4.1 Directive 3020.26 ("Defense Continuity Program")

In direct response to NSPD 51 / HSPD-20 (and the resulting NCPIP), the DoD wrote Directive 3020.26 ("Defense Continuity Program") to provide guidance to "components" (major commands and agencies such as the four uniformed services, the Defense Logistics Agency, and others). This Directive echoes much of what is found within FCP 65, calling for COOP Plans to (p 2):

- *Assume that disruption will strike without warning.* Continuity plans must assume that COOP activation can occur at any time. The distributed nature of the DoD further complicates this issue, because smaller programs (like the Army Program use case) may very well be called upon to help mitigate a disruption event that does not directly affect them.
- *Provide for geographic distribution of key staff (especially command and control).* While problematic for smaller programs, COOP practitioners can address this requirement through reciprocal agreements, cross-training, and the publication of a clear command structure with delegation capabilities.
- *Incorporate continuity requirements into daily activities.* This corresponds closely to BS 25999's overall BCM strategy in that the COOP practitioner must ensure that the COOP Plan has a process for embedding COOP into the organization's culture as shown below:

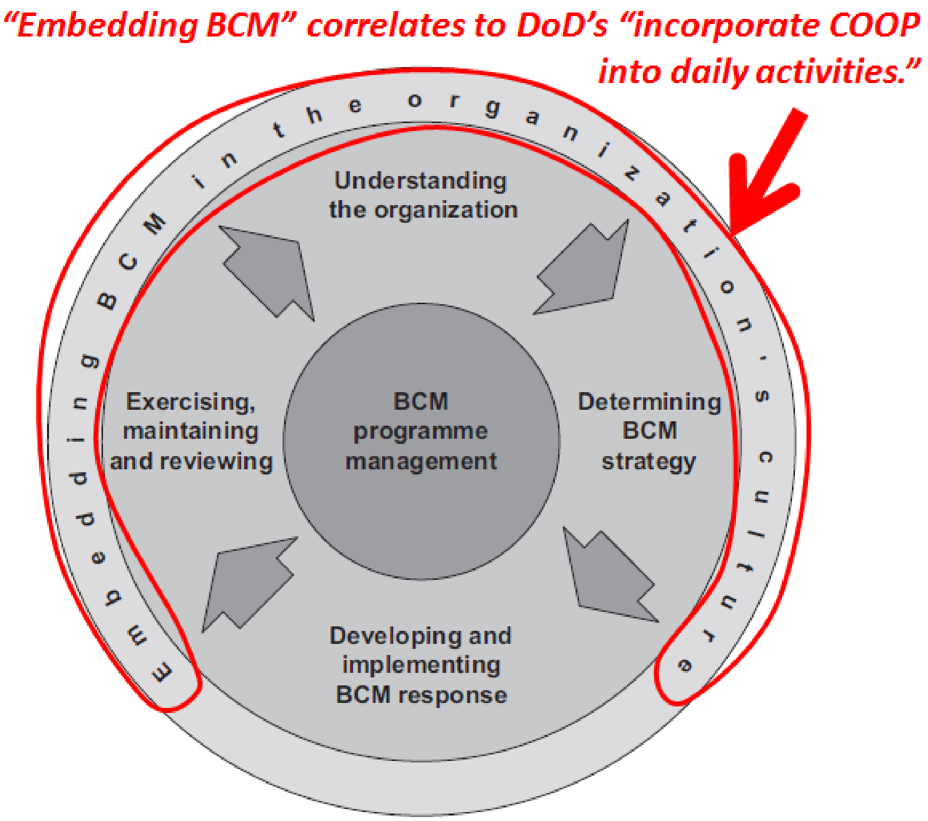

"Embedding BCM" correlates to DoD's "incorporate COOP into daily activities."
Embedding BCM in the organization's culture
Understanding the organization
Determining BCM strategy
Developing and implementing BCM response
Exercising, maintaining and reviewing
BCM programme management

Figure 2: Correlation between DoD 3020.26 and BS 25999[20]

The use of Directive 3020.26 as a high-level sanity check for individual COOP Plan implementation decisions helps to ensure that plans fully address DoD requirements.

2.4.2 Instruction 3020.42 ("Defense Continuity Plan Development")

While still at a very high level, DoD Instruction 3020.42 ("Defense Continuity Plan Development") provides specific guidance to the COOP practitioner for planning and implementation. The policy statements reiterate the higher-level Directive 3020.26 but with an additional emphasis on ensuring that identified specific MEFs should "be the basis for continuity planning, preparation, and execution" (p 2). The individual Service Chiefs and Combatant Commanders are further responsible for ensuring that COOP Plans exist to support the overall Defense Continuity Plan (DCP). This further reinforces the need for individual programs and functions to perform COOP planning (if not outright implementation); higher-level Commanders and Chiefs cannot be assured that their own COOP Plans are fully inclusive without this type of bottom-up support.

More to the point for the COOP Practitioner, the Instruction describes three essential functions that COOP planning must address (highlights follow):[21]

- *Establish Core COOP Plan Development Requirements.* Perform an impact analysis to determine MEFs;

[20] Source: BS 25999, p 15 (modified by the author).

[21] Paraphrased from the Instruction, Section 6 (p 3-11).

useful criteria include those functions affecting: 1) Command and Control functions; 2) Command decision and strategies; 3) Crisis communications (the reader should bear in mind that, at the federal level, this is *the single most important* DoD function); 4) Crisis data storage (ability to retrieve necessary information in the face of significant disruption); 5) Legal obligations; 6) Fiscal / contractual obligations (for the Army Program use case, consider any existing binding customer agreements); 7) Personnel (any function that affects the health and safety of human resources); 8) Critical support to other DoD components or agencies.[22] The Instruction also lists a repeat of the functions required by FPC 65 (vital records, staffing requirements, orders of succession, and so forth).

- *Determine Capability Requirements. Capabilities* here refer to the specialized functions and expertise that constitute an organization's value-add; thus, any COOP Plan must prevent the loss of specific capabilities. It does little good, for example, to recover a data service provider's facility if key knowledge on proxy authentication (which constituted the provider's primary market differentiator) has been lost. The Instruction echoes NIST's SP 800-34 recommendations for alternate processing facilities to be identified ahead of time and that command personnel be distributed geographically. One additional item for the COOP practitioner to consider is what the Instruction refers to as "fly-away kits;" those "critical office items/records that cannot be pre-positioned at alternate operating facilities" (p 7). Items falling into this category consist of personal items like prescriptions.
- *Write Plans and Procedures.* These include sub-plans such as the Communications Management Plan and Incident Management Plan, as well as the procedure for how COOP activation will be transmitted from higher authority to all personnel (especially key personnel). The Instruction does not provide specific guidance or suggestions on how these communications should occur. This overall step includes the Reconstitution Phase of a COOP activation, and the Instruction adds the useful tip that external parties must be carefully considered; these external parties include contacts and organizations responsible for providing reconstitution support (like the GSA) or vendors and outsourcing sources. Finally, general instructions that COOP "[p]lans will be tested and exercised" reinforce the ongoing nature of COOP in the public sector.

These general notes emphasize the formal nature of COOP planning and the fact that DoD policy requires all programs to participate in COOP planning (not just large "national essential functions").

2.5 Army Standards and Guidance

At the Army level, more specific guidance helps the COOP practitioner to write the COOP Plan. This section looks at two such documents: Army Regulation (AR) 500-3 ("U.S. Army COOP Program Policy and Planning") and Pamphlet (PAM) 25-1-2 ("Information Technology Contingency Planning").

2.5.1 Regulation 500-3 ("U.S. Army COOP Program Policy and Planning")

AR 500-3 was written in response to the requirements of DoD Directive 3020.26 for the sake of specifying how Army functions must support the big-picture Continuity of Government (CoG) capabilities assigned to DoD (and other federal agencies) by the NCPIP.

AR 500-3's planning requirements begin with DoD's injunction to *protect mission essential functions first*;

[22] That last element of MEF identification (support to other DoD components / agencies) clearly provides a policy support basis for each program (including the small Army Program use case) to perform a formal impact analysis. Only in this way can such support be identified and addressed within the COOP Plan.

therefore, to *identify these functions* is a top priority (p 13). In other words, the impact analysis is the most critical component of any COOP Plan and should be the driving force for every other Plan element. Additionally, COOP Plans must be *flexible* and must:[23]

a. *Align to organizational goals.* COOP Plans form Army functions must “support COOP Plans of higher headquarters and supported organizations.”

b. *Allow for implementation at any time (regardless of hours) and account for all possible events.* Such an exhaustive approach has become the “new norm for the Army.”

c. *Define a decision-making process; hence, also a plan of succession.* These procedures must be defined ahead of time (in the midst of an emergency, there should be no debate as to who is in charge if the Colonel is incommunicado).

d. *Prioritize all MEFs and identify those MEFs that could be “deferred without impact to the unit’s core mission.”* (These might be cyclical MEFs such as year-end processing or strategic reporting.) For the public-sector COOP practitioner and the private-sector BCM planner, the implication is that not all mission essential functions are necessarily essential all of the time. Judgment and discretion must be the hallmark of any COOP Plan (or BCM Plan, for that matter).

e. *Reflect that facility and personnel safety are* ***not*** *at the top of the list.* In fact, the Regulation goes somewhat out of its way to state that facilities come before people and that the Mission comes before everything. This is completely the reverse of BCM in the private arena, so the COOP practitioner must not be afraid of putting people second when drawing out the plan. Where this becomes complex is when the people involved are essential to the mission; such an Orwellian situation calls to mind the notion that “some animals are more equal than others.”[24]

f. *Include training and exercises and hold trained personnel accountable for their roles during an emergency.* The Plan must make provisions for emergency notification of Emergency Response Group (ERG) personnel. For the small Army Program use case, this means that low-cost redundant communications are integral to any COOP Plan exercise schedule. Finally, the COOP practitioner should remember that, by policy driven ultimately from NSPD 51 / HSPD-20, a COOP activation must result in MEFs being operational within 12 hours and prepared to run for 30 days. For small Army Programs (or any other small organization), this type of rapid response must be supported by higher-level management. In a commercial organization, only the Chief Financial Officer (CFO) can provide that type of capability support. In a public-sector organization like the Army, this translates to support at the Senior Executive Staff (SES) level. One can imagine the difficulty in getting this level of commitment for a lower-echelon program; a useful approach is to put an identified MEF within the smaller program on the critical path of a larger owning program. The importance of establishing lines of communication in support of these relationships cannot be overstated!

g. *Be validated by qualified and authoritative personnel.* As with the 12-hour operational capability requirement listed above, finding an individual willing to authorize a COOP Plan can be challenging in a public-sector organization. The above practical suggestion recommends the identification of MEFs that affect higher-level organizations and communicate this dependency to the higher-level organization.

[23] See the Regulation, p 7-8.

[24] George Orwell (1946). *Animal Farm*. New York, NY: Random House.

This approach ensures that, at the very least, the COOP Plan portion pertaining to those identified MEFs will be validated. Because of the impact on the higher-level organization from the identified MEF, there exists an excellent chance that a decision (positive or negative) will be forthcoming. Such an approach does lead to a piecemeal overall validation solution for the smaller program but it is quite possibly the best solution that can occur in a disjointed and resource-constrained environment like the Army.

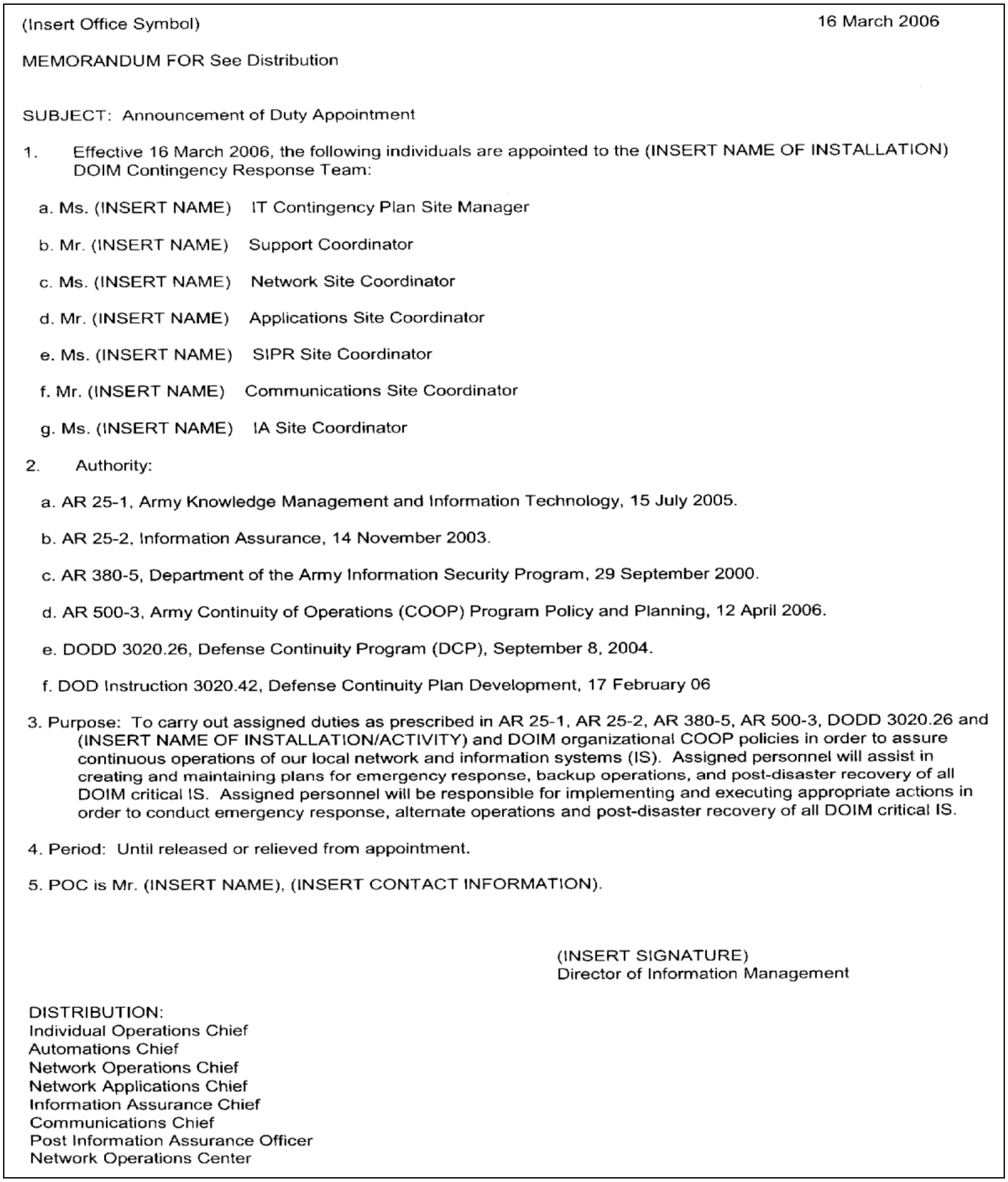
These directives highlight the need for the COOP practitioner to apply sound judgment and careful attention to maximize relationships with other organizations. The practitioner may then craft a defensible COOP plan in an environment where every expended dollar is scrutinized.

2.5.2 Pamphlet 25-1-2 ("Information Technology Contingency Planning")

The Army's IT Contingency Planning from Pamphlet 25-1-2 provides an interesting extension to NIST's SP 800-34 highlighted above. As with SP 800-34, IT contingency is a subset of an overall COOP Plan. One point that the Pamphlet raises is that "there is a definite relationship between an IT system and the business process it supports," so "care must be taken to ensure that recovery strategies and supporting resources neither negate nor duplicate efforts" (p 8). The COOP practitioner can apply this to the larger COOP Plan effort to ensure that continuity efforts between different plans do not result in a duplication of effort.

The very IT systems that the Pamphlet strives to protect provide the COOP practitioner with a potent tool to avoid duplicative efforts by automating the COOP Plan effort (for example, to create a cross-referenced database of initiatives and efforts). The scope of the Pamphlet, however, is on how to protect the IT infrastructure. From a cost-effectiveness viewpoint, the Pamphlet's close relationship to NIST's SP 800-34 can be discerned clearly. The Pamphlet specifies the use of the same set of cost-effective preventive approaches as NIST does (UPS, appropriate fire suppression, proven backup techniques, and so on). The Army's Pamphlet emphasizes that preventive controls must be well-documented and staff must have formal training (that is, a formal signoff of the operator's understanding and competence in applying and maintaining the preventive controls). Other specific cost-effective controls (such as creating reciprocal agreements with other organizations, or using alternate network wiring within a primary facility) appear almost word-for-word as in the NIST document.

The Army Pamphlet does provide a sample "contingency response team duty appoint letter" that is of interest to the COOP practitioner because it highlights the need for the COOP Plan to have a formal team member appointment process. From a COOP activation viewpoint, such formality is indispensable; COOP team members across the board must be cognizant of their responsibilities and roles. A sample of this form is shown below:



(Insert Office Symbol) 16 March 2006

MEMORANDUM FOR See Distribution

SUBJECT: Announcement of Duty Appointment

1. Effective 16 March 2006, the following individuals are appointed to the (INSERT NAME OF INSTALLATION) DOIM Contingency Response Team:

a. Ms. (INSERT NAME) IT Contingency Plan Site Manager

b. Mr. (INSERT NAME) Support Coordinator

c. Ms. (INSERT NAME) Network Site Coordinator

d. Mr. (INSERT NAME) Applications Site Coordinator

e. Ms. (INSERT NAME) SIPR Site Coordinator

f. Mr. (INSERT NAME) Communications Site Coordinator

g. Ms. (INSERT NAME) IA Site Coordinator

2. Authority:

a. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

c. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

d. AR 500-3, Army Continuity of Operations (COOP) Program Policy and Planning, 12 April 2006.

e. DODD 3020.26, Defense Continuity Program (DCP), September 8, 2004.

f. DOD Instruction 3020.42, Defense Continuity Plan Development, 17 February 06

3. Purpose: To carry out assigned duties as prescribed in AR 25-1, AR 25-2, AR 380-5, AR 500-3, DODD 3020.26 and (INSERT NAME OF INSTALLATION/ACTIVITY) and DOIM organizational COOP policies in order to assure continuous operations of our local network and information systems (IS). Assigned personnel will assist in creating and maintaining plans for emergency response, backup operations, and post-disaster recovery of all DOIM critical IS. Assigned personnel will be responsible for implementing and executing appropriate actions in order to conduct emergency response, alternate operations and post-disaster recovery of all DOIM critical IS.

4. Period: Until released or relieved from appointment.

5. POC is Mr. (INSERT NAME), (INSERT CONTACT INFORMATION).

(INSERT SIGNATURE)
Director of Information Management

DISTRIBUTION:
Individual Operations Chief
Automations Chief
Network Operations Chief
Network Applications Chief
Information Assurance Chief
Communications Chief
Post Information Assurance Officer
Network Operations Center

Figure 3: Example of formal COOP Team Duty Appointment[25]

The Pamphlet also includes a sample recovery budget plan. The COOP practitioner needs to include recovery costs as part of the overall COOP Plan (an area where the commercial BS 25999 standard is lacking). Thus, while the general COOP practitioner may not take much of an interest in the Army's IT contingency approach, the

[25] Source: Pamphlet 25-1-2, p 7.

example templates (duty appointment, contingency policy, recovery budget estimates, and numerous checklists) emblemize best practices that apply equally well across the federal government and private industry.

2.6 Summary

This section has analyzed how different standards and guidelines from private industry and the federal government provide guidance to the COOP practitioner for writing the COOP Plan. Common to all sources is the notion that individual human beings must be identified as responsible within individual COOP elements. It is not sufficient to have a policy statement of "The IT Director is responsible for ensuring System X has an alternate processing facility available for activation within Y hours." Rather, the COOP Plan must identify a specific individual, identified by name, aligned with this responsibility. Moreover, these specific individuals must be fully aware of their responsibilities; this is best accomplished using a format similar to the "duty assignment" example presented by Army's Pamphlet 25-1-2.

The COOP practitioner in the federal space must accept that *the mission comes first*. The goal of COOP at the federal level is to ensure the durability of the nation's constitutional form of government. The overriding goal of DoD in general (and the Army in particular) is to support the missions essential to enduring constitutional government (ECG). People and facilities fall further down the list; only particular COOP sub-plans (such as the Crisis Communications Plan) will set personnel safety as a top priority. This necessitates a highly rational approach to the COOP Plan that emphasizes how identified MEFs will be completed no matter what the disruption might be.

The most important takeaway is that disruptions are "expected to be unexpected" and MEFs must have a continuity plan to continue operations under any circumstances. This extremely high operational bar requires that all programs (small and large) must identify their specific MEFs and how those MEFs affect higher-level programs.

Smaller entities such as the Army Program use case most definitely have a requirement to create and implement a COOP Plan. The next section of this paper examines best-practices templates available for use within this effort.

3.0 COOP Plan Templates

Public sector COOP practitioners must start with an existing, pre-approved template. COOP Plans are held to stringent requirements to make sure that they account for all possible scenarios. To build a COOP Plan outline from scratch would be a daunting, and unnecessary, proposition. This section highlights various types of COOP Plan templates available for use by the COOP practitioner.

3.1 Overview: Continuity vice Contingency

NIST's SP 800-34 distinguishes between continuity and contingency as elements of overall organizational *resilience* ("the ability to quickly adapt and recover from any known or unknown changes to the environment").[26] Continuity is concerned with business processes, while contingency is concerned with the IT infrastructure that supports those business processes. The business processes comprise what the federal government calls "mission essential functions," or those functions that enable the organization to support the

[26] SP800-34, p 19.

nation's enduring constitutional government.

The difference from a COOP practitioner's view between contingency and continuity is that no continuity plan is complete without a contingency plan in place. The business processes (the "MEFs") supported by the contingency plans must be identified via an impact analysis effort.[27] Continuity plans focus on ensuring that business functions can continue via alternate methods: personnel are notified when an emergency occurs; suppliers and customers are contacted and can quickly leverage the alternate business methods (example: receiving deliveries at an alternate distribution center if the primary distribution center is not available); and, supporting vital records continue to be usable (such as service level agreements, contract terms, and so on). Contingency plans focus on safeguards to prevent disruption (such as high availability disk storage or network access) in addition to expeditious recovery procedures in the event that a disruption occurs (such as satisfying end-user Web applications via a backup processing center). Contingency plans concentrate on ensuring that the organization can support identified recovery point objectives (RPOs)[28] and recovery time objectives (RTOs).[29]

Both template types are critical elements of a COOP Plan; this section describes example templates from the federal sector. For COOP practitioners working in a budget- and resource-constrained environment such as a small Army Program, leveraging the power of an existing template represents an excellent cost-savings measure.

3.2 COOP Plan Template (FEMA)

COOP Plans in the federal government address organizational resilience and what would be termed "business continuity" in the commercial world: the organization's ability to continue as a viable enterprise in a range of business disruption scenarios. This paper presents an example COOP Plan in "Appendix A: Sample COOP Plan" for a notional Army Program use case and uses a standard federal template provided by FEMA. This template provides a best-standards approach to overall business continuity within the federal government and is of immediate practical use both to Army and to federal COOP practitioners.

3.2.1 The FEMA Coop Web Site

There is no single "FEMA COOP Plan Template" master document; rather, FEMA offers a complete set of resources tailored to federal and non-federal entities at its COOP Plan Web site.[30] These resources include the COOP Plan templates themselves, optional instructions for filling out these templates, specialized checklists (such as pandemic influenza operational plans), a briefing for federal agencies on vital records management, reconstitution (functional recovery) and devolution (the subsumption of one entity's MEFs within another entity) templates, and an entire set of exercise templates.

3.2.2 FEMA COOP Plan Template Sections

For this paper the selected COOP Plan template is the "Continuity of Operations Plan Template and Instructions

[27] NIST uses the term "business impact analysis" as is common in the commercial sector, other federal publications leave out the term "business" but the practical meaning is identical.

[28] RPO is "a factor of how much data loss the mission/business process can tolerate during the recovery process" (SP800-34, p 31).

[29] RTO is the "maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, [and] supported mission/business processes" (SP800-34, p 31).

[30] See FEMA's COOP Plan Web site at http://www.fema.gov/about/org/ncp/coop/templates.shtm (accessed: July 23, 2011).

for Federal Departments and Agencies" (FEMA-COOP). The key characteristics of this template include the "standard" COOP sections that have been highlighted throughout this series of papers:

Table 2: FEMA COOP Plan Elements

Element	Included in this Paper?[31]	Discussion
Governance and Change Management.	Partial	The organization using the plan, their authority for so doing, the changes made after the initial draft acceptance, and the list of entities that should receive plan updates. For privacy, the Promulgation Statement is not included.
Purpose and Scope.	Yes	In commercial terms, this would be the organizational strategy that defines why a BCM Plan is necessary: what lines of business must be considered; what critical revenue streams must be preserved; the customer market space (Netflix might cite its need to remain a dominant information streaming media source no matter what disruption occurs); and so on. In the government COOP model, this is a more formal statement of the organizational mission and how it ties to the higher-level owning organization.
Concept of Operations.	Yes	The plan for the "how" portion of COOP; it may consist of: the definition of "COOP readiness," how a COOP activation actually occurs and what relocation options must be considered, ensuring continuity of mission essential functions (MEFs) during a COOP activation; recovering MEFs to a primary site after a COOP standdown, and instructions for devolution in case MEFs should no longer be performed by this organization after a COOP activation and another organization must step in.
Organization and Responsibilities.	Yes	The organizational chart showing hierarchy of command; the COOP Plan includes assigning specific individuals to COOP roles.[32]
Direction and Control.	Yes	In military terms, Command and Control (C2); how this COOP Plan integrates horizontally and vertically with other COOP Plans throughout the organization.
Disaster Intelligence.	Yes	The strategy plan for keeping abreast of different classes of disaster data, such as the number of Emergency Response Group personnel that have arrived onsite during a disaster.
Communications.	Yes	The redundant communication infrastructure that helps to ensure a

[31] All statements regarding policy, organization, staffing, MEF identification, and so on are representative only and do not apply to a real Army Program. They reflect the author's judgment and experience and should not be taken as authoritative by the COOP practitioner.

[32] This paper does not personally identify any individuals within the COOP Plan for the Army Program use case.

Element	Included in this Paper?[31]	Discussion
		successful COOP activation, process, and standdown (to include recovery).
Budgeting / Acquisition.	Yes	Information on how the COOP budget is integrated into the organizational budget and the correlation of external vendor contracts to this budgeting activity.
Plan Development and Maintenance	Yes	Change control for the plan to include review boards.
Authorities and References	No	The list of authoritative guidance (included as the "Reference List" within this paper).
Functional Annex: Essential Functions	Yes	A notional but specific MEF within the Army Program use case.
Functional Annex: Continuity Personnel	Notional	For space and privacy reasons, only selected functions and the format are presented.
Functional Annex: Vital Records Management	Yes	Specific vital records are redacted to protect confidentiality and privacy.
Functional Annex: Continuity Facilities	Yes	COOP Plan requirements indicate that at least one additional site should provide functional capabilities for executing identified MEFs. This paper does not provide details on site locations.
Functional Annex: Continuity Communications	Yes	The specific communication capabilities used during COOP activation.
Functional Annex: Leadership / Staff	Yes	Includes orders of succession, delegations of authority, and human capital management.
Test and Training	Yes	The "continuous service improvement" aspect of the COOP Plan; that is, how individual COOP implementation plans will be verified against a baseline, aligned to changing organizational needs, and improved over time.

The Army's Regulation 500-3 explicitly calls for plans to correlate to guidance from FPC 65, which in turn references the FEMA COOP Plan Templates (AR500-3, p 16) Army practitioners using this approach can rest assured that their efforts will not be wasted.

3.3 Contingency Plan Templates

Contingency refers to the ability of the organization's IT infrastructure to support business continuity needs. Contingency plan templates provide value to the COOP practitioner because they force consideration of the underlying operational constraints within which a COOP Plan must operate. This section analyzes two different types of contingency plans: one from NIST (general-purpose and targeted to the entire federal government) and one from the Army (for application to the Army Program use case). Specific elements from the contingency that map back to the FEMA COOP Plan template presented in the section "COOP Plan Template (FEMA)" are highlighted for consideration to the overall COOP Plan.

3.3.1 NIST Contingency Plan Template

NIST provides no direct guidance for either Business Continuity Management (BCM) or Continuity of Operations (COOP). As a *technical* standards body, NIST releases guides that address risk management for the network infrastructure and applications running on top of that infrastructure. NIST's Web site includes a section for Federal Agency Security Practices (FASP),[33] where contingency templates from different federal agencies can be accessed.[34] The generalized NIST contingency template which this paper uses is not directly available from the FASP Areas page (NIST-CONT).[35]

3.3.1.1 NIST Contingency Plan Phases

NIST's contingency template concentrates on preventive controls that ensure technological resilience, as well as operations within the specific contingency phases as identified by NIST:

- *Response Phase.* Respond immediately at the incident site: identify that an incident has occurred and classify it; disseminate information regarding that incident to determine, based upon severity, whether system access should be disabled; and provide management with the information necessary to make the best decisions.
- *Resumption Phase.* Establish C2 over the incident: mobilize incident response teams; notify time-sensitive operations of the incident's impact; and alert stakeholders (employees, vendors, and customers) of severity and impact.
- *Recovery Phase.* Prepare and implement procedures that recover critical business functions to an operational state within defined RTOs (albeit possibly degraded). Next, coordinate the incident response and allow escalation to occur as defined by decision makers (authorized management). This coordination includes communicating status and directions to all stakeholders within a timely manner.
- *Restoration Phase.* Recover business functions to their original operational levels at either a new or a repaired facility.

The reader should notice immediately the close correlation between contingency phases and COOP phases. NIST's contingency template adds value for the COOP planning process because it emphasizes *measurable performance levels* for both operational and resumption levels.[36]

[33] For the entire FASP, see http://csrc.nist.gov/groups/SMA/fasp/index.html (accessed: July 23, 2011).

[34] For the FASP Areas, see http://csrc.nist.gov/groups/SMA/fasp/areas.html (accessed: July 23, 2011).

[35] The generic NIST contingency plan template is available from http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc (accessed: July 23, 2011). This template does not originate from a specific agency's template and is thus suitable to a wide audience.

[36] Section 3.6 within NIST's contingency plan template immediately follow the "Contingency Phases" section and requires the practitioner to define "Critical Success Factors and Issues." As a COOP Plan generally operates at a very high level with abstract "triggers" (e.g. "COOP activation shall be considered when two lines of business fail to meet their defined

3.3.1.2 Critical Functions Supported by Information Systems

NIST's contingency plan template provides another level of information cross-check for the COOP practitioner: the identification of the critical functions ("MEFs" to use the DoD term) each system supports and of specific threats to each system's infrastructure. Because the first step of COOP planning is the Business Impact Analysis (BIA) and the Risk Assessment, a natural question to pose to the COOP practitioner is: "Which comes first? The BIA at the *organizational* level or the BIA at the *system* level?" For a small organization such as the Army Program use case, the practical answer is "Neither." Rather, the BIA must be conducted as a facilitated group effort where business unit managers identify major lines of business and operations, with qualified technical advisers at hand.

3.3.2 Pamphlet 25-1-2 ("Information Technology Contingency Planning")

The Army's Pamphlet 25-1-2 ("Information Technology Contingency Planning"). This Pamphlet has a Chapter 6 ("IT Contingency Plan Services") is especially pertinent to this paper's example Army use case and serves as an excellent operational reference for any COOP practitioner. Takeaways from the pamphlet include:

Contingency Support must be in place for information services. Information systems requirements must be prioritized within any contingency plan. These requirements should reflect the MEF findings from the COOP program's impact analysis. As with the above NIST contingency plan template section on "Critical Functions Supported by Information Systems," system impacts for each MEF identified by the high-level COOP impact analysis should be considered in light of findings by SMEs at the operational level. If the COOP practitioner overlooks the synergy between business and operations, an apparently thorough COOP Plan may turn out to be a negative asset in an actual emergency due to the false sense of confidence it inspires. COOP Plan exercises that occur within a controlled environment may easily overlook hidden relationships.

Mobilization information services support planning. Cell phones can overload even without a disaster, as evidenced by AT&T's iPhone problem in September 2009.[37] During an emergency, this communications channel is prone to overload.[38] The Pamphlet includes a number of mitigations that the COOP practitioner should consider:

- Define additional leased lines for intra-organizational communications capability ahead of time. (The Pamphlet uses the phrase "premobilization (peacetime) period.")
- Ensure that redundant communication paths are defined wherever these can be justified. For the Army Program use case, this includes not only any additional leased lines but arranging for issuance of Government Emergency Telecommunications Service access numbers to receive priority for making cellular telephone calls.
- Consider the need for communicating with *all* stakeholders; especially in the military, it can be assumed that communication to higher authority is all that is necessary. In a true emergency where

SLA to affect revenue in the amount of 35% for that day"), the specific Critical Success Factors identified in the contingency plans form the practical implementation of COOP policy for the organization. The COOP implementer needs to consider this "effective COOP policy implementation" side-effect carefully.

[37] Jenna Wortham, September 2, 2009. "Customers Angered as iPhones Overload AT&T," *nytimes.com* (http://www.nytimes.com/2009/09/03/technology/companies/03att.html, accessed: July 23, 2011).

[38] Christopher R. Cox, December, 2005. "Preparing for Travel Disasters," *Travel+Leisure* (http://www.travelandleisure.com/articles/preparing-for-the-worst, accessed: July 23, 2011).

headquarters-level personnel are swamped, how will other dependent organizations be notified in a timely manner of disruptions? Establishing authorized alternate communications channels to key stakeholders as well as defining straightforward policies on when these alternate communications channels must be used provides a valuable weapon in the COOP practitioner's arsenal for handling a specific disaster.

The Army-specific IT Contingency Plan template clearly demonstrates that it has much information for the COOP practitioner to consider when building the COOP Plan.

3.4 Summary

Space does not permit a full correlation between all contingency plan functions and continuity plan functions. The reader should see from this brief overview that an effective COOP Plan cannot be created without the active involvement of Operations (specifically, IT Operations) at every phase of the impact analysis and risk assessment. Modern business systems' reliance on information technology calls into question any COOP approach not grounded in such cooperation.

4.0 Concluding Remarks

This paper has provided the COOP Practitioner with an overview of the COOP Plan from commercial, federal, DoD, and Army levels. The striking difference between the commercial world of Business Continuity Management (BCM) and the federal world of Enduring Constitutional Government (ECG) and Continuity of Government (CoG) is the inversion of human safety. The commercial world considers human safety to be the single most important factor within any disaster response plan. Federal guidance, particularly within DoD and the Army, considers human safety secondary to the durability of Mission Essential Functions (MEFs). CoG must be ensured despite *any disruption* and *within 12 hours*.

From an implementation view, all COOP practitioners for all federal-sector programs, large and small, must first determine which of the eight top-most level National Essential Functions (NEFs) a program's MEFs support.[39] MEFs *must be identified* and *must not be allowed to fail*. Every program therefore must perform an impact analysis to determine its MEFs relative priority to the nation.

This paper has made a number of recommendations that are summarized and estimated in Appendix B (immediately follows "Appendix A: Sample COOP Plan."). This sample COOP Plan for a small Army Program use case is designed to show a COOP practitioner specific wording and approaches applicable even to small programs.

To reinforce the best practices demonstrated within the sample COOP Plan, this paper analyzed continuity and contingency plan templates available from FEMA, NIST, and the Army. The guidance from the IT-focused contingency plan templates reminds the COOP practitioner that modern business systems cannot have continuity unless the underlying information systems are highly resilient; moreover, it is only by integrating the detailed results of an impact analysis and function prioritization at the information system level that *hidden*

[39] See NSPD51, p 2 for the eight NEFs. They are listed in the Introduction but they bear repeating here : 1) Continued functioning of the three Branches of Government; 2) Visible leadership to the American People; 3) Defend the Constitution; 4) Maintain foreign relations; 5) Protect against threats to the homeland; 6) Rapid domestic response and recovery to attacks and incidents; 7) Protect and stabilize the Nation's economy; 8) Provide critical Federal Government services for the health, safety, and welfare needs of the U.S.

continuity relationships can be uncovered between higher-level business functions.[40]

In closing, this entire series on Continuity of Operations (COOP) has emphasized how such a difficult function as COOP, comprising as it does so many functions (mission resilience, stakeholder communications, organizational structure and decision making, human safety to include family members, recovery planning, reconstitution, and even devolution in the case of an unrecoverable disaster) can be planned to succeed even in a highly constrained personnel, time, and budget environment. Such an approach at the smallest program level leads to a more secure and more reliable federal government and military response capability; within the DoD, this ultimately leads to improved information and situational dominance for the most important customer of all: the Warfighter operating in the last mile.

[40] As a practical case in point: the author's own Business Continuity Course featured an interactive discussion in which one course student (an IT Director for a cloud-services organization) shared the amazing fact that a key component to *all lines of business* and *all revenue functions* was a single legacy "AS 400" computer system connected to the FDIC. That single-point-of-failure bound the entire company together in a way that only a thorough impact analysis at the IT Operations level could have uncovered. In no other higher-level business impact analysis had this common thread been understood or reported.

Appendix A: Sample COOP Plan

This section provides a sample Continuity of Operations (COOP) Plan based upon FEMA's plan template described in "The FEMA Coop Web Site" section from this paper. This template provides the COOP Practitioner with an A to Z COOP solution guide, and the best-practices represented by this federal plan apply well to the Army Program use case.

This sample COOP is broken down based on FEMA's outline and as described in Section "3.2.2 FEMA COOP Plan Template Sections." Bolded text represents the areas customized for the Army Program use case. Where information cannot be provided due to privacy / possible security concerns, the bolded text indicates "REDACTED." Where the FEMA plan template references an "owning organization" the bolded text indicates [OWNING PROGRAM] to maintain the privacy of the Army Program use case.

The FEMA plan template presented here applies well to a large mix of federal organizations, but does not apply exactly to the Army Program use case. The template is used to demonstrate how closely aligned the federal and DoD COOP processes are; where applicable, additional DoD-specific communications and verbiage have been added.

A.1 BASIC PLAN

I. Promulgation Statement

The **ARMY PROGRAM**'s mission is to **ensure the cloud-based delivery of solutions and infrastructure to Army and DoD customers**. To accomplish this mission, **ARMY PROGRAM** must ensure its operations are performed efficiently with minimal disruption, especially during an emergency. This document provides planning and program guidance for implementing the **ARMY PROGRAM** Continuity of Operations Plan and programs to ensure the organization is capable of conducting its essential missions and functions under all threats and conditions.

Key **ARMY PROGRAM** personnel who are relocated under this plan are collectively known as the **Emergency Relocation Group**. Upon plan activation, these members will deploy to **SECONDARY IT FACILITY**. Upon arrival, continuity personnel must establish an operational capability and perform essential functions within 12 hours from the time of the activation of the Continuity Plan, for up to a 30-day period or until normal operations can be resumed.

This plan has been developed in accordance with guidance in Executive Order (EO) 12656, *Assignment of Emergency Preparedness Responsibilities*; National Security Presidential Directive – 51/Homeland Security Presidential Directive – 20, *National Continuity Policy*; Homeland Security Council, *National Continuity Policy Implementation Plan*; Federal Continuity Directive (FCD) 1, *Federal Executive Branch National Continuity Program and Requirements*, February 2008; **ARMY PROGRAM** Management Directive **DoD Directive 3020.26, Army Regulation 500-3**, and other related Directives and guidance.

[Organization Head signs here]

[Enter Organization Head's name here]

[Enter Organization Head's title here]

[Enter Organization Name here]

II. Record of Changes

Table 3: COOP Plan: Document Change Table

Change Number	Section	Date of Change	Individual Making Change	Description of Change
1	All	20 AUG 11	Owner	Initial creation

III. Record of Distribution

Table 4: COOP Plan: Document Transmittal Record

Date of Delivery	Number of Copies Delivered	Method of Delivery	Name, Title, and Organization of Receiver
20 AUG 11	1	Email	Business Continuity Management Course Instructor

IV. Purpose, Scope, Situations, and Assumptions

A. PURPOSE

The **ARMY PROGRAM**'s mission is to **ensure the cloud-based delivery of solutions and infrastructure to Army and DoD customers**. To accomplish this mission, **ARMY PROGRAM** must ensure its operations are performed efficiently with minimal disruption, especially during an emergency. This document provides planning and program guidance for implementing the **ARMY PROGRAM** Continuity of Operations Plan and programs to ensure the organization is capable of conducting its essential missions and functions under all threats and conditions. While the severity and consequences of an emergency cannot be predicted, effective contingency planning can minimize the impact on **ARMY PROGRAM** missions, personnel, and facilities.

The overall purpose of continuity of operations planning is to ensure the continuity of the National Essential Functions (NEFs) under all conditions. The current changing threat environment and recent emergencies, including acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents, have increased the need for viable continuity of operations capabilities and plans that enable agencies to continue their essential functions across a spectrum of emergencies. These conditions, coupled with the potential for terrorist use of weapons of mass destruction, have increased the importance of having continuity programs that ensure continuity of essential government functions across the Federal Executive Branch.

B. SCOPE

This Plan applies to the functions, operations, and resources necessary to ensure the continuation of **ARMY PROGRAM**'s essential functions, in the event its normal operations at **PRIMARY IT FACILITY** are disrupted or threatened with disruption. This plan applies to all **ARMY PROGRAM** personnel. **ARMY PROGRAM** staff must be familiar with continuity policies and procedures and their respective continuity roles and responsibilities.

This document ensures **ARMY PROGRAM** is capable of conducting its essential missions and functions under all threats and conditions, with or without warning.

C. SITUATION OVERVIEW

According to NSPD 51/HSPD 20, it is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government programs in order to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions. Continuity requirements shall be incorporated into daily operations of all executive departments and agencies.

Further, continuity planning must be based on the assumption that organizations will not receive warning of an impending emergency. As a result, a risk assessment is essential to focusing continuity planning. Risk-specific appendices that address the results of the **ARMY PROGRAM** risk assessment are found later in the plan.

The **ARMY PROGRAM** continuity facilities were selected following an all-hazards risk assessment of facilities for continuity operations use. The **ARMY PROGRAM** risk assessment is found at **[CANNOT BE PROVIDED FOR THIS PAPER]**. This risk assessment addresses the following for each continuity facility:

- Identification of all hazards
- A vulnerability assessment to determine the effects of all hazards
- A cost-benefit analysis of implementing risk mitigation, prevention, or control measures
- A formal analysis by management of acceptable risk

- Sufficient distance between each facility location or threatened area and other facilities or locations that are potential sources of disruptions or threats
- Sufficient levels of physical security required to protect against identified threats
- Sufficient levels of information security required to protect against identified threats

Further, **ARMY PROGRAM** has evaluated its daily operating facilities in accordance with Interagency Security Commission Standards or applicable organization standards. This evaluation is found at **[CANNOT BE PROVIDED FOR THIS PAPER]**.

D.PLANNING ASSUMPTIONS

This Continuity Plan is based on the following assumptions:

- An emergency condition may require the relocation of **ARMY PROGRAM**'s Emergency Relocation Group (ERG) members to the continuity facility at **DISA DECC FACILITY.**
- The **DISA DECC FACILITY** will support ERG members and the continuation of **ARMY PROGRAM** essential functions by available communications and information systems within 12 hours or less from the time the Continuity of Operations Plan is activated, for potentially up to a 30-day period or until normal operations can be resumed
- **ARMY PROGRAM** regional operations are unaffected and available to support actions directed by the **HEAD OF SOFTWARE ENGINEERING CENTER** or his successor. However, in the event that ERG deployment is not feasible due to the loss of personnel, the **ARMY PROGRAM** will devolve to **ARMY MATERIEL COMMAND.**
- **DISA DECC FACILITY maintains sufficient operating capability to handle COOP requirements the ARMY PROGRAM as well as at least three other programs of equal size at all times.**
- **ARMY PROGRAM customers continue to require cloud consumption capabilities; upon a lack of activity for 24 hours the DISA DECC FACILITY will stand down COOP operations for ARMY PROGRAM.**

E.OBJECTIVES

The continuity planning objectives that all Federal Executive Branch departments and agencies are required to meet are identified in Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, dated February 2008.

The **ARMY PROGRAM** continuity objectives are listed below:

(1) Ensure that **ARMY PROGRAM** can perform its Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs), if applicable, under all conditions

(2) Reduce the loss of life and minimize property damage and loss

(3) Execute a successful order of succession with accompanying authorities in the event a disruption renders **[Organization Name]** leadership unable, unavailable, or incapable of assuming and performing their authorities and responsibilities of the office

(4) Reduce or mitigate disruptions to operations

(5) Ensure that **[Organization Name]** has facilities where it can continue to perform its MEFs and PMEFs, as appropriate, during a continuity event

(6) Protect essential facilities, equipment, records, and other assets, in the event of a disruption

(7) Achieve **[Organization Name]**'s timely and orderly recovery and reconstitution from an emergency

(8) Ensure and validate continuity readiness through a dynamic and integrated continuity test, training, and exercise program and operational capability

F. SECURITY AND PRIVACY STATEMENT

This document is **[insert classification information here, e.g. For Official Use Only]**. Portions of this Plan containing information that raises personal privacy or other concerns may be exempt from mandatory disclosure under the Freedom of Information Act (see 5 United States Code §552, 41 Code of Federal Regulations Part 105-60). This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with **[insert security reference document]** and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of **[insert title of approving authority]**.

Some of the information in this Plan, if made public, could endanger the lives and privacy of employees. In addition, the disclosure of information in this plan could compromise the security of essential equipment, services, and systems of **ARMY PROGRAM** or otherwise impair its ability to carry out essential functions. Distribution of the Continuity plan in whole or in part is limited to those personnel who need to know the information in order to successfully implement the plan.

ARMY PROGRAM, PROGRAM MANAGEMENT OFFICE will distribute copies of the Continuity Plan on a need to know basis. **COOP Plans will be distributed via DoD-standard encrypted email and via secure, CAC-enabled, and permission-trimmed Web sites**. In addition, copies of the plan will be distributed to other organizations as necessary to promote information sharing and facilitate a coordinated interagency continuity effort. Further distribution of the plan, in hardcopy or electronic form, is not allowed without approval from **PROGRAM MANAGEMENT OFFICE**. **ARMY PROGRAM, PROGRAM MANAGEMENT OFFICE** will distribute updated versions of the Continuity Plan annually or as critical changes occur.

V. Concept of Operations

A. PHASE I: READINESS AND PREPAREDNESS

ARMY PROGRAM participates in the full spectrum of readiness and preparedness activities to ensure its personnel can continue essential functions in an all-hazard risk environment. **ARMY PROGRAM** readiness activities are divided into two key areas:

- Organization readiness and preparedness
- Staff readiness and preparedness

Organization Readiness and Preparedness

ARMY PROGRAM preparedness incorporates several key components. Two major components of readiness are the Continuity of Government Conditions (COGCON), for organizations in the National Capital Region, and the DHS Homeland Security Advisory System (HSAS). **ARMY PROGRAM** uses other warning and threat systems, which include **DoD Force Protection Condition (FPCON)**.

COGCON Procedures

The **ARMY PROGRAM** has established internal plans and procedures for executing changes to the COGCON level, if applicable. In addition to the items set forth in Annex M and N of FCD 1, **ARMY PROGRAM** has identified the following additional activities to undertake at each COGCON level, if applicable.

Table 5: COOP Plan: COGCON Level Activities

COGCON Level	Activity	Frequency
Level 4	Ongoing operational readiness checks Continue to perform operations at regular locations	Daily
Level 3	Perform additional training Ongoing operational readiness checks Continue to perform operations at regular locations	Weekly Daily
Level 2	Perform additional training Ongoing operational readiness checks Continue to perform operations at regular locations	Weekly Daily

	Ensure alternate location can be activated within 12 hours	
Level 1	Perform additional training Ongoing operational readiness checks Continue to perform operations at regular locations Ensure alternate location can be activated immediately	Daily Semi-daily

HSAS Procedures

Further, **ARMY PROGRAM** has established internal plans and procedures for executing changes to the HSAS level. **ARMY PROGRAM** has identified the following activities to undertake at each HSAS level.

Table 6: COOP Plan: HSPD-3 Threat Level Activities

HSPD-3 Threat Condition Level	HSPD-3 Threat Condition Criteria	ARMY PROGRAM Specific Response
Green (Low)	There is a low risk of terrorist attacks.	The continuity plan is not activated.
Blue (Guarded)	There is a general risk of terrorist attacks.	The continuity plan is not activated.
Yellow (Elevated)	There is a significant risk of terrorist attacks.	Place continuity personnel upon alert if there is a specific threat in the region.
Orange (High)	There is a high risk of terrorist attacks.	Place continuity personnel on alert if there is a non-specific threat and/or activate the continuity plan if there is a specific threat to the region.
Red	There is a severe risk of terrorist attacks.	Activate the continuity plan if there is a specific threat to the

(Severe)		region.

Other Warning and Threat System Procedures

Upon notification from other identified stakeholders of a related threat level, apply that as warning input to ARMY PROGRAM.

Staff Readiness and Preparedness

ARMY PROGRAM personnel must also prepare for a continuity event. **ARMY PROGRAM** personnel should plan in advance what to do in an emergency and should develop a Family Support Plan to increase personal and family preparedness. To develop your Family Support Plan, use the templates available at www.ready.gov. This site includes a “Get Ready Now” pamphlet, which explains the importance of planning and provides a template that you and your family can use to develop your specific plan. If you need assistance in creating your family support plan, please contact **ARMY PROGRAM PMO**.

ARMY PROGRAM continuity personnel have the responsibility to create and maintain drive-away kits. Continuity personnel are responsible for carrying the kits to the continuity facility or pre-storing the kits at the continuity site. **ARMY PROGRAM** has identified what these kits should contain in the following table. In order to maintain currency of drive-away kits, **ARMY PROGRAM** has established procedures for updating the kits. **These procedures include: having continuity personnel bring kits on annual exercises, distributing quarterly update materials, and establishing an acquisition program to regularly replace agency-supplied emergency items**.

Table 7: COOP Plan: Drive Away Kit

Drive Away Kit	
• Identification and charge cards ○ Government identification card ○ Drivers license ○ Government travel card ○ Health insurance card ○ Personal charge card • Communication equipment ○ Pager/BlackBerry ○ Government cell phone ○ Personal cell phone ○ Government Emergency Telephone Service card • Hand-carried vital records	• Business and personal contact numbers ○ Emergency phone numbers and addresses (relatives, medical doctor, pharmacist) • Toiletries • Chargers/Extra Batteries for phones, GPS, and laptop • Directions to continuity facility • Bottled water and non-perishable food (i.e., granola, dried fruit, etc.) • Medical needs ○ Insurance information ○ List of allergies/blood type ○ Hearing aids and extra batteries

- Directions to continuity facility
- Maps of surrounding area
- Business and leisure clothing
- Continuity plan
- Flashlight

- Glasses and contact lenses
- Extra pair of eyeglasses/contact lenses
- Prescription drugs (30-day supply)
- o Over-the-counter medications, dietary supplements

In addition, **ARMY PROGRAM** conducts the following continuity readiness and preparedness activities: **Orientation training, brown bags, working lunch informational sessions, and senior leadership addresses to the organization regarding continuity**.

B. PHASE II: ACTIVATION AND RELOCATION

To ensure the ability to attain operational capability at continuity sites and with minimal disruption to operations, **ARMY PROGRAM** has developed detailed activation and relocation plans, which are captured in the following sections.

Decision Process Matrix

Based on the type and severity of the emergency situation, the **ARMY PROGRAM** Continuity Plan may be activated by one of the following methods:

(1) The President may initiate Federal Executive Branch continuity activation

(2) The **Secretary of Defense**, or a designated successor, may initiate the Continuity Plan activation for the entire organization, based on an emergency or threat directed at the organization

(3) The Director of Army Materiel Command (AMC) may initiate the Continuity Plan throughout AMC; the Director of Communications – Electronics Command (CECOM) may initiate the Continuity Plan throughout CECOM; the [OWNING ORGANIZATION] may initiate the Continuity Plan; the ARMY PROGRAM Commander may request initiation of the Continuity Plan based upon local circumstances.

Continuity Plan activation and relocation are scenario-driven processes that allow flexible and scalable responses to the full spectrum of emergencies and other events that could disrupt operations with or without warning during duty and non-duty hours. Continuity Plan activation is not required for all emergencies and disruptive situations, since other actions may be deemed appropriate. The decision to activate the **ARMY PROGRAM** Continuity Plan and corresponding actions to be taken are tailored for the situation, based upon projected or actual impact and severity, that may occur with or without warning. Decision-makers may use the below decision matrix to assist in the decision to activate the Continuity Plan.

Table 8: COOP Plan: Decision Matrix

Decision Matrix for Continuity Plan Implementation

	Duty Hours	Non-Duty Hours
Event With Warning	• Is the threat aimed at the facility or surrounding area? • Is the threat aimed at organization personnel? • Are employees unsafe remaining in the facility and/or area? • [Insert additional points here]	• Is the threat aimed at the facility or surrounding area? • Is the threat aimed at organization personnel? • Who should be notified of the threat? • Is it safe for employees to return to work the next day?
Event Without Warning	• Is the facility affected? • Are personnel affected? Have personnel safely evacuated or are they sheltering-in-place? • What are instructions from first responders? • How soon must the organization be operational?	• Is the facility affected? • What are instructions from first responders? • How soon must the organization be operational?

As the decision authority, the **ARMY PROGRAM** will be kept informed of the threat environment using all available means, including official government intelligence reports, national/local reporting channels, and news media. The **ARMY PROGRAM** will evaluate all available information relating to:

(1) Direction and guidance from higher authorities

(2) The health and safety of personnel

(3) The ability to execute essential functions

(4) Changes in readiness or advisory levels

(5) Intelligence reports

(6) The potential or actual effects on communication systems, information systems, office facilities, and other vital equipment

(7) The expected duration of the emergency situation

(8) Guidance from Secretary of Defense, AMC, CECOM, and other DoD / Army organizations as appropriate.

Alert and Notification Procedures

ARMY PROGRAM maintains plans and procedures for communicating and coordinating activities with personnel before, during, and after a continuity event.

Prior to an event, personnel in **ARMY PROGRAM** must monitor advisory information, including the DHS Homeland Security Advisory System, the Federal Government Response Stages for Pandemic Influenza, intelligence, and **DoD FPCON**. In the event normal operations are interrupted or if an incident appears imminent, **ARMY PROGRAM** will take the following steps to communicate the organization's operating status with all staff:

(1) The **ARMY PROGRAM Commander** or designated successor will notify **[OWNING PROGRAM PMO]** of the emergency requiring continuity activation

(2) The ARMY PROGRAM Operations Officer commences notification, and operations personnel along with customer support must respond to the operations officer upon notification.

(3) ARMY PROGRAM personnel will notify family members, next of kin, and/or emergency contacts of the continuity plan activation

Upon the decision to activate the continuity plan or to reconstitute following an event, **ARMY PROGRAM** will notify all **ARMY PROGRAM** personnel, as well as affected and interdependent entities with information regarding continuity activation and relocation status, operational and communication status, and the anticipated duration of relocation. These entities include:

- Continuity facilities and on-site support teams with information regarding continuity activation and relocation status and the anticipated duration of relocation
- FEMA Operations Center (FOC) via the RRS or telephone (540.665.6100 or 800.634.7084) and other applicable operations centers with information regarding continuity activation and relocation status, the **ARMY PROGRAM** alternate location, operational and communication status, and anticipated duration of relocation
- All **ARMY PROGRAM** employees, both continuity personnel and non-deployed personnel with instructions and guidance regarding the continuity activation and relocation
- **[OWNING PROGRAM PMO]**

Relocation Process

Following activation of the plan and notification of personnel, **ARMY PROGRAM** must move personnel and vital records to a continuity facility. Upon activation, **ARMY PROGRAM** continuity personnel deploy to the assigned continuity facility to perform **ARMY PROGRAM** essential functions and other continuity tasks. A map and directions to the continuity facility is found **[REDACTED]**.

Emergency procedures during duty hours with or without a warning are as follows:

- Continuity personnel, including advance team personnel, if applicable, will depart to their designated continuity facility from the primary operating facility or their current location using **privately owned vehicles, buses, or trains. Disabled continuity employees will be transported using accessible government-furnished conveyances.**
- Individuals who are not continuity personnel present at the primary operating facility or another location at the time of an emergency notification will receive instructions from **ARMY PROGRAM Operations Officer**. In most scenarios, staff members will be directed to proceed to their homes or to other **ARMY PROGRAM** facilities to wait for further guidance.
- At the time of notification, information will be provided on routes to use during departure from the primary operating facility, if available, or other appropriate safety precautions.

Emergency procedures during non-duty hours with or without a warning are as follows:

- Advance team members, if applicable, will deploy to their assigned continuity facility from his/her current location using **privately owned vehicles, buses, or trains. Disabled continuity employees will be transported using accessible government-furnished conveyances.**
- Each continuity member will depart to his/her assigned continuity facility from his/her current location using **privately owned vehicles, buses, or trains. Disabled continuity employees will be transported using accessible government-furnished conveyances. This will occur** at **the time specified during notification**.
- Individuals who are not continuity personnel will remain at his or her residence to wait for further instructions.

Personnel not identified as continuity staff may be required to replace or augment the identified continuity personnel during activation. These activities will be coordinated by **ARMY PROGRAM Operations Officer** with the staff on a case-by-case basis. Individuals who are not identified as continuity personnel will remain available to replace or augment continuity members, as required.

ARMY PROGRAM Operations Officer will direct **ARMY PROGRAM** personnel who are not designated as continuity personnel to move to **another duty station or home** until further notice.

In the event of an activation of the Continuity Plan, **ARMY PROGRAM** may need to procure necessary personnel, equipment, and supplies that are not already in place for continuity operations on an emergency basis. **ARMY PROGRAM Commander** maintains the authority for emergency procurement. Instructions for these actions are found **within the ARMY PROGRAM PMO acquisition and maintenance plans**.

C. PHASE III: CONTINUITY OPERATIONS

Upon activation of the Continuity of Operations Plan, **ARMY PROGRAM** will continue to operate at its primary operating facility until ordered to cease operations by **[OWNING PROGRAM DIRECTOR], CECOM Director, or other relevant authority** using **encrypted and digitally signed email transmission or secure telephonic communications**. At that time, essential functions will transfer to the continuity facility. **ARMY PROGRAM** must ensure that the continuity plan can become operational within the minimal acceptable period for MEF disruption, but in all cases within 12 hours of plan activation.

The advance team will arrive at the continuity facility first to prepare the site for the arrival of the continuity personnel. Upon arrival at the continuity facility, the advance team will:

- Ensure infrastructure systems, such as power and HVAC are functional
- Prepare check-in duty stations for ERG arrival
- Field telephone inquiries from ERG and non-ERG staff
- **Verify that data backups and stored vital records are available**

As continuity personnel arrive at the continuity facility, **ARMY PROGRAM Operations Officer** will in-process the staff to ensure accountability. In-processing procedures are conducted in **[REDACTED]** and will consist of the following steps: **1) Locate the staff member in the continuity roster; 2) Update the time arrived for the staff member; 3) Notify the local area commander of the new arrival; 4) Locate current concept of operations (CONOPS) plan for the in-process activities; 5) Dispatch the staff member to the zone of operation (escorted). Individuals not accounted for will continue to be contacted at regular intervals not to exceed 90 minutes.** In addition, the office will identify all organization leadership available at the continuity facility.

Upon arrival at the continuity facility, **ARMY PROGRAM** continuity personnel will:

- Report immediately to **[REDACTED]** for check-in and in-processing
- Receive all applicable instructions and equipment
- Report to their respective workspace as identified in **the current CONOPS plan** or as otherwise notified during the activation process
- Retrieve pre-positioned information and activate specialized systems or equipment
- Monitor the status of **ARMY PROGRAM** personnel and resources
- Continue **ARMY PROGRAM** essential functions
- Prepare and disseminate instructions and reports, as required
- Comply with any additional continuity reporting requirements with the FOC
- Notify family members, next of kin, and emergency contacts of preferred contact methods and information

A significant requirement of continuity personnel is to account for all **ARMY PROGRAM** personnel. **ARMY PROGRAM** will use the following processes to account for all personnel:

- **Call down telephone trees**
- **1-800 number as provided [REDACTED]**
- **Alert and notification system pager**
- **ARMY PROGRAM secure operations website.**

The ARMY PROGRAM Operations Officer is responsible for communicating with personnel who are unaccounted for via repeated communications attempt at intervals not to exceed 90 minutes.

During continuity operations, **ARMY PROGRAM** may need to acquire necessary personnel, equipment, and supplies on an emergency basis to sustain operations for up to 30 days or until normal operations can be resumed. **ARMY PROGRAM PMO** maintains the authority for emergency acquisition. Instructions for these actions are found **within the ARMY PROGRAM PMO acquisitions office**.

D. PHASE IV: RECONSTITUTION OPERATIONS

Within **72 hours** of an emergency relocation, the following individuals will initiate and coordinate operations to salvage, restore, and recover the **ARMY PROGRAM** primary operating facility after receiving approval from the appropriate local, State, and Federal law enforcement and emergency services:

- **ARMY PROGRAM Operations Officer** will serve as the Reconstitution Manager for all phases of the reconstitution process
- Each **ARMY PROGRAM** subcomponent will designate a reconstitution point-of-contact to work with the Reconstitution Team and to update office personnel on developments regarding reconstitution and provide names of reconstitution point-of-contact to **ARMY PROGRAM Operations Officer** within **24** hours of the Continuity Plan activation

During continuity operations, **ARMY PROGRAM operations offer** must access the status of the facilities affected by the event by **physical inspection, verbal reports from selected team members, or by CONOPS-directed local supervisors**. Upon obtaining the status of the facility, **ARMY PROGRAM** will determine how much time is needed to repair the affected facility and/or acquire a new facility. This determination is made in conjunction with **[OWNING PROGRAM]**. Should **ARMY PROGRAM** decide to repair the affected facility, **ARMY PROGRAM Operations Officer** has the responsibility of supervising the repair process and must notify **ARMY PROGRAM Commander** of the status of repairs, including estimates of when the repairs will be completed.

Reconstitution procedures will commence when the **ARMY PROGRAM Commander** or other authorized person ascertains that the emergency situation has ended and is unlikely to reoccur. These reconstitution plans are viable regardless of the level of disruption that originally prompted implementation of the Continuity of Operations Plan. Once the appropriate **ARMY PROGRAM** authority has made this determination in coordination with other Federal and/or other applicable authorities, one or a combination of the following options may be implemented, depending on the situation:

- Continue to operate from the continuity facility
- Reconstitute the **ARMY PROGRAM** primary operating facility and begin an orderly return to the facility
- Begin to establish a reconstituted **ARMY PROGRAM** in some other facility in the metro area or at another designated location

Prior to relocating to the current primary operating facility or another facility, **ARMY PROGRAM Operations Officer** will conduct appropriate security, safety, and health assessments to determine building suitability. In addition, **ARMY PROGRAM Operations Officer** will verify that all systems, communications, and other required capabilities are available and operational and that **ARMY PROGRAM** is fully capable of accomplishing all essential functions and operations at the new or restored facility.

Upon a decision by the **ARMY PROGRAM** or other authorized person that the **ARMY PROGRAM** primary operating facility can be reoccupied or that **ARMY PROGRAM** will re-establish itself in a different facility:

- The **ARMY PROGRAM** Continuity Coordinator or other authorized individual must notify the FEMA Operations Center (FOC) via telephone (540.665.6100 or 800.634.7084) or RRS, when available, and other applicable operations centers with information regarding continuity activation and relocation status, the **ARMY PROGRAM** alternate location, operational and communication status, and anticipated duration of relocation. **ARMY PROGRAM** shall submit a Continuity Status Reporting Form, only if it contains more information beyond what has been reported, to fema-ncp-coop@dhs.gov, by fax to 940.323.2822, or **[REDACTED]** using the form and procedures provided by FEMA's National Continuity Programs Directorate or other specified continuity point-of-contact.
- **ARMY PROGRAM Operations Officer** will develop space allocation and facility requirements
- **ARMY PROGRAM Operations Officer** will notify all personnel that the emergency or threat of emergency has passed and actions required of personnel in the reconstitution process using **encrypted and digitally signed email or other secure telephonic transmissions**
- **ARMY PROGRAM Commander** will coordinate with the General Services Administration (GSA) and/or other applicable facility management group to obtain office space for reconstitution, if the primary operating facility is uninhabitable
- **ARMY PROGRAM Operations Officer** will develop procedures, as necessary, for restructuring staff

Upon verification that the required capabilities are available and operational and that **ARMY PROGRAM** is fully capable of accomplishing all essential functions and operations at the new or restored facility, **ARMY PROGRAM Commander** will begin supervising a return of personnel, equipment, and documents to the normal operating facility or a move to another temporary or permanent primary operating facility. The phase-down and return of personnel, functions, and equipment will follow the priority-based plan and schedule outlined below; **ARMY PROGRAM** will begin development of specialized return plans based on the incident and facility within **72** hours of plan activation.

ARMY PROGRAM will continue to operate at its continuity facility until ordered to cease operations by **[OWNING PROGRAM] or other authorized entity** using **encrypted and digitally signed email or other secure telephonic transmissions**. At that time, essential functions will transfer to the primary operating facility. **ARMY PROGRAM** has developed plans to instruct personnel on how to resume normal operations as outlined below; **ARMY PROGRAM** will begin development of specialized resumption plans based on the incident and facility within **72** hours of plan activation.

ARMY PROGRAM PMO will identify any records affected by the incident by **reviewing them with the ARMY PROGRAM Operations Officer**. In addition, **ARMY PROGRAM PMO** will effectively transition or recover vital records and databases, as well as other records that had not been designated as vital records, using the plan outlined below; **ARMY PROGRAM** will begin development of specialized vital records transition and recovery plans based on the incident and facility within **72** hours of plan activation.

When the continuity personnel, equipment, and documents are in place at the new or restored primary operating facility, the remaining **ARMY PROGRAM** staff at the continuity facility or devolution site will transfer essential functions, cease operations, and deploy to the new or restored primary operating facility. **ARMY PROGRAM Operations Officer** shall oversee the orderly transition from the continuity facility of all **ARMY PROGRAM** functions, personnel, equipment, and records to a new or restored primary operating facility. **ARMY PROGRAM human resources** is responsible for developing a process for receiving and processing employee claims during the continuity event, including processing human capital claims (including, workmans compensation for injuries, overtime pay, etc) and replacing lost or broken equipment.

ARMY PROGRAM will conduct an After Action Review (AAR) once it is back in the primary operating facility or established in a new primary operating facility. **ARMY PROGRAM Operations Officer** has the responsibility for initiating and completing the AAR. All offices within **ARMY PROGRAM** will have the opportunity to provide input to the AAR. This AAR will study the effectiveness of the continuity plans and procedures, identify areas for improvement, document these in the **ARMY PROGRAM** corrective action program (CAP), and then develop a remedial action plan as soon as possible after the reconstitution. **ARMY PROGRAM Operations Officer** has the responsibility for documenting areas for improvement in the CAP and developing a remedial action plan. In addition, the AAR will identify which, if any, records were affected by the incident, and will work with **ARMY PROGRAM PMO** to ensure an effective transition or recovery of vital records and databases and other records that had not been designated as vital records. AAR and CAP documentation are maintained by **ARMY PROGRAM PMO** and are found within **ARMY PROGRAM PMO configuration management database**.

E. DEVOLUTION OF CONTROL AND DIRECTION

ARMY PROGRAM is prepared to transfer all of their essential functions and responsibilities to personnel at a different location should emergency events render leadership or staff unavailable to support the execution of **ARMY PROGRAM** essential functions. If deployment of continuity personnel is not feasible due to the unavailability of personnel, temporary leadership of **ARMY PROGRAM** will devolve to **[OWNING PROGRAM**

DIRECTOR].

ARMY PROGRAM Operations Officer maintains responsibility for ensuring the currency of the **ARMY PROGRAM** devolution plan. The **ARMY PROGRAM** devolution plan:

(1) Includes the elements of a viable continuity capability: program plans and procedures, budgeting and acquisitions, essential functions, orders of succession and delegations of authority specific to the devolution site, interoperable communications, vital records management, staff, test, training, and exercise (TT&E), and reconstitution. The **ARMY PROGRAM** devolution plan is located **within the ARMY PROGRAM PMO configuration management database**.

(2) Identifies prioritized essential functions, defines tasks that support those essential functions, and determines the necessary resources to facilitate those functions. The list of prioritized essential functions for devolution is found at **within the ARMY PROGRAM PMO configuration management database**.

(3) Includes a roster that identifies fully equipped and trained personnel who will be stationed at the designated devolution site and who will have the authority to perform essential functions and activities when the devolution option of the continuity plan is activated. The devolution personnel roster is found at **within the ARMY PROGRAM PMO configuration management database**.

(4) Identifies what would likely activate or “trigger” the devolution option and specifies how and when direction and control of **ARMY PROGRAM** operations will be transferred to and from the devolution site. Devolution activation protocols or “triggers’ are found **within the ARMY PROGRAM PMO configuration management database**.

(5) Determines and lists or references the necessary resources (i.e., equipment and materials) to facilitate the immediate and seamless transfer of and performance of essential functions at the devolution site. The list of necessary resources for devolution is found at **within the ARMY PROGRAM PMO configuration management database**.

(6) Establishes and maintains reliable processes and procedures for acquiring the resources necessary to continue essential functions and to sustain those operations for extended periods. The **ARMY PROGRAM Operations Officer** is responsible for acquiring resources during a devolution situation. Acquisition processes and procedures are found **within the ARMY PROGRAM PMO acquisitions department**.

(7) Establishes and maintains a capability to restore or reconstitute **ARMY PROGRAM** authorities to their pre-event status upon termination of devolution.

ARMY PROGRAM conducts and documents annual training of devolution staff and a biennial exercise to ensure devolution capabilities are prepared and capable of performing essential functions. This documentation includes the dates of all TT&E events and names of participating staff. The **ARMY PROGRAM** devolution TT&E documentation is maintained by **ARMY PROGRAM Operations Officer** and is found at **within the ARMY PROGRAM PMO configuration management database**. Further, the **ARMY PROGRAM** CAP supports the devolution program. The **ARMY**

PROGRAM CAP is maintained by **ARMY PROGRAM PMO** and CAP documentation is found at **within the ARMY PROGRAM PMO configuration management database**.

VI. Organization and Assignment of Responsibilities

Key staff positions within **ARMY PROGRAM**, to include individual continuity members, those identified in the order of succession and delegation of authority, the **ARMY PROGRAM** Continuity Coordinator, continuity managers, and others possess additional continuity responsibilities. The responsibilities of these key continuity personnel are delineated **within the ARMY PROGRAM PMO configuration management database**.

Table 9: COOP Plan: Continuity of Operations Responsibilities

Position	Responsibilities
Commander	• Provide strategic leadership and overarching policy direction for the continuity program • Implement the Continuity of Operations Plan when necessary, or when directed by higher authority • Update and promulgate orders of succession and delegations of authority • Ensure adequate funding is available for emergency operations • Ensure all organization components participate in continuity exercises • Update continuity of operations plan annually
Communications Specialist, Standards and Planning Division	• Update telephone rosters monthly • Conduct alert and notification tests
Records Specialist, Standards and Planning Division	• Review status of vital files, records, and databases
Training Specialist, Standards and Planning Division	• Develop and lead Continuity of Operations training • Plan Continuity of Operations exercises
Continuity Personnel	• Be prepared to deploy and support organization essential functions in the event of a Continuity Plan implementation • Provide current contact information to their manager

	• Be familiar with continuity planning and know individual roles and responsibilities in the event of continuity of operations plan activation • Participate in continuity training and exercises as directed • Have a telework agreement for this position, if applicable

VII. Direction, Control, and Coordination

During an activation of the Continuity Plan, the **ARMY PROGRAM Commander** maintains responsibility for direction and control of **ARMY PROGRAM**. Should the **ARMY PROGRAM Commander** become unavailable or incapacitated; the organization will follow the directions laid out in Annex V.A, *Orders of Succession*, and Annex V.B, *Delegations of Authority*.

The contents and procedures laid forth in this Continuity Plan are consistent with the direction found in Federal Continuity Directive 1. As a result, this Plan and its concepts are integrated horizontally with other Federal executive branch organizations. Further, the Plan is reviewed and vetted by **ARMY PROGRAM PMO Risk Management** to ensure vertical integration within **ARMY PROGRAM**.

VIII. Disaster Intelligence

During a continuity event, **ARMY PROGRAM** will require the collection and dissemination of critical information. While specific incidents may cause additional or specialized reporting requirements, the following table lists examples of the information that **ARMY PROGRAM** must collect and report regardless of incident type during a continuity event.

Table 10: COOP Plan: Disaster Intelligence Collection

Information Element	Specific Requirement	Responsible Element	Deliverables	When Needed	Distribution
Personnel Accountability	Account for all ERG and non-ERG employees Account for all contract personnel	Human Capital Division	Report Briefing	Status update hourly following Plan activation	**ARMY PROGRAM Commander**
Operational Status	Percent of ERG personnel arrived at site	Continuity Manager Divisional representatives	Situation briefings Situation reports	NLT than 6 hours after plan activation, then hourly	**ARMY PROGRAM Commander**

	Ability to conduct each essential function Status of communications and IT systems				
Hazard Information	Threat details specific to the continuity facility	Response coordination center or emergency operations center	Situation briefings Situation reports	Two times per day at shift change	**ARMY PROGRAM Operations Officer** **Each department head**

IX. Communications

ARMY PROGRAM has identified available and redundant critical communication systems that are located at the primary operating facility and continuity facility. Further, **ARMY PROGRAM** maintains fully capable continuity communications that could support organization needs during all hazards, to include pandemic and other related emergencies, and give full consideration to supporting social distancing operations including telework and other virtual offices. In addition, [Organization Name] maintains communications equipment for use by employees with disabilities and hearing impairment.

All **ARMY PROGRAM** necessary and required communications and IT capabilities must be operational as soon as possible following continuity activation, and in all cases, within 12 hours of continuity activation.

Additional detailed information on **ARMY PROGRAM** communications systems and requirements is found in Annex IV, *Continuity Communications*.

X. Budgeting and Acquisition

ARMY PROGRAM budgets for and acquires those capabilities that are essential to continuity. A copy of the continuity budget is found **ARMY PROGRAM PMO**. Within this budget, **ARMY PROGRAM** budgets for continuity capabilities in accordance with National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20 and National Communications System Directive 3-10 or other applicable directives and provides for the acquisition of those resources necessary for continuity operations on an emergency basis for up to 30 days or until normal operations can be resumed.

As part of the budget process, **ARMY PROGRAM** uses a risk management methodology to identify, prioritize, and justify the allocation of budgetary resources. The risk management methodology used is **ARMY FIELD MANUAL 5-19 ("Composite Risk Management")** and a copy of the risk management documents can be found **ARMY PROGRAM PMO Risk Management**.

ARMY PROGRAM integrates the continuity budget with its multiyear strategy and program management plan and links the budget directly to objectives and metrics set forth in that plan. A copy of the multiyear strategy and program management plan is found **ARMY PROGRAM PMO Acquisition**.

For those contracts vital to the support of organization essential functions, **ARMY PROGRAM** has ensured contractor statements of work include the provision to provide staffing, services, and necessary resources during emergency conditions. A list of vital contracts is found **ARMY PROGRAM PMO Acquisition Management System** and maintained by **ARMY PROGRAM PMO**. During an emergency situation, **ARMY PROGRAM PMO Acquisition** is responsible for oversight and handling of emergency work by contractors.

XI. Plan Development and Maintenance

The **ARMY PROGRAM PMO Risk Management** is responsible for maintaining the **ARMY PROGRAM** Continuity of Operations Plan.

This Continuity Plan, **ARMY PROGRAM** essential functions, and supporting activities, will be reviewed by **ARMY PROGRAM PMO Risk Management** and updated annually from the date of publication as part of the annual maintenance of Continuity plans and procedures. **ARMY PROGRAM PMO Risk Management** is responsible for the annual plan review and update. In addition, the plan will be updated or addended when there are significant organizational or procedural changes or other events that impact continuity processes or procedures. Comments or suggestions for improving this plan may be provided to **ARMY PROGRAM PMO Risk Management** at any time.

A.2 FUNCTIONAL ANNEXES

I. Essential Functions

A. IDENTIFICATION OF ESSENTIAL FUNCTIONS

ARMY PROGRAM has completed the MEF/PMEF process as identified in FCD 2 to identify those functions that **ARMY PROGRAM** must continue.

Government Functions

To identify, prioritize, and document essential functions, **ARMY PROGRAM** first identified all government functions and missions and reviewed which functions were directed by applicable laws, presidential directives, executive orders, and other directives. **ARMY PROGRAM** government functions are **the location and support of Army data services and cloud provisioning to support Army and DoD support organizations.**

Mission Essential Functions

Upon identifying all government functions, **ARMY PROGRAM** identified those functions that are MEFs and PMEFs. Mission Essential Functions are a limited set of agency-level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

- Per FCD 2, **ARMY PROGRAM** completed the following worksheets to identify and analyze MEFs. This documentation also identifies the components, processes, requirements, and interdependencies that ensured the continued performance of **ARMY PROGRAM** MEFs.
- MEF Identification Worksheet #1. This worksheet is documented at **ARMY PROGRAM PMO Risk Management configuration management** and is maintained by **ARMY PROGRAM PMO Risk Management**.
- MEF Identification Worksheet #2. This worksheet is documented at **ARMY PROGRAM PMO Risk Management configuration management** and is maintained by **ARMY PROGRAM PMO Risk Management**.
- MEF Business Process Analysis (BPA) Worksheet. This worksheet is documented at **ARMY PROGRAM PMO Risk Management configuration management** and is maintained by **ARMY PROGRAM PMO Risk Management**.
- MEF Business Process Elements Worksheet. This worksheet is documented at **ARMY PROGRAM PMO Risk Management configuration management** and is maintained by **[insert office/title]**.

ARMY PROGRAM MEFs, as validated and approved by the **ARMY PROGRAM Commander**, are as follows: **1) Support cloud systems for shared hosting environments; 2) Army Data Services Layer support; 3) Support Army data service access**.

Primary Mission Essential Functions

The ARMY PROGRAM has no identified PMEFs.

B. IDENTIFICATION OF CONTINUITY PERSONNEL

In order to continue its government functions, MEFs, and PMEFs, **ARMY PROGRAM** has determined the staff positions necessary to relocate under continuity plan activation. A copy of the current roster is found within **ARMY PROGRAM PMO Risk Management configuration management**. **ARMY PROGRAM PMO Risk Management** is responsible for maintaining roster currency and ensuring personnel are matched against needed positions.

Each continuity member is selected by **ARMY PROGRAM PMO Risk Management** based upon:

- The predetermined essential functions that must be performed, regardless of the operational status of the **ARMY PROGRAM** primary operating facility
- The member’s knowledge and expertise in performing these essential functions
- The member’s ability to rapidly deploy to the relocation site in an emergency situation

Table 11: COOP Plan: Example Continuity Plan Roster

Function	Title / Position	Name	Telephone Numbers	Additional Information
Function #1: Approve and oversee transition to alternate facility	ARMY PROGRAM Operations Officer *Alternate: ARMY PROGRAM PMO Quality Assurance*	[REDACTED]	[REDACTED]	[REDACTED]

II. Vital Records Management

"Vital records" refers to information systems and applications, electronic and hardcopy documents, references, and records, to include classified or sensitive data, needed to support PMEFs and MEFs during a continuity event. **ARMY PROGRAM** has incorporated its vital records program into the overall continuity program, plans, and procedures.

ARMY PROGRAM's vital records program incorporates into the overall continuity plan with a clear authority to include:

- Policies
- Authorities
- Procedures

The written designation of **ARMY PROGRAM** vital records manager

As soon as possible after activation of the Continuity Plan, but in all cases within 12 hours of activation, continuity personnel at the continuity facility for **ARMY PROGRAM** must have access to the appropriate media for accessing vital records, including:

- A local area network
- Electronic versions of vital records
- Supporting information systems and data

ARMY PROGRAM's official vital records program:

- Identifies and protects those records that specify how an organization will operate in an emergency or disaster
- Identifies those records necessary to the organization's continuing operations
- Identifies those records needed to protect the legal and financial rights of the Government and citizens

- Internal and external e-mail and e-mail archives
- Hard copies of vital records

Identifying Vital Records

ARMY PROGRAM has identified the following as vital to its operations, and has assigned responsibility for those records to **ARMY PROGRAM PMO Risk Management**, which includes a combination of continuity personnel, personnel in the chief information officer's department, and records management personnel.

ARMY PROGRAM maintains a complete inventory of vital records, along with the locations of and instructions on accessing those records. These records are located at **ARMY PROGRAM PMO Risk Management**. This inventory will be maintained at a back-up/offsite location located at **ARMY PROGRAM PMO Risk Management configuration management** by **ARMY PROGRAM PMO Risk Management** to ensure continuity if the primary site is damaged, destroyed, or unavailable.

ARMY PROGRAM PMO Risk Management developed and maintains a vital records plan packet or collection located at **ARMY PROGRAM PMO Risk Management**. The packet or collection includes:

- A hard copy or electronic list of **ARMY PROGRAM** key organization personnel and continuity personnel with up-to-date telephone numbers
- A vital records inventory with the precise locations of vital records prepared by **ARMY PROGRAM PMO Risk Management**
- Updates to the vital records
- Necessary keys or access codes
- Listing of the access requirements and sources of equipment necessary to access the records
- **ARMY PROGRAM** continuity facility locations
- Lists of records recovery experts and vendors provided by **ARMY PROGRAM PMO Risk Management** and located at **ARMY PROGRAM PMO Risk Management configuration management**
- A copy of the **ARMY PROGRAM** continuity plans

For the above items, **ARMY PROGRAM PMO Risk Management** is responsible for providing access requirements and lists of sources of equipment necessary to access the records (this may include hardware and software, microfilm readers, Internet access, and/or dedicated telephone lines). These requirements and lists are found at **ARMY PROGRAM PMO Risk Management configuration management**.

This packet will be annually reviewed by **[insert office]** with the date and names of the personnel conducting the review documented in writing to ensure that the information is current. A copy will be securely maintained at the **ARMY PROGRAM** continuity facilities and **other ARMY PROGRAM primary facilities**, so it is easily accessible to appropriate personnel when needed.

Protecting Vital Records

The protection of vital records is essential to ensuring the records are available during a continuity event, thus enabling agencies to conduct MEFs and PMEFs. **ARMY PROGRAM** has conducted a vital records and database risk assessment to:

- Identify the risks involved if vital records are retained in their current locations and media, and the difficulty of reconstituting those records if they are destroyed
- Identify offsite storage locations and requirements
- Determine if alternative storage media is available
- Determine requirements to duplicate records and provide alternate storage locations to provide readily available vital records under all conditions

The vital records and database risk assessment was performed by **ARMY PROGRAM PMO Risk Management** and is located **ARMY PROGRAM PMO Risk Management configuration management**.

Appropriate protections for vital records will be provided by **ARMY PROGRAM PMO Risk Management** and will include dispersing those records to other agency locations or storing those records offsite. Other protections include **multiple redundant media for storage**.

When determining and selecting protection methods, **ARMY PROGRAM PMO** takes into account the special protections needed by different kinds of storage media. Microforms, paper photographs, and computer disks, tapes, and drives, all require different methods of protection. Some of these media may also require equipment to facilitate access.

Training and Maintenance

The **ARMY PROGRAM** vital records program includes a training program conducted by **ARMY PROGRAM PMO Risk Management** for all staff, to include periodic briefings to managers about the vital records program and its relationship to their vital records and business needs. **ARMY PROGRAM** staff training focuses on identifying, inventorying, protecting, storing, accessing, and updating the vital records. Training records for vital records are maintained by **ARMY PROGRAM PMO Risk Management** and are found at **ARMY PROGRAM PMO Risk Management configuration management**.

ARMY PROGRAM vital records program includes an annual review of the program to address new security issues, identify problem areas, update information, and incorporate any additional vital records generated by new agency programs or functions or by organizational changes to existing programs or functions. The review is conducted by **ARMY PROGRAM PMO Risk Management**. The review provides an opportunity to familiarize staff with all aspects of the vital records program. It is appropriate to conduct a review of the vital records program in conjunction with **ARMY PROGRAM** continuity exercises. Documents confirming review of the vital records program are maintained by **ARMY PROGRAM PMO Risk Management** and are found at **ARMY PROGRAM PMO Risk Management configuration management**. At a minimum, **ARMY PROGRAM** vital records are annually reviewed, rotated, or cycled so that the latest versions will be available.

ARMY PROGRAM conducts annual testing, documented in **ARMY PROGRAM** testing records, of the capabilities for protecting classified and unclassified vital records and for providing access to them from the alternate facility. Testing records for vital records are maintained by **ARMY PROGRAM PMO Risk Management** and are found at **ARMY PROGRAM PMO Risk Management configuration management**.

Table 12: COOP Plan: Examples of Vital Files, Records, and Databases

Vital File, Record, or Database	Support to Essential Function	Form of Record (e.g. hardcopy, electronic)	Pre-positioned at Continuity Facility	Hand Carried to Continuity Facility	Multiple Storage Locations (Y/N)	Maintenance Frequency
GIS Mapping Database	Function #1	Electronic	X		Y	Monthly
MOAs with Customers	Function #2, #2, and #3	Electronic		X	Y	Annually
List of DISA DECC Key Personnel	Function #3	Electronic	X		N	Annually

III. Continuity Facilities

Continuity Facility Information

ARMY PROGRAM has designated continuity facilities as part of its continuity of operations plan and has prepared ERG personnel for the possibility of unannounced relocation to these sites to continue essential functions. **ARMY PROGRAM** completed and forwarded a Standard Form 336 for each facility to GSA, as applicable. A copy of the form is found **ARMY PROGRAM PMO Risk Management configuration management.** **ARMY PROGRAM** reevaluates its continuity facilities at least annually and whenever the continuity plans are reviewed and updated.

ARMY PROGRAM does maintain Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) and reviews the MOA/MOU annually, as applicable. An MOA/MOU is necessary because **ARMY PROGRAM** is **co-located with another agency**. A copy of the MOA/MOU is found **ARMY PROGRAM PMO Risk Management configuration management** and maintained by **ARMY PROGRAM PMO Risk Management**.

The **ARMY PROGRAM** primary continuity facility is located at **[REDACTED]**. A map of the surrounding area, including directions and route from the primary operating facility, is located **below**. Additional facility details are as follows:

1) This facility is **rented** by **ARMY PROGRAM**.

2) The site has security and on-site personnel support, but no extensive medical support.

3) **Security and access controls must exist to support classified data storage.**

4) Medical support is available within the metropolitan area.

The **ARMY PROGRAM** continuity facilities provide the following in sufficient quantities to sustain operations for up to 30 days or until normal business activities can be resumed:

(1) Sufficient space and equipment, including computer equipment and software. The continuity facility is able to accommodate **25** personnel. Facility floor plans, equipment inventory, and **other applicable documents** are found at **ARMY PROGRAM PMO Risk Management configuration management**.

(2) Capability to perform MEFs and PMEFs within 12 hours of plan activation or an event, respectively, for up to 30 days or until normal operations can be resumed.

(3) Reliable logistical support, services, and infrastructure systems. Details on these infrastructure systems are available at **ARMY PROGRAM PMO Risk Management configuration management** from **ARMY PROGRAM PMO Risk Management**.

(4) Consideration for health, safety, security, and emotional well-being of personnel. Considerations available at the alternate site include **physical security, access to the Employee Assistance Program, and presence of security**.

(5) Interoperable communications for effective interaction. Additional information on continuity communications is found **ARMY PROGRAM PMO Risk Management configuration management** in this plan.

(6) Capabilities to access and use vital records. Additional information on accessing vital records is found **ARMY PROGRAM PMO Risk Management configuration management** in this plan.

(7) Systems and configurations that are used in daily activities. IT support at the continuity facility is **provided by DISA DECC** Details on the systems and configurations are available at **ARMY PROGRAM PMO Risk Management configuration management** from **ARMY PROGRAM PMO Risk Management**.

(8) Emergency/back-up power capability. Details on the power capability are available at **ARMY PROGRAM PMO Risk Management configuration management** from **ARMY PROGRAM PMO Risk Management**.

Continuity Facility Logistics

ARMY PROGRAM continuity facilities maintain pre-positioned or detailed site preparation and activation plans in order to achieve full operational capability within 12 hours of notification. These site preparation and activation plans are **ARMY PROGRAM PMO Risk Management configuration management**.

ARMY PROGRAM maintains a transportation support plan that describes procedures for warning and no-warning events.

- During a no-warning event, advance team and ERG personnel are transported to the continuity facility via **rally points, means of notification, back-up transportation methods, and any other necessary information**.
- During a with warning event, advance team and ERG personnel are transported to the continuity facility via **rally points, means of notification, back-up transportation methods, and any other necessary information**.

ARMY PROGRAM has addressed the need for housing to support continuity personnel at or near the continuity facility sites by **on-site housing, and a list of nearby hotels**.

Continuity Facility Orientation

ARMY PROGRAM regularly familiarizes its ERG members with its continuity facilities. **ARMY PROGRAM** accomplishes this orientation through **deployment exercises, orientation sessions at the site, and briefings**. This familiarization training is reflected in organization training records located **ARMY PROGRAM PMO Risk Management configuration management**.

Further, **ARMY PROGRAM** annually trains and prepares its personnel for the possibility of an unannounced relocation to all continuity facilities. This training is reflected in organization training records located **ARMY PROGRAM PMO Risk Management configuration management**.

IV. Continuity Communications

ARMY PROGRAM has identified available and redundant critical communication systems that are located at the continuity facility. Further, **ARMY PROGRAM** maintains fully capable continuity communications that could support organization needs during all hazards, to include pandemic and other related emergencies, and give full consideration to supporting social distancing operations including telework and other virtual offices. These systems provide the ability to communicate within and outside the organization and are found **ARMY PROGRAM PMO Risk Management configuration management**.

Table 13: COOP Plan: Example Tracking Modes of Communication

Communication System	Support to Essential Function	Current Provider	Specification	Alternate Provider	Special Notes
Non-secure Phones	Yes	Various	[REDACTED]		Available at alternate site
Secure Phones	Yes	SIPR	[REDACTED]		Available at alternate site
Fax Lines	No	Phones			
Cellular Phones	Yes	Blackberry			
Pagers	Yes	Sprint			
E-mail	Yes	SIPR		NIPR	Both commercial and government email available
Internet Access	Yes	NIPR		SIPR	
GETS Cards	No				Available from shared pool

All **ARMY PROGRAM** necessary and required communications and IT capabilities must be operational as soon as possible following continuity activation, and in all cases, within 12 hours of continuity activation. **ARMY PROGRAM** has planned accordingly for essential functions that require uninterrupted communications and IT support, as detailed in the table below.

Table 14: COOP Plan: Uninterrupted IT Support

Organizations that:	If yes, the organization must:
Support a NEF	Possess, operate, and maintain, or have dedicated access communications capabilities, at their headquarters and alternate-facility locations, as well as mobile capabilities as required that ensure the continuation of those organizations' functions across the full spectrum of hazards, threats, and emergencies, including catastrophic attacks or disasters.
Do not support a NEF	Possess, operate, and maintain, or have dedicated access to communications capabilities at their headquarters and alternate-facility locations, as well as mobile capabilities, as required, that ensure the continuation of those organizations' essential functions.
Are designated as Category I	Coordinate with the Secretary of Homeland Security and the Secretary of Defense to obtain and operate secure

or II	and integrated continuity of government communications.
Share a continuity facility	Have a signed agreement that ensures that each one will have adequate access to communications resources.

ARMY PROGRAM possesses communications capabilities to support the organization's senior leadership while they are in transit to alternate facilities. These capabilities are maintained by **ARMY PROGRAM PMO Risk Management** and documentation regarding these communications capabilities is found **ARMY PROGRAM PMO Risk Management configuration management**.

ARMY PROGRAM satisfies the requirement to provide assured and priority access to communications resources, including **Telephone Service (GETS), Wireless Priority Service, and Telecommunications Service Priority**. The **ARMY PROGRAM** point-of-contact for these services is **ARMY PROGRAM Operations Officer**.

V. Leadership and Staff

A. ORDERS OF SUCCESSION

Pre-identifying orders of succession is critical to ensuring effective leadership during an emergency. In the event an incumbent is incapable or unavailable to fulfill essential duties, successors have been identified to ensure there is no lapse in essential decision making authority. **ARMY PROGRAM** has identified successors for the positions of **Commander and operations officer**. A copy of these orders of succession is found **ARMY PROGRAM PMO Risk Management configuration management**. **ARMY PROGRAM PMO Risk Management** is responsible for ensuring orders of succession are up-to-date. When changes occur, **ARMY PROGRAM PMO Risk Management** distributes the changes to **Program Management, Operations, and [OWNING PROGRAM]** by **encrypted and digitally-signed email**.

ARMY PROGRAM's orders of succession are:

- At least three positions deep, where possible, ensuring sufficient depth to ensure **ARMY PROGRAM**'s ability to manage and direct its essential functions and operations
- Include devolution counterparts, where applicable
- Geographically dispersed, where feasible
- Described by positions or titles, rather than by names of individuals holding those offices
- Reviewed by the organization's general counsel as changes occur
- Included as a vital record, with copies accessible and/or available at both the primary and continuity facilities at **DISA DECC facility**

In the event of a change in leadership status, **ARMY PROGRAM** must notify the successors, as well as internal and external stakeholders. In the event the **ARMY PROGRAM** leadership becomes unreachable or incapable of performing their authorized legal duties, roles, and responsibilities, **ARMY PROGRAM PMO** will initiate a notification of the next successor in line **via encrypted and digitally-signed email**. **ARMY PROGRAM PMO** will use the following procedures to notify internal and external stakeholders of the change in leadership: **via encrypted and digitally-signed email**.

ARMY PROGRAM training records document the conduct of annual successor training for all personnel who assume the authority and responsibility of the organization's leadership to include briefing successors to the position of **ARMY PROGRAM Commander** on their responsibilities and duties as a successor. Methods of successor training include **exercise training**. This training is reflected in **ARMY PROGRAM** training records located **ARMY PROGRAM PMO Risk Management configuration management**.

B. DELEGATIONS OF AUTHORITY

Generally, **ARMY PROGRAM** pre-determined delegations of authority will take effect when normal channels of direction are disrupted and terminate when these channels have resumed. Pre-determined delegations of authority may be particularly important in a devolution scenario.

ARMY PROGRAM has identified the following delegations of authority:

Orderly succession of officials to the position of **ARMY PROGRAM Commander** in the case of the **ARMY PROGRAM Commander**'s absence, a vacancy at that office, or the inability of the **ARMY PROGRAM Commander** to act during an emergency or national security emergency. The delegation of authority for **ARMY PROGRAM Commander** is found in a separate Annex file.

Succession of officials to the position of ARMY PROGRAM Operations Officer in the case of the ARMY PROGRAM Operations Officer's absence, a vacancy at that office, or the inability of the ARMY PROGRAM Operations Officer to act during an emergency or national security emergency. The delegation of authority for ARMY PROGRAM Operations Officer is found in a separate Annex file.

ARMY PROGRAM's delegations of authorities are found at the continuity facility and at **the primary operating facility** and:

(1) Are included as vital records

(2) Are written in accordance with applicable laws ensuring that the organization's PMEFs and MEFs are performed

(3) Outline explicitly in a statement the authority of an official to re-delegate functions and activities, as appropriate

(4) Delineate the limits of and any exceptions to the authority and accountability for officials

(5) Define the circumstances, to include a devolution situation if applicable, under which delegations of authorities would take effect and would be terminated

ARMY PROGRAM has informed those officials who might be expected to assume authorities during a continuity situation. Documentation that this has occurred is found **within ARMY PROGRAM PMO Risk Management** and at the continuity facility. Further, **ARMY PROGRAM** has trained those officials who might be expected to assume authorities during a continuity situation at least annually for all pre-delegated authorities for making policy determinations and all levels using **tests and exercises**. This training is reflected in agency training records located **within ARMY PROGRAM PMO Risk Management**.

C. HUMAN CAPITAL

Continuity Personnel

People are critical to the operations of any organization. Choosing the right people for an organization's staff is vitally important, and this is especially true in a crisis situation. Leaders are needed to set priorities and keep focus. During a continuity event, emergency employees and other special categories of employees will be activated by **ARMY PROGRAM** to perform assigned response duties. One of these categories is continuity personnel, commonly referred to as Emergency Relocation Group (ERG) members.

In respect to these continuity personnel, **ARMY PROGRAM** has:

- Identified and designated those positions and personnel they judge to be critical to organization operations in any given emergency situation as continuity personnel. A roster of these positions is maintained by **ARMY PROGRAM PMO Risk Management** and is found at **ARMY PROGRAM PMO Risk Management configuration management**
- Identified and documented its continuity personnel. These personnel possess the skill sets necessary to perform essential functions and supporting tasks. A roster of these personnel is maintained by **ARMY PROGRAM PMO Risk Management** and is found at **ARMY PROGRAM PMO Risk Management configuration management**
- Officially informed all continuity personnel of their roles or designations by providing documentation in the form of **electronic records and awareness training** to ensure that continuity personnel know and accept their roles and responsibilities. Copies of this documentation is maintained by **ARMY PROGRAM PMO Risk Management** and found at **ARMY PROGRAM PMO Risk Management configuration management**
- Ensured continuity personnel participate in their organization's continuity TT&E program, as reflected in training records. Training records are maintained by **ARMY PROGRAM PMO Operations Management** and found at **ARMY PROGRAM PMO Operations Management configuration management**
- Provided guidance to continuity personnel on individual preparedness measures they should take to ensure response to a continuity event using **computer-based training**. Copies of this guidance is maintained by **ARMY PROGRAM PMO Operations Management** and found at **ARMY PROGRAM PMO Operations Management configuration management**

All Staff

It is important that **ARMY PROGRAM** keep all staff, especially individuals not identified as continuity personnel, informed and accounted for during a continuity event. **ARMY PROGRAM** has established procedures for contacting and accounting for employees in the event of an emergency, including operating status.

- **ARMY PROGRAM** employees are expected to remain in contact with **supervisors** during any closure or relocation situation. **Employees use their personal cell phones or the ARMY PROGRAM secured Web site emergency checkin service to notify supervisors of their location and status.**
- **ARMY PROGRAM** ensures staff is aware of and familiar with human capital guidance in order to continue essential functions during an emergency. **ARMY PROGRAM** uses the following methods to increase awareness: **the ARMY PROGRAM secured Web site and regularly scheduled employee orientation briefing**.

Accounting for all personnel during a continuity event is of utmost importance. In order to account for all staff, **ARMY PROGRAM** will **call trees, an automated system, and a 1-800 number**. Accountability information is reported to **ARMY PROGRAM PMO Operations Officer** at **8** hour increments. **ARMY PROGRAM PMO Operations Officer** has the responsibility of attempting contact with those individuals who are unaccounted for.

An event that requires the activation of the Continuity Plan may personally affect **ARMY PROGRAM** staff. Therefore, the **ARMY PROGRAM PMO Operations Officer** has the responsibility to create provisions and procedures to assist all staff, especially those who are disaster victims, with special human capital concerns following a catastrophic disaster. These provisions and procedures are found at **ARMY PROGRAM PMO Risk Management configuration management**.

Human Capital Considerations

The **ARMY PROGRAM** continuity program, plans, and procedures incorporate existing agency-specific guidance and direction for human capital management, including guidance on pay, leave, work scheduling, benefits, telework, hiring, authorities, and flexibilities. The **ARMY PROGRAM PMO HR** has the responsibility for **ARMY PROGRAM** human capital issues. A copy of these policies and guidance is found **ARMY PROGRAM PMO HR configuration management**.

The **ARMY PROGRAM** Continuity Coordinator and Continuity Manager work closely with the **ARMY PROGRAM PMO HR** to resolve human capital issues related to a continuity event. **ARMY PROGRAM PMO HR** serves as the **ARMY PROGRAM** human capital liaison to work with the Continuity Coordinator or Continuity Manager when developing or updating the organization’s emergency plans.

ARMY PROGRAM has developed organization-specific guidance and direction for continuity personnel on human capital issues. This guidance is integrated with human capital procedures for its facility, geographic region, and the Office of Personnel Management (OPM) or similar organization. This guidance is maintained by **ARMY PROGRAM PMO HR** and found at **ARMY PROGRAM PMO HR configuration management**.

ARMY PROGRAM has issued continuity guidance for human capital on the following issues:

- Additional Staffing: **The ARMY PROGRAM Operations Officer is authorized to request temporary staff for previously identified COOP personnel positions as early as 4 hours after a COOP activation.**
- Work Schedules and Leave: **The ARMY PROGRAM Operations Officer has the authority to modify work schedules and to notify COOP personnel of additional duties and restrictions upon leave for the duration of the COOP activation as well as immediately following a COOP standdown.**
- Employee Assistance Program: **Maintained within the ARMY PROGRAM PMO HR configuration management**
- Special Needs Employees: **Maintained within the ARMY PROGRAM PMO HR configuration management**
- Telework: **The ARMY PROGRAM Operations Officer has the authority telework and remote access for previously identified COOP personnel at his/her discretion.**
- Benefits: **Maintained within the ARMY PROGRAM PMO HR configuration management**
- Premium and Annual Pay Limitations: **Maintained within the ARMY PROGRAM PMO HR configuration management**

Further, **ARMY PROGRAM PMO HR** communicates human capital guidance for emergencies (pay, leave, staffing, work scheduling, benefits, telework, hiring authorities and other human resources flexibilities) to managers in an effort to help continue essential functions during an emergency. The process for communicating this information is as follows: **encrypted and digitally-signed email or verified telephonic access.**

VI. Test, Training, and Exercises Program

ARMY PROGRAM maintains a robust TT&E program that complies with the DHS-mandated National Exercise Program, as appropriate.

ARMY PROGRAM provides organizational assistance to FEMA in conducting annual full-scale continuity exercises and biennial assessments of the organization's continuity program to support reports submitted to the NCC and the President or other applicable senior officials. Assistance includes **participation on a working group and providing controllers and/or evaluators**. Additional documentation of this assistance is found **within ARMY PROGRAM PMO Operations Management configuration management**.

ARMY PROGRAM performs TT&E events at regular intervals, in accordance with the requirements specified in FCD 1, throughout the year as depicted in the following table.

Table 15: COOP Plan: Continuity TT&E Requirements

Continuity TT&E Requirements	Monthly	Quarterly	Annually	As Required

Test and validate equipment to ensure internal and external interoperability and viability of communications systems	X			
Test alert, notification, and activation procedures for all continuity personnel		X		
Test capabilities to perform MEFs			X	
Test plans for recovering vital records, critical information systems, services, and data			X	
Test and exercise of required physical security capabilities at continuity facilities			X	
Test internal and external interdependencies with respect to performance of MEFs			X	
Train continuity personnel on roles and responsibilities			X	
Conduct continuity awareness briefings or orientation for the entire workforce			X	
Train organization’s leadership on PMEFs and MEFs			X	
Train personnel on all reconstitution plans and procedures			X	
Allow opportunity for continuity personnel to demonstrate familiarity with continuity plans and procedures and demonstrate organization’s capability to continue essential functions			X	
Conduct exercise that incorporates the deliberate and preplanned movement of continuity personnel to continuity facilities			X	
Conduct assessment of organization’s continuity TT&E programs and continuity plans and programs			X	
Report findings of all annual assessments as directed to FEMA			X	
Conduct successor training for all organization personnel who assume the authority and responsibility of the organization’s leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity situation			X	
Train on the identification, protection, and ready availability of electronic and hardcopy documents, references, records, information systems, and data management software and equipment needed to support essential functions during a continuity situation for all staff involved in the vital records program			X	

Test capabilities for protecting classified and unclassified vital records and for providing access to them from the continuity facility			X	
Train on an organization's devolution option for continuity, addressing how the organization will identify and conduct its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency			X	
Conduct personnel briefings on continuity plans that involve using or relocating to continuity facilities, existing facilities, or virtual offices				X
Allow opportunity to demonstrate intra- and interagency continuity communications capability				X
Allow opportunity to demonstrate that backup data and records required for supporting essential functions at continuity facilities are sufficient, complete, and current				X
Allow opportunity for continuity personnel to demonstrate their familiarity with the reconstitution procedures to transition from a continuity environment to normal activities				X
Allow opportunity for continuity personnel to demonstrate their familiarity with agency devolution procedures				X

ARMY PROGRAM formally documents and reports all conducted continuity TT&E events, including documenting the date of the TT&E event, the type of event, and names of participants. Documentation also includes test results, feedback forms, participant questionnaires, and any other documents resulting from the event. Continuity TT&E documentation for **ARMY PROGRAM** is managed by **ARMY PROGRAM PMO Operations Management** and is found **ARMY PROGRAM PMO Operations Management configuration management**. Further, **ARMY PROGRAM** conducts a comprehensive debriefing or hotwash after each exercise, which allows participants to identify systemic weaknesses in plans and procedures and to recommend revisions to organization's continuity plan. Documentation from TT&E hotwashes is found **ARMY PROGRAM PMO Operations Management configuration management**.

ARMY PROGRAM has developed a Corrective Action Program (CAP) to assist in documenting, prioritizing, and resourcing continuity issues identified during continuity TT&E activities, assessments, and emergency operations. The **ARMY PROGRAM** CAP incorporates evaluations, after-action reports, and lessons learned from a cycle of events into the development and implementation of its CAP. The **ARMY PROGRAM** CAP is maintained by **ARMY PROGRAM PMO Operations Management** and CAP documentation is found at **ARMY PROGRAM PMO Operations Management configuration management**. The **ARMY PROGRAM**'s continuity CAP:

1) Identifies continuity deficiencies and other areas requiring improvement

2) Provides responsibilities and a timeline for corrective action

3) Identifies program and other continuity funding requirements for submission to organization leadership and the Office of Management and Budget

4) Identifies and incorporates efficient acquisition processes and, where appropriate, collects all interagency requirements into one action

5) Identifies continuity personnel requirements for organization leadership and their supporting Human Resource Offices and OPM, where appropriate

Appendix B: Recommendations by Cost and Priority

The focus of this paper has been a complete COOP Plan reference implementation, using FEMA's federal template, and applied to a small Army Program use case. Space does not permit a complete COOP Plan development and implementation estimate; however, specific recommended aspects of a COOP Plan can be estimated. This section identifies five specific recommended aspects of a COOP Plan implementation and their relative costs and priority. Recommendations are taken from throughout this paper and are applied to the Army Program use case shown below:

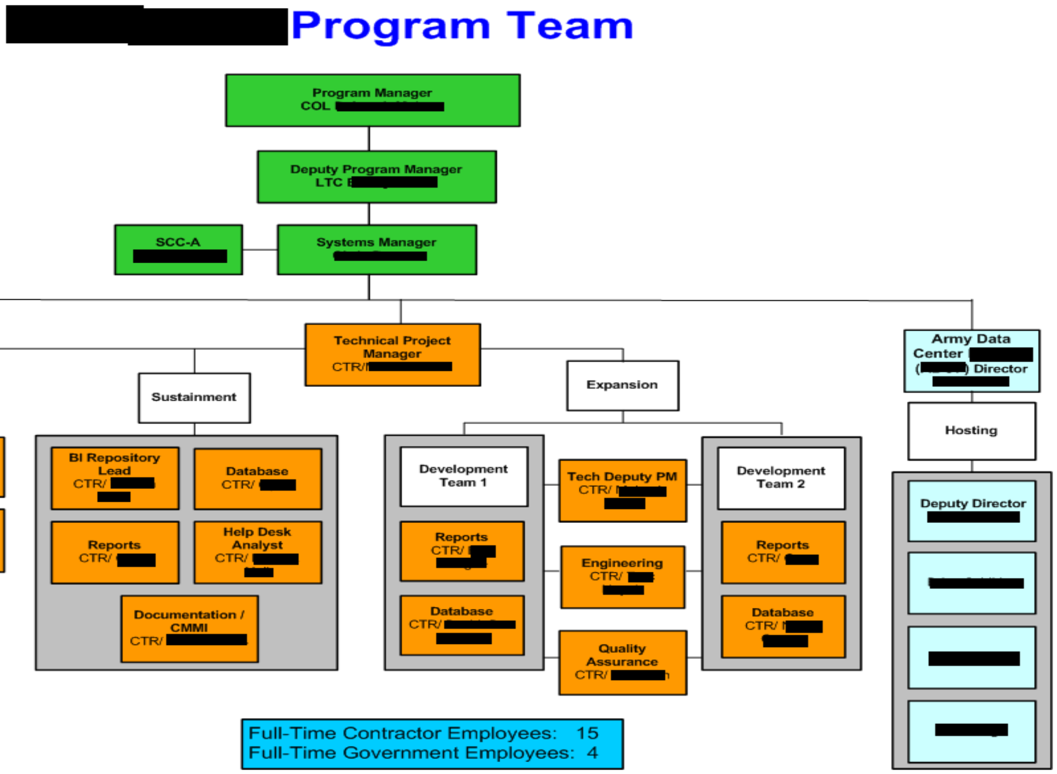

[redacted] Program Team
Program Manager COL [redacted]
Deputy Program Manager LTC [redacted]
SCC-A [redacted]
Systems Manager [redacted]
Prog Planning Manager CTR/ [redacted]
Program Planning
Prog Analyst CTR/ [redacted]
QA Tester CTR/ [redacted]
Functional Requirements
Functional Lead CTR/ [redacted]
Sr. Functional Analyst CTR/ [redacted]
Sustainment
BI Repository Lead CTR/ [redacted]
Database CTR/ [redacted]
Reports CTR/ [redacted]
Help Desk Analyst CTR/ [redacted]
Documentation / CMMI CTR/ [redacted]
Technical Project Manager CTR/ [redacted]
Expansion
Development Team 1
Reports CTR/ [redacted]
Database CTR/ [redacted]
Tech Deputy PM CTR/ [redacted]
Engineering CTR/ [redacted]
Quality Assurance CTR/ [redacted]
Development Team 2
Reports CTR/ [redacted]
Database CTR/ [redacted]
Army Data Center [redacted] ([redacted]) Director [redacted]
Hosting
Deputy Director [redacted]
[redacted]
[redacted]
[redacted]
Full-Time Contractor Employees: 15
Full-Time Government Employees: 4

Figure 4: Redacted Organizational Chart from an Army Program[41]

[41] Source: U.S. Army program documentation.

B.1: Summary

The following table shows the estimated costs for each recommendation made by the paper. Estimates should be considered as rough orders of magnitude with -50% to +150% being the possible range of actual implementation costs.

Table 16: Summary of Cost Estimates

Recommendation	Costs	Total Days
Reciprocal Agreements	$18,034	18
IT UPS	$7,148	1
BIA Implementation	$4,567	10
Fly-Away Kits / Family Preparedness	$4,130	9.5
Implement GETS	$3,694	7.5
Totals:	**$37,573**	**46**

These estimates, in conjunction with the other nine papers making up this series on COOP Plan implementation for a small Army Program use case, should provide the COOP practitioner of a sense for the cost involved in the various COOP implementation tasks.

B.2: Recommendations by Cost (Highest to Lowest)

Recommendations made by this paper have a cost and a priority associated with them; this section estimates those costs.

B.2.1 Reciprocal Agreements

Reciprocal agreements can be a low-cost way to help protect an organization during COOP activation. As an example, this paper looks at the Memorandum of Agreement (MOA) between FEMA and the American Red Cross (ARC).[42]

[42] See http://www.nvoad.org/resource-library/documents/doc_download/16-moa-red-cross-and-arc for this MOA.

Table 17: Reciprocal Agreement Estimates

			Costs		**Total Days**
Activity	**Detail**	**Roles**	*Calculation*	*Value*	
High Level Agreement	Create MOA	Executives	2 days x 2 x 463	$1,852	2
COOP Responsibilities	Define Mission Overlap (2 SMEs from each)	SMEs	7 days x 4 x 403	$11,284	7
Testing and Training	Create training material	Tech Editor	5 days x 192	$960	5
	Implement Training Plan (Director from each)	IT Ops Dir	3 days x 2 x 346	$2,076	3
	Perform tests (1 time per year, .25 days per person)	Staff	.25 x 38 * 196	$1,862	1
Totals:				**$18,034**	**18**

B.2.2 IT Contingency Plan Opportunities – UPS Costs

A key portion any COOP Plan is how well the organization has prepared for IT disasters; in fact, this paper posits that the heavy reliance by today's business environment on technology effectively means that COOP is considered to be primarily an IT Operations concern. While such a narrow focus on just the IT assets instead of the entire organizational infrastructure shortchanges true continuity (for example, how would new employees be brought onboard during a COOP activation?) it is certainly true that in the absence of a strong IT contingency plan even the best-laid continuity plan will quickly fail. This section estimates the cost to implement an uninterruptible power supply for the Army Program.

The estimates are based on the Army Program's use case of 8 rack-mounted Dell 2950 servers, 3 Dell PowerConnect 2224 switches, 1 Brocade Communications M4700 Fabric Switch, and 2 Buffalo Tera Station Pro II storage access network devices.

Table 18: IT UPS Estimates

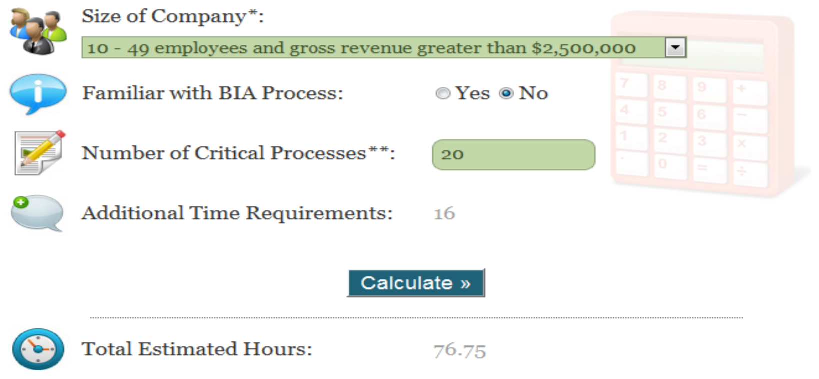
			Costs		**Total Days**
Activity	**Detail**	**Roles**	*Calculation*	*Value*	
UPS	Estimate from APC uninterruptible power supply to provide 20 minutes of run and 40% room for growth		Estimate	$6,904	0
	Installation	Config Mgmt Spec	1 day	$244	1
Fireproof safes	Estimate from *FireProofSafes.com* (July 27, 2011). QA0110 Waterproof Fire Chest Key Lock Fire Safe		Estimate (7 safes x $79.98)	$560	0
Totals:				**$7,708**	**1**

B.2.1 The Business Impact Analysis (BIA)

This paper has recommended the use of a Business Impact Analysis (BIA) as a critical component of any COOP Plan. The BIA allows the COOP practitioner to work with customers and stakeholders to identify the true cost of an outage throughout an organization. Moreover, the BIA allows hidden relationships between processes to be uncovered and to have appropriate risk reduction strategies applied to them.

The Continuity Compliance group has created a simple online calculator for determining the cost and effort associated with a BIA.[43] This calculator takes as input the number of people in the organization (19), the number of "critical processes" (these correspond to MEFs as defined by this paper, estimated at 20), and a qualitative assessment of the organization's familiarity with the BIA process (assessed as "low"). The results are shown to the side. The calculator provides a rough estimate only; the specific value returned of 76.75 hours can be used to get an idea of the time investment required in order for the BIA to be completed successfully.

Constructing an estimate from this raw number requires some additional estimates as shown below:



Size of Company*:
10 - 49 employees and gross revenue greater than $2,500,000

Familiar with BIA Process: ○ Yes ● No

Number of Critical Processes**: 20

Additional Time Requirements: 16

Total Estimated Hours: 76.75

Figure 5: BIA Calculator (Source: Continuity Compliance)

- 6 departmental groups (Program Leadership, Program Planning, Functional Requirements, Sustainment, Expansion, and Hosting.
- 2 interviews of 1 hour each for each department (two individuals chosen).
- 3 follow-up interviews with Management (1 hour each).
- Supplies cost of $100.

[43] See http://www.continuitycompliance.org/tools-resources/community-projects/business-impact-analysis (accessed: July 26, 2011).

Table 19: BIA Implementation Estimates[44]

Activity	Detail	Roles	Costs		Total Days
			Calculation	*Value*	
BIA Management		BC Pro	10 days x 403	$4030	10
Interviews	IT Workers	Avg InfoTech	1.5 days x 196	$294	0
	Management	IT Operations	2 hours x 43.25	$86	0
		IT Executive	1 hour x 57	$57	0
Supplies			Estimated	**$100**	**0**
Totals:				**$4,567**	**10**

B.2.4 Fly-Away Kits / Family Preparedness

Within FEMA's COOP Plan template, the concept of "Readiness and Preparedness" requires the federal organization "should plan in advance what to do in an emergency and should develop a Family Support Plan to increase personal and family preparedness" (p 13). This consists of having a "fly-away kit" as identified within DoD 3020.42 (the FEMA template calls this a "drive-away kit" but the meaning is identical); it also requires the organization to help employees verify that they and their families are ready for an emergency. From a COOP implementation view, this requires the investment of time and resources into overall employee preparedness.

Fly-away kits should contain those items that employees need both to accomplish their individual jobs as well as any personal items (such as known allergens, 30-day supply of prescription drugs, and so on).

These estimates and recommendations should provide a useful frame of reference to the COOP practitioner charged with implementing a COOP Plan in the context of a small, resource-starved, and fully-engaged organization. Such organizations need to have a COOP Plan of their own in order to complete their individual missions; federal, DoD, and Army policy all make this requirement quite clear. The challenge is for the COOP practitioner to achieve mission continuity despite the resource constraints that may exist. Only in this way can the federal government and the country as a whole have the assurance that the nation's business will be taken care of even in the event of a major disruption.

[44] Costs are expressed as units (days) multiplied by estimated salary. See Appendix "B.4: Selected Employee Costs" for salary estimates.

Table 20: Fly-Away Kit / Family Preparedness Estimates

			Costs		Total
Activity	**Detail**	**Roles**	*Calculation*	*Value*	**Days**
Orientation Training	Define policies	HR Director	1 day	$320	1
	Update training documents	Technical Editor	2 days x 192	$384	2
Ongoing Awareness	Include into BC plan	BC Pro	1 day	$403	1
	Update corporate intranet / define email	Web Developer	2 days x 196	$392	2
	Brown bag lunches / presentations (2x per year, 1 hour each)	All Staff	.25 * 19 * 196	$931	.25
		Mgmt / Presenters	1 day x 2 x 346	$692	2
Inclusion into Testing	Management Training	BC Pro	1 day	$403	1
		Mgmt	.25 days x 7 * 346	$605	.25
Totals:				**$4,130**	**9.5**

B.2.5 Implement GETS

In order to help ensure that communications during an emergency will be effective and available, the organization should include the capability of acquiring Government Emergency Telecommunications Service (GETS) cards for each of their critical staff. GETS is a service provided by the federal government (the National Communications System, or NCS, operating under the purview of the DHS).[45] From the Web site, this service offers "personnel a high probability of completion for their phone calls when normal calling methods are unsuccessful" and "is designed for periods of severe network congestion or disruption." GETS works by ensuring that subscribers receive priority when the call's virtual circuit is being created (thus, GETS has meaning only for switched telephone networks and not for dedicated lines which have a permanent point-to-point circuit). This priority is established by having the emergency personnel dial a reserved number and then entering an assigned 12-digit card number. Cellular service is provided by the Wireless Priority Service (WPS), which not all carriers support.[46]

The NCS does not charge a fee for the GETS service (except a nominal 7 or 10 cents per minute charge for each use). Thus, costs to implement the GETS fall into the planning and maintenance phases. NCS requires that organizations justify their need for GETS and that they maintain an

[45] See http://gets.ncs.gov/faq.html for more information on GETS (last accessed: July 27, 2011).

[46] The author's own company (Computer Sciences Corporation, http://www.csc.com/) worked with T-Mobile in 2003 to provide the first WPS service (http://tinyurl.com/csc-gets, accessed: July 27, 2011).

updated roster of those employees who have been issued a GETS card.

Table 21: GETS Implementation Estimates

Activity	Detail	Roles	Costs		Total Days
			Calculation	*Value*	
MOA	Create MOA and justification with NCS	Executives	1 day	$463	1
Establish POC	Define duties	BC Pro	1 day	$403	1
	Annual integration with GETS program (updates / deletes)	IT Ops Mgr	1 day	$346	1
Testing and Training	Create training material	BC Pro	1 day	$403	1
	Update materials	Tech Editor	2 days	$384	2
	Train users	InfoSec Officer (typical)	.5 days x 7 x 346	$1,211	.5
	Verify operations as part of COOP Plan testing	Mgmt	.1 days x 2 x 7 x 346	$484	1
Totals:				**$3,694**	**7.5**

B.3: Recommendations by Priority

This section prioritizes recommendations in the order that they should be implemented by the PMO.

Table 22: Recommendations by Priority

Item	Reasoning
Business Impact Analysis	This is the single most important element of a success COOP Plan. An organization cannot protect its vital functions and accomplish its mission unless it clearly understands what those functions are. Moreover, a BIA helps the organization to understand and address dependencies that it has on other agencies; in the federal government and DoD it is rare to find any organization that does not have at least one critical dependency. In the author's own case, the small Army Program use case depends entirely upon the local Network Enterprise Center (NEC); in the event of any emergency, the NEC's well-being is essential to the Army Program's capabilities.
Fly-Away Kits	Despite the fact that COOP policy at the federal, DoD, and Army levels all reiterate that the organization's ability to accomplish its primary mission overrides even human safety, no organization can be successful without ensuring that employees and their families are prepared for an emergency. "Fly-Away" kits are just one example of a low-cost and high-return investment that the

	program can make; employees are reminded that the organization cares about them personally and not simply as resources that can accomplish a job. Moreover, the ongoing awareness of such sites as *ready.gov* that drill into each person what responsibilities are entailed in preparing for emergency helps the organization to become one in which continuity concerns permeate the culture.
Implement GETS	This low-cost and high-reward investment requires only time and planning. GETS is a free service provided by the NCS and helps to ensure that critical response employees can communicate using the wired (and wireless) telephone grid.
IT Contingency	The suggested example of a UPS for the small Army Program use case depends upon whether the specific organization uses a hosting center with reliable backup generator power. Where sufficient backup power exists, the benefit of a UPS decreases. However, other IT Contingency preparation opportunities (such as fireproof safes) offer excellent value regardless of the hosting environment.
Reciprocal Agreements	The high price tag associated with this estimate assumes that there is tight integration between the two facilities and that a significant amount of SME time and expertise is used to ensure that, during an emergency, the facilities could truly be an alternate location for each other. The out-of-pocket cost of such reciprocal agreements tends to approach zero, which is why they are superficially so popular. Despite NIST's (and the federal government's) statements in favor of these agreements they are often castigated by practicing professionals because of their unenforceable nature and the fact that such agreements have a number of assumptions in them.[47] (Not least in these assumption is that the hardware and software within both organizations will remain compatible over time.)

These estimates and recommendations should provide a useful frame of reference to the COOP practitioner charged with implementing a COOP Plan in the context of a small, resource-starved, and fully-engaged organization. Such organizations need to have a COOP Plan of their own in order to complete their individual missions; federal, DoD, and Army policy all make this requirement quite clear. The challenge is for the COOP practitioner to achieve mission continuity despite the resource constraints that may exist. Only in this way can the federal government and the country as a whole have the assurance that the nation's business will be taken care of even in the event of a major disruption.

[47] Richard Snyder, 1999. "Reciprocal Agreements: Do They Work?" *DisasterRecoveryJournal*. http://www.drj.com/drworld/content/w1_095.htm (accessed: July 27, 2011).

B.4: Selected Employee Costs

The following table lists average salaries for selected roles. All values are rounded to the nearest whole number and averaged between the low and high values available from the data source. In order to provide the reader with a more complete reference this paper includes common roles in addition to the specific employee roles identified in the cost estimates above.

Table 23: Selected Employee Costs for a 2,000-person Company[48]

Position	Average Annual Salary	Average Daily Cost
Executive (CEO / CFO / COO / CIO)	$120,481	$463
Vice President (includes PMO, Chief Engineer, etc.)	$110,000	$423
IT Project Manager	$88,000	$338
Regulatory Compliance Manager (LRP Compliance)	$77,000	$296
Business Continuity Professional	$105,000	$403
HR Director	$84,000	$320
Facilities Manager	$62,000	$238
IT Operations Manager	$90,000	$346
Configuration Management Specialist (Config Mgmt Spec)	$64,000	$246
QA Engineer	$63,500	$244
Information Security Officer	$82,000	$315
Information Assurance Analyst	$68,000	$261
Technical Editor	$50,000	$192
Senior Software Engineer (typically Subject Matter Experts for all disciplines)	$105,000	$403
Business Analyst (Database)	$55,000	$211
Average Information Technology Worker (including average Web developer)	$51,000	$196

[48] Salary estimates come from http://www.payscale.com/research/US/ (accessed: May 14, 2011).

Appendix C: Acronyms and Abbreviations

Where an acronym has meaning in a specific context (for example, with regard to a specific NIST publication), that context is noted parenthetically.

AAR	After Action Review (COOP Plan)
AMC	Army Materiel Command
ARC	American Red Cross
BCM	Business Continuity Management
BCP	Business Continuity Planning
C2	Command and Control
CAP	Corrective Action Program
CECOM	U.S. Army Communications-Electronics Command
CFO	Chief Financial Officer
CHDS	Center for Homeland Defense and Security
COG	Continuity of Government
CONOPS	Concept of Operations
COOP	Continuity of Operations (federal term)
DCCM	Defense Continuity & Crisis Management
DCP	Defense Continuity Plan
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DoD	Department of Defense
ECG	Enduring Constitutional Government (federal COOP)
ERG	Emergency Response Group
FASP	Federal Agency Security Practices
FCD	Federal Continuity Directive
FedRAMP	Federal Risk and Authorization Management Program
FPC	Federal Preparedness Circular
FPCON	DoD Force Protection Condition
FOC	FEMA Operations Center
GETS	Government Emergency Telecommunications Service

GSA	General Services Agency
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
MEF	Mission Essential Function (federal COOP)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCPIP	National Continuity Policy Implementation Plan
NCS	National Communications System
NEC	Network Enterprise Center
NEF	National Essential Function (preserves ECG)
NIST	National Institute of Standards and Technology
NSPD	National Security and Presidential Directive
OMB	Office of Management and Budget
PMEF	Primary Mission Essential Function (supports a NEF)
PMO	Program Management Office
POR	Program of Record
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SES	Senior Executive Staff
SLA	Service Level Agreement
TT&E	Test, Training, and Exercise (COOP Plan)
U.S.	United States
UPS	Uninterruptible Power Supply
USD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
WPS	Wireless Priority Service

About the Author

Andrew Bruce is a Cloud Architect for D&SCI in the Army Programs group out of Aberdeen Proving Ground, MD. D&SCI provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that enable tight integration to the Army's datacenter consolidation and cloud virtualization enterprise portfolio initiatives. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing Army customers' network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning three decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers. Mr. Bruce holds the CISSP, PMP, and FITSP-D certifications as well as a Master's Degree in Information Assurance from Norwich University.

Reference List

The following references contributed authoritatively to this paper.

[AR500-3] DA. April 18, 2008. Army Regulation 500-3: U.S. Army Continuity of Operations Program Policy and Planning. <http://www.fas.org/irp/doddir/army/ar500-3.pdf>. Accessed: June 12, 2011. 39 p.

[BS25999] BSI. November, 2006. Business Continuity Management: Part 1: Code of Practice. London. 50 p.

[DOD-3020.26] Department of Defense. January 9, 2009. DoDD 3020.26: Department of Defense Continuity Programs. <http://www.dtic.mil/whs/directives/corres/pdf/302026p.pdf>. Accessed: June 15, 2011. 10 p.

[DOD-3020.42] Department of Defense. February 17, 2006 (Certified current as of April 27, 2011). DODI 3020.42: Defense Continuity Plan Development. <http://www.dtic.mil/whs/directives/corres/pdf/302042p.pdf>. Accessed: June 21, 2011. 11 p.

[FALTUM] Faltum, A. January 9, 2009. A National Information Policy (Finalist: 2nd Annual CHDS Essay Competition). <http://www.chds.us/?media/openmedia&id=2167>. Accessed: July 18, 2011. 6 p.

[FCD-2] DHS. February, 2008. FCD 2: Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process. <http://www.fema.gov/pdf/about/offices/fcd2.pdf>. Accessed: July 18, 2011. 33 p.

[FEMA-COOP]. FEMA. March 25, 2011. Continuity of Operations Plan Template and Instructions for Federal Departments and Agencies. <http://www.fema.gov/pdf/about/org/ncp/coop/continuity_plan_federal_d_a.pdf>. Accessed: July 25, 2011. 62 p.

[FM5-19] Headquarters, Department of the Army. August, 2006. FM 5-19: Composite Risk Management. <https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fm5_19.pdf> (requires AKO login). Accessed: June 25, 2011. 108 p.

[FPC-65] Federal Emergency Management Agency. June 15, 2004. FPC 65: Federal Executive Branch Continuity of Operations (COOP). <http://www.fema.gov/pdf/library/fpc65_0604.pdf>. Accessed: June 25, 2011. 50 p.

[NIST-CONT] NIST. 2011. NIST Contingency Plan Template. <http://csrc.nist.gov/groups/SMA/fasp/documents/contingency_planning/contingencyplan-template.doc>. Accessed: July 25, 2011. 70 p.

[NSPD51] Bush, GW. May 9, 2007. National Security and Homeland Security Presidential Directive (NSPD 51 / HSPD-20): National Continuity Policy. White House: Office of the Press Secretary. 6 p.

[SP800-34] NIST. May 2010. SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>. Accessed: June 21, 2011. 149 p.

[PAM25-1-2] DA. November 16, 2006. Pamphlet 25-1-2: Information Technology Contingency Planning. <http://www.apd.army.mil/pdffiles/p25_1_1.pdf>. Accessed: July 6, 2011. 155 p.

Miscellaneous References

The following references contributed indirectly to this paper or provide additional information for the interested reader.

Acohido B. “New cyberattacks target small businesses,” USATODAY.com, July 4, 2011. http://www.usatoday.com/tech/news/2011-07-04-small-business-cyber-attackss_n.htm (accessed: July 14, 2011).

Corrin A, January 6, 2011. “Gates details DOD budget cuts, consolidations,” defensesystems. http://defensesystems.com/articles/2011/01/06/gates-updates-dod-budgetary-measures.aspx (accessed: July 18, 2011).

Corrin A, March 11, 2011. “Fight brewing over DOD budget cut,” defensesystems. http://defensesystems.com/articles/2011/03/14/homepage-defense-fiscal-2012-budget-cuts.aspx (accessed: July 18, 2011).

DeccanHeral. “Al-Qaeda and terror groups planning attack on US facilities,” February 13, 2011. http://www.deccanherald.com/content/52422/al-qaeda-terror-groups-planning.html (accessed: July 14, 2011).

FEMA COOP Plan Templates. http://www.fema.gov/about/org/ncp/coop/templates.shtm. Accessed: July 25, 2011.

FEMA Disasters. http://www.fema.gov/news/disasters.fema. Accessed: July 25, 2011.

GETS Frequently Asked Questions Page. http://gets.ncs.gov/faq.html. Accessed: July 27, 2011.

Giffin R, November 1, 2009. “Why is DRI Speaking Out Against Organizational Certification?” DisasterRecoveryJournal, http://www.drj.com/view-by-tag/bs-25999/ (accessed: July 19, 2011).

GSA Web Site for COOP Services. http://www.gsa.gov/portal/content/101727. Accessed: July 25, 2011.

Llanos M. “2011 already costliest year for natural disasters,” today.msnbc.msn.com, July 12, 2011. http://today.msnbc.msn.com/id/43727793/ns/world_news-world_environment/ (accessed: July 14, 2011).

Snyder R. 1999. “Reciprocal Agreements: Do They Work?” DisasterRecoveryJournal.

http://www.drj.com/drworld/content/w1_095.htm (accessed: July 27, 2011).

Thom G. “Sony restarts internet services weeks after hacking debacle,” Herald Sun, May 15, 2011. http://tinyurl.com/sony-debacle (accessed: July 14, 2011). Sony was down for 22 days in 2011 from April 21 to May 15.

Voigt K. “Analysis: The hidden cost of cybercrime,” CNN, June 7, 2011. http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html (accessed: July 14, 2011).