Continuity of Operations within DoD

Part 1 of 10 – Define the Landscape

Topic Summary:

- Continuity of Operations (COOP) defined within DoD and compared to commercial industry
- DoD and Army policy shaping COOP
- Challenges and Opportunities for COOP within a small Army program
- Summary and Recommendations for next steps

Andrew Bruce

Coop in DoD - Part 01 of 10.doc

Table of Contents

1.0 Introduction 1
2.0 DoD and Army COOP Policy 1
2.1 Federal Level: HSPD-20 1
2.2 DoD Level: DoDD 3020.26 2
2.3 Army Level: AR300-5 3
2.4 COOP Comparison: Military and Commercial 3
3.0 Organizational Analysis 4
3.1 Areas that Support a COOP Program 4
3.1.1 Management Requirements 4
3.1.2 IT Infrastructure 5
3.1.3 Certification and Accreditation (C&A) 6
3.2 Areas that Challenge a COOP Program 7
3.2.1 Budget Issues 7
3.2.2 Cost-Based Contracting 7
3.2.3 Workload 8
4.0 Concluding Remarks 8
4.1 Summary 8
4.2 Recommendations 9
4.3 Next Steps 9
Appendix A: Acronyms and Abbreviations 10
Reference List 11

Illustration Index

Figure 1: DIACAP Lifecycle 6

Table Index

Table 1: Recommendations 9

1.0 Introduction

The Department of Defense (DoD) and the federal government recognize the value of ensuring continuity of government (COG) for all operations deemed critical to the health of the nation. However, this emphasis on protecting only the “most critical” systems can detract from the resiliency of smaller operations. The “iron triangle” of project scope, cost, and schedule can prove difficult enough to work under during the best times as an organization works to accomplish its mission; adding the expense of maintaining resiliency when things go massively wrong can sometimes be seen as a misdirection of scarce resources.

This paper, the first in a ten-part series, analyzes how a full Continuity of Operations (COOP) program can be implemented for a small, non-mission-critical Army program operating under tight budgetary and personnel constraints. This paper begins by understanding the policy guidelines that drive the larger organization and the Army program. It then analyzes the program to determine what areas either hinder or support the establishment of a COOP program. The paper then closes by providing recommendations on how some possible COOP program implementation problems can, as well as the steps to be addressed in the next paper.

2.0 DoD and Army COOP Policy

An organization must have a method for ensuring its ability to accomplish its mission even in the face of unexpected and highly-destructive events. In the commercial world, this methodology (both planning and implementation) is called Business Continuity Management (BCM); it includes both the ability to continue executing critical business functions (“business continuity”) as well as the ability to restore normal business activity (“disaster recovery,” or DR). The federal government and DoD use the term “Continuity of Operations” or *COOP* to refer to both these functions (business continuity and disaster recovery).

This section analyzes policy drivers that affect COOP within the DoD and the Army, as well as the differences between military and commercial environments.

2.1 Federal Level: HSPD-20

The DoD (to include the four uniformed services) operates within the Executive branch; the President as Commander-in-Chief drives policy and authorizes regulatory requirements affecting it. In May, 2007, then-President Bush authorized a National Security and Homeland Security Presidential Directive that “establishes a comprehensive national policy on the continuity of Federal Government structures and operations” (HSPD-20, p 1). This directive established the Secretary of Homeland Security is listed as “the President’s lead agent” in the implementation of a “Continuity of Government” (COG) strategy that seeks to identify and protect “National Essential Functions” (NEFs) that, among other things:[1]

1. Ensures the continuing effective function of our constitutional form of government.
2. Provides visible leadership to, and maintains the confidence of, the nation and the world.
3. Defends our Constitution against all enemies, foreign and domestic.

[1] Paraphrased from the NCPIP, p 7.

4. Provides rapid and effective response to, and recovery from, an attack or other national incident.
5. Protects the national economy and maintains confidence in the nation's financial system.

This Directive quickly led to the creation of the National Continuity Policy Implementation Plan (NCPIP), which provided guidance for the Executive branch to follow.[2] The DoD is primarily responsible for the "operational" aspect of COG; it must maintain "secure, integrated, Continuity of Government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies." (NCPIP, p 94).

2.2 DoD Level: DoDD 3020.26

In the event of a national emergency, the DoD must maintain that the critical communications infrastructure underlying COG.[3] The Secretary of Defense established Under Secretary of Defense for Policy, or "USD(P)," as the policy creation arm for establishing a COOP program. The USD(P) created DoD Directive (DoDD) 3020.26 ("Department of Defense Continuity Programs") to articulate this policy. Within the Directive, only Mission Essential Functions (MEFs)[4] must provide a COOP program; each program must have the following key characteristics:[5]

1. Assume that no warning of attack or event will be received.
2. Ensure MEF performance until normal operations can be resumed, with no more than a 12 hour delay in any required alternate site operation after a COOP activation.
3. Provide risk-management assessments which consider the probability of an attack or incident and its consequences.
4. Maximize the use of interoperable and robust technological solutions to enable leadership to maintain situational awareness during COOP activation.
5. Integrate critical infrastructure protection, information assurance (IA), and operational security, and crisis management requirements across all DoD "Components."[6]

[2] One interesting side note on the NCPIP: The Executive branch, as a co-equal element of our constitutional government, does not have the power to enforce policy on the Legislative or Judicial branches. Instead, the Executive branch issued HSPD-20 and provided it to the other two government branches as a resource only; Congress and the Supreme Court were responsible for creating their own continuity plans.

[3] This includes, for example, the maintenance of secure locations (like the Raven Rock Mountain Complex) capable of allowing all three branches of the federal government to continue to function and to assemble as a quorum.

[4] An MEF supports one or more NEFs; in the words of the Directive, those functions whose failure would "significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control" (DODD-3020, p 2).

[5] Paraphrased from the Directive, p 2-3.

[6] A DoD "Component" refers to the Office of the Secretary of Defense, the Military Departments (uniformed services), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (DODD-3020, p 1).

Finally, each COOP program within DoD must be "exercised" (tested and verified for operational effectiveness) at least annually.

2.3 Army Level: AR300-5

As a DoD Component, the U.S. Army was tasked with developing its own COOP program and ensuring that it could support COG requirements. In April, 2008, the Army released the Army Regulation (AR) 500-3 ("U.S. Army Continuity of Operations Program Policy and Planning") to ensure conformity to DoDD 3020.26 and to apply to Army, Army National Guard, Army Commands and Component Commands, Direct Reporting Units, field operating agencies, and Army-owned / Army-Managed installations and garrisons. This Regulation explicitly ties itself to higher-level Executive branch guidance (including, for example, Federal Emergency Management Agency or "FEMA" guidelines). Within the Army, a MEF is primarily defined as a function that affects Command, Control, Communications, Computers, and Intelligence (C4I), especially those functions that affect or support operational troop activities. Specifically, each COOP program must:[7]

1. Establish primary points-of-contact (POCs) for individual COOP plans.
2. Identify and prioritize MEFs.
3. Identify, train, and maintain an updated roster of all Emergency Relocation Group (ERG) personnel.
4. Conduct test upon and assess the effectiveness of the COOP program at least annually.
5. Update the COOP program at least every *two* years.
6. Integrate the COOP program with other agencies at the same level, especially to ensure that MEFs are fully supported (dependency analysis).

2.4 COOP Comparison: Military and Commercial

Within the DoD and the Army, a COOP program emphasizes the continuity of government functions and the maintenance of a resilient command and control structure. Within the commercial world, a BCM program concerns itself primarily with the ability of the organization to continue executing its business functions in the face of severe disasters.

The military and commercial approaches to continuity management have strong similarities, just a few of which include:

- *Maintain operations in an uncertain threat landscape.* Disasters can occur without warning; floods, fires, and terrorists affect both military and commercial targets. Processes must exist to identify when a significant incident has occurred (such as "any critical network outage lasting more than 75 minutes shall activate the continuity plan"), and resources must exist to enable people to continue performing their jobs.
- *Understand business interdependencies.* Both military and commercial organizations must have a detailed map of how different internal functions interrelate (for example, facilities management and personnel availability). Furthermore, external dependencies must also be defined; consider incoming supply chains or created customer deliverables.

[7] Paraphrased from the Regulation, p 7-8.

- *Plan for business resumption.* Once a disaster (or any significant incident) has occurred, the organization must be prepared to resume operations based upon an objective plan. This plan must include milestones (such as “primary facility is declared safe for occupancy by local municipal authority”) and timelines (such as “restoration of critical hardware support to the primary facility shall occur no later than 3 days after the designated project manager has declared the facility to be fully restored”).

Despite these similarities, some obvious continuity differences exist:

- *Focus upon revenue generation*. In the commercial world, the organization must be capable of generating revenue to survive. While an effective BCM plan includes financial reserves to cover emergency operations, these can go only so far. The BCM plan must be built around ensuring a revenue stream. Within the military, the focus is different; the COOP program emphasizes accomplishing the mission (albeit in a cost-effective way).
- *Scope of Recovery.* In the commercial world, the fact that a competitor across town failed during a crisis may actually be cause for considerable rejoicing. Furthermore, for a multinational corporation, the fact that a particular city was impacted by a disaster is perhaps of less practical importance to senior management than whether the organization has the ability to shift operations nimbly to another geographic location. In the military, the emphasis on the continuity of *all* government means that this is not the case (except, perhaps, in the case of organizations run by hostile foreign agents). Rather, the military must be intimately concerned with the survival even of rival organizations (the Central Intelligence Agency as opposed to the Defense Intelligence Agency comes to mind). Because the military is charged with defending the citizens of the nation, DoD and the Army must include local jurisdictions in their COOP program.

As this paper looks at the difficulties and opportunities in setting up a COOP program for a small Army program, these similarities and differences must be kept in mind.

3.0 Organizational Analysis

Within the scope of a small Army program, problems and opportunities abound for a COOP program. In the Army program used as this case study, there is no doubt that both the government and the contractor see the need for and would welcome a full COOP program implementation. The question becomes one only of practicality.

3.1 Areas that Support a COOP Program

Three distinct areas support the implementation of a COOP program within the Army program: the management requirements (local administrative), the Information Technology (IT) Infrastructure requirements (operations), and the Certification and Accreditation (C&A) requirements.

3.1.1 Management Requirements

When the Army program was established, the Performance Work Statement (PWS) establishing the program’s scope identified the following key management provisions required for the executing contractor to conform to the program’s requirements. While each PWS is unique (as is each Army program, large or small), the wording used within this PWS is typical of those found within many Army projects (emphasis added):[8]

- “Provide task order management support…[to include]… quality control/**risk mitigation**.”
- “Contractor personnel…shall comply with all **applicable government security regulations and procedures** contained in AR 25-2, DODI 8500-2, Information Assurance & DoD 5220.22M – NISP” (*see sidebar “IA Within DoD and the Army”*).
- “the contractor shall provide Program Management, Systems Engineering, **Information Assurance**, Business Process Engineering, Biometrics Integration, SOA/ERP/Business Intelligence, Cloud Computing, Enterprise Resource Planning, Service Oriented Architectures, Virtualization, Software Requirements Engineering, Software Design, full lifecycle Software Development/Management, Software/Systems Testing, Software Maintenance, Configuration Management, Software Engineering Management, Systems Modeling, Network Infrastructure Assistance, Business Intelligence, Enterprise Data Management, Enterprise Data Warehousing, emerging technologies and […] development and maintenance.”
- Furthermore, the PWS requires the contractor to demonstrate “Information Assurance experience – policy/guidelines and writing/maintaining Information Assurance/SSAA documents, **working with DIACAP policies and guidelines**”[9]

Sidebar: IA Within DoD and the Army

AR 25-2 is the Army’s “Information Assurance” manual, and requires COOP as a defined aspect of an information system’s IA. DODI 8500-2 refers to DoD’s “Information Assurance (IA) Implementation” Instruction (correctly referred to as “DoDI 8500.2”), and defines COOP as an element of required IA control PRTN-1 (“Information Assurance Training”). DoD 5220.22M (NISP) refers to DoD’s “National Industrial Security Program” Manual and primarily relates to the handling of secure classified information and its protection from foreign adversaries; Section 8-202 within this Manual requires COOP as part of an automated information system’s security posture.

As can be seen, the management aspect of the Army program encourages the implementation of a COOP program to demonstrate compliance to the named Army and DoD IA references.

3.1.2 IT Infrastructure

The Army program’s IT infrastructure must be capable of supporting a “cloud” environment featuring IT service-delivery to a dispersed and mobile audience. The “cloud” aspect means that the program provides shared hosting services for a number of Army and DoD customers, and these customers have each negotiated both Memorandums of Agreement (MOAs) and Service Level Agreements (SLAs) with the Army program. As a fee-for-service organization, the Army program charges its customers based on hosting costs (for data Providers) and pay-per-usage access costs (for data Consumers). While this “payment” differs from in the commercial world in that no actual money is exchanged, it bears similarities to the IT Infrastructure Library (ITIL) notion of “shared service provider,” or an intra-organizational group that supports the IT service provider in their delivery of services (ITILv3, p 66).

[8] Source: PWS from Reference List, May 24, 2011.

[9] SSAA refers to “System Security Authorization Agreement,” the document written for delivery to a Designated Accrediting Authority (DAA) to allow an information system to be operated within a military network.

As a sound business practice, the Army program must be concerned with its customers' level of availability and utility to the set of provided IT services. A COOP program adds to this assurance by ensuring that a level of resilience exists so that unexpected failures can be handled gracefully and without a failure of service to customers.

3.1.3 Certification and Accreditation (C&A)

From Section 3.1.1, the reference to the DoD Information Assurance Certification and Accreditation Process (DIACAP) is perhaps the most germane. The DIACAP document (DoD Instruction 8510.01) requires that the Army program shall be compliant to all required IA controls as defined within AR 25-2, DoD 8500.2, and other IA documents. This compliance is demonstrated by the program's delivered information systems following the DIACAP lifecycle as shown below.

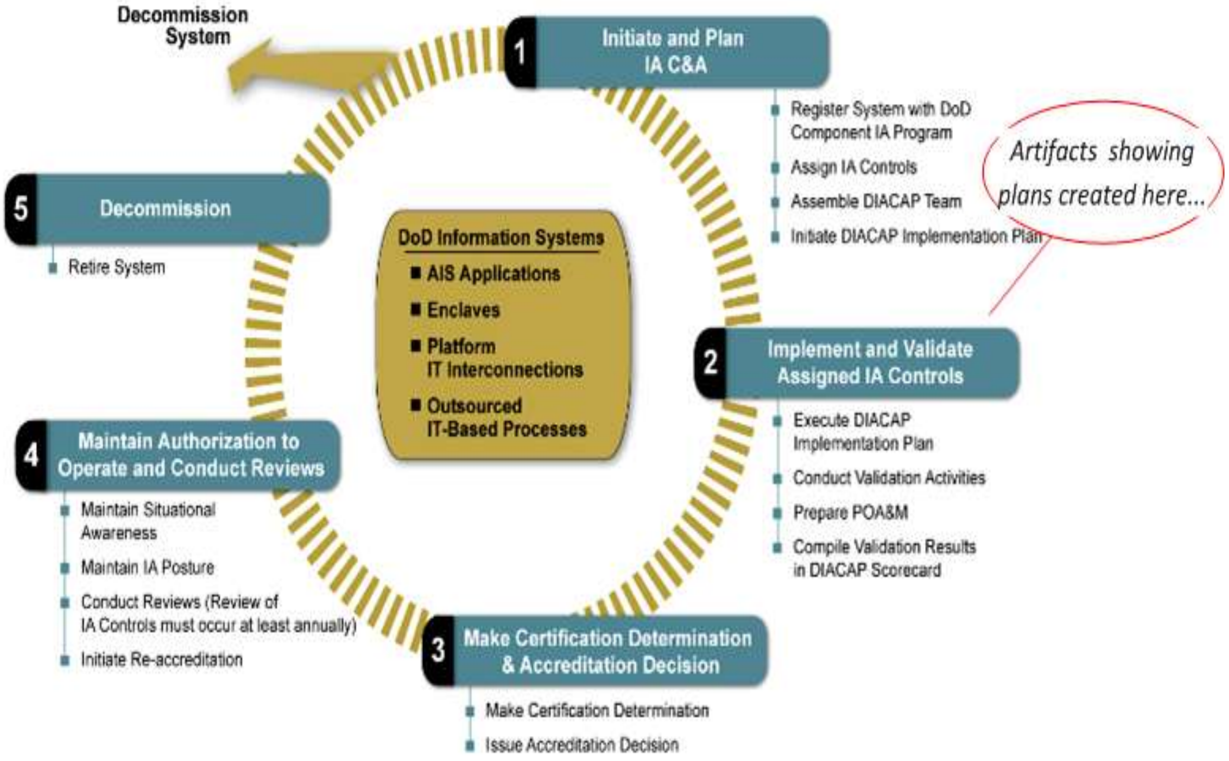
Decommission System
1 Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
Artifacts showing plans created here...
5 Decommission
Retire System
DoD Information Systems
AIS Applications
Enclaves
Platform IT Interconnections
Outsourced IT-Based Processes
2 Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Prepare POA&M
Compile Validation Results in DIACAP Scorecard
4 Maintain Authorization to Operate and Conduct Reviews
Maintain Situational Awareness
Maintain IA Posture
Conduct Reviews (Review of IA Controls must occur at least annually)
Initiate Re-accreditation
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision

Figure 1: DIACAP Lifecycle[10]

DIACAP requires that IT systems must be capable of operating in a resilient manner, which certainly supports the implementation of a COOP program within this small Army program.

[10] Source: DIACAP Knowledge Service (CAC required). https://diacap.iaportal.navy.mil/ks/ImplementationGuidance/Activities/Pages/default.aspx (accessed: June 12, 2011).

3.2 Areas that Challenge a COOP Program

The selected small Army program has a number of challenges facing it in any COOP program implementation. These challenges can best be thought of as budget-related, contractual-related, and workload related. As the contractor's project manager for the Army program under analysis reported to the author, "[t]he funding will definitely be a challenge. [The Program Manager] doesn't have the funding to execute a lot of it… there may be an opportunity to pitch a "reasonably-priced" plan. [The Program Manager]…is going to have to address COOP in some way to ensure his customers have a level of comfort that their data won't be lost if something happens."[11]

3.2.1 Budget Issues

The current federal monetary issues are rippling throughout DoD, as each program is asked to accomplish the same functions (or more) with the same (or smaller) allocated budget. Added to this is the fact that, from the policy level, COOP programs target primarily mission *essential* functions (MEFs); while the selected small Army program is essential to its customers, program management may find it difficult to defend extensive allocation of funds to establish the level of availability and utility that the program's customers demand.

One solution to this problem is for the PMO to look at the COOP program using a recommendation by the Institute for Business and Home Safety (IBHS). Rather than looking at COOP as an all-or-nothing effort, the PMO can start by breaking down the effort into much smaller (and easier to fund) parts. For example, beginning with an informal self-assessment can help to identify the major business processes and interdependencies with a minimal cost (IBHS, p 8).

3.2.2 Cost-Based Contracting

One major obstacle to overcome in establishing a COOP program is to determine just *how* such a program can be funded. Even assuming that funds are available, this particular Army program is using a Cost-Plus-Fixed-Fee (CPFF) structure; this structure offers the contractor only a fixed dollar amount based on the number of hours actually used compared to the hours budgeted when the contractor's proposal was accepted. While the actual cost of items can be increased, this can occur only if the Program Management Office (PMO) can receive approval from the relevant Army contracting officer. For the COOP program to be approved the PMO must allocate hours for a formal Trade Study (or Analysis of Alternatives); then, the contractor must create this study and propose an end-to-end solution. The Trade Study may or may not be funded within the scope of the current contract, which exposes the contractor to risk of unreimbursed cost (a full COOP could be quite expensive even to model).

One solution to this cart-before-the-horse situation is for the contractor to view a COOP study not as a contract expense, but as a value-add to help differentiate it for future awards. Defense contractors already invest a significant amount of time and money into winning new work; writing proposals is a time-consuming and resource-intensive task. Fully understanding the alternatives available for a COOP program helps the contractor understand its government customer better, while also providing it with ready-made tools and techniques for implementing the program in a production environment.

[11] Source: Personal interview with the contractor's project manager, June 8, 2011.

3.2.3 Workload

Another significant issue in establishing a COOP program is how to execute on the work. From a contract standpoint, it may not be possible to negotiate additional specialized labor categories in the awarded contract. Thus, the work may need to be completed with existing resources (or with workers having only contract-defined IA and business analysis skills). Thus, the added workload of implementing and maintaining a COOP program could jeopardize the Army program's ability to accomplish its primary mission. To make matters worse, the National Journal identifies skilled cyber specialists as being in short supply, thus adding to budget and labor pressures on both the government and the contractor.[12]

A possible solution to this dilemma is for the contractor to work with the government to allow more-qualified personnel on the contract. Normally, the government customer is quite happy to accept over-qualified resources onto a program presuming that the contractor can show there is no corresponding risk of losing these resources abruptly (for example, to a better job opportunity). The contractor can fund these positions by taking a lower margin (essentially, donating some profit to the government). This "donation" is by means one-sided in its benefit; the contractor helps to grow a COOP program implementation practice that, over time, can be an institutional capability to generate additional work and to differentiate the contractor from its competitors.

4.0 Concluding Remarks

4.1 Summary

This paper has reviewed COOP within DoD and the Army, specifically as it applies to a small Army program of record. The federal government realizes the value of a COOP program, as shown by HSPD-20, DoDD 3020.26, AR300-5, and the numerous IA publications that refer to the importance of implementing COOP to ensure continuity of government. Furthermore, even within a small Army program one finds the active interest within program management (government) and project management (contractor) to implement an effective COOP program.

However, DoD's focus on prioritizing COOP for "mission-essential" functions (MEFs) that are critical to ensure the continuity of the nation's constitutional form of government can serve to deemphasize the need for *all* programs to have an appropriate COOP level. Added to this difficulty is the need for programs to operate within an increasingly-constrained budgetary environment where funds may simply not be available from Congress. Furthermore, a negotiated contract may be quite difficult to work with when establishing a COOP program for the simple reason that additional labor categories and required up-front work (such as Trade Studies or Analysis of Alternatives) may not be capable of funding based on the contract's current wording. Finally, the age-old problem of too-much-work-for-too-few-people applies here; the documented shortage of highly-skilled IT assurance personnel can translate into difficulty in filling COOP program positions.

[12] Aliya Sternstein, "Shortage of Skilled Cyber Specialists Fuels Debate Over Pay," *NationalJournal*, April 19, 2011. Available at http://www.nationaljournal.com/nationalsecurity/shortage-of-skilled-cyber-specialists-fuels-debate-over-pay-20110419 (accessed: June 12, 2011).

4.2 Recommendations

This paper has recommended several approaches to resolve the problems in setting up a COOP program as shown in the table below:

Table 1: Recommendations

Recommendation	Affects Whom?	Rationale
Decompose the Problem	Government	Rather than looking at COOP as an all-or-nothing effort, the PMO can start by breaking down the effort into much smaller (and easier to fund) parts. For example, beginning with an informal self-assessment can help to identify the major business processes and interdependencies with a minimal cost.
COOP Trade Study as Value-Add	Contractor	Defense contractors already invest a significant amount of time and money into winning new work; writing proposals is a time-consuming and resource-intensive task. Fully understanding the alternatives available for a COOP program helps the contractor understand its government customer better, while also providing it with ready-made tools and techniques for implementing the program in a production environment.
Insufficient Personnel to implement COOP program	Government / Contractor	The contractor can work with the government to allow more-qualified personnel on the contract. The contractor can fund these positions by taking a lower margin; the contractor benefits by "growing" an internal COOP program implementation practice that, over time, can be an institutional capability to generate additional work and to differentiate the contractor from its competitors.

4.3 Next Steps

The next paper in this series will identify how the small Army program can begin to implement COOP. Some good approaches include defining the specific COOP program's policies and management reporting structure that will make the program a success. The federal, DoD, and Army policy drivers identified in this paper will be used as a basis for the COOP program policy suggested in the next paper.

Appendix A: Acronyms and Abbreviations

AR	U.S. Army Regulation
BCM	Business Continuity Management
C&A	Certification and Accreditation
C4I	Command, Control, Communications, Computers, and Intelligence
COG	Continuity of Government
COOP	Continuity of Operations
CPFF	Cost-Plus-Fixed-Fee (*contract*)
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
DR	Disaster Recovery
ERG	Emergency Relocation Group
FEMA	Federal Emergency Management Agency
HSPD	*(National Security and)*Homeland Security Presidential Directive
IBHS	Institute for Business and Home Safety
IA	Information Assurance
IT	Information Technology
ITIL	IT Infrastructure Library
MEF	Mission Essential Function
MOA	Memorandum of Agreement
NEF	National Essential Function
NCPIP	National Continuity Policy Implementation Plan
PMO	Program Management Office
POC	Point-of-Contact
PWS	Performance Work Statement
SLA	Service Level Agreement
U.S.	United States

USD(P)	Under Secretary of Defense for Policy

Reference List

[AR25-2] Department of the Army. October 24, 2007 (Rapid Action Revision Issue Date: March 23, 2009). Army Regulation 25-2: Information Assurance. <http://www.apd.army.mil/pdffiles/r25_2.pdf>. Accessed: June 12, 2011. 103 p.

[AR500-3] Department of the Army. 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.

[DODD-3020] 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.

[DODD-5220] Department of Defense. January 1995. DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM). <http://www.usaid.gov/policy/ads/500/d522022m.pdf>. Accessed: June 11, 2011. 96 p.

[DOD-8500.2] Department of Defense. February 6, 2003. DoD Instruction 8500.02: Information Assurance (IA) Implementation. <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>. Accessed: May 2, 2011. 102 p.

[HSPD-20] 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.

[IBHS] McClure D. 2007. Open for Business: A Disaster Protection and Recovery Planning Toolkit for the Small to Mid-Sized Business. IBHS: Tampa, FL. 76 p.

[ITILv3] Malone T, Menken I, Blokdijk G. January 18, 2010. ITIL V3 Foundation Complete Certification Kit (Third Edition). Emereo Pty Ltd; 3 Pap/Psc edition.

[NCPIP] Homeland Security Council. August, 2007. National Continuity Policy Implementation Plan. <http://www.fema.gov/pdf/about/org/ncp/ncpip.pdf>. Accessed: June 14, 2011. 98 p.

[PWS] Army Organization. May 24, 2011. Performance Work Statement (proprietary).