AIR FORCE AUDIT AGENCY

CONTINUITY OF OPERATIONS PLANS FOR COMPUTER NETWORKS

AUDIT REPORT

F2007-0009-FB4000
24 August 2007

Executive Summary

INTRODUCTION

Continuity of Operations (COOP) planning refers to measures needed to sustain or recover information technology services during and following an emergency or system disruption. These measures may include relocating information technology systems operations to an alternate facility, recovering information technology functions using alternate equipment, or performing functions manually. The Air Force and its reserve components operate 7 Major Command Communication Coordination Centers (MCCCs), a Network Operations and Security Center (NOSC), 6 Regional Operations and Security Centers (ROSCs), and 204 Network Control Centers (NCCs) requiring COOPs.

OBJECTIVES

We conducted this audit because COOP plans provide an essential roadmap for sustaining and restoring computer networks during contingencies, natural disasters, and other threats. The objective was to determine whether communications squadron personnel effectively managed COOP plans for MCCCs, NOSC, ROSCs, and installation NCCs. Specifically, we determined whether communications squadron personnel properly:

- Prepared plans to identify contingencies that could disrupt operations and actions required to restore operations.
- Exercised plans annually to ensure restoration capability during contingencies.
- Classified plans.

CONCLUSIONS

Air Force communications personnel need to improve overall COOP plan management. Specifically:

- Communications squadron personnel did not properly prepare COOP plans. As a result, communications personnel were not prepared to respond to contingencies and mitigate the impact on Air Force computer networks. This lack of capability could disrupt communications vital to accomplishing the supported installation and Air Force mission. (Tab A, page 1)
- Communications squadron personnel did not effectively exercise their COOP plans. Plans must be

exercised annually to identify, mitigate, and resolve shortfalls in procedures or resources. This includes alternate facilities, staffing, equipment, or training needed to sustain or timely restore network operations during or following a contingency. (Tab B, page 5)

- Communications squadron personnel did not properly classify COOP plans. Plans must be properly classified to help ensure sensitive information concerning network operations is not compromised. (Tab C, page 7)

RECOMMENDATIONS

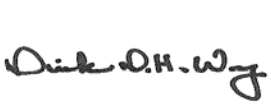
We made five recommendations to improve COOP plan preparation, exercises, and classification. (Reference the individual Tabs for specific recommendations.)

MANAGEMENT'S RESPONSE

Management concurred with the audit results and recommendations, and management actions planned should correct the problems. Therefore, this report contains no issues requiring elevation for resolution.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The Federal Information Security Management Act (FISMA) as codified in Title III of the E-Government Act of 2002, Public Law 107-347, requires each Chief Information Officer report material weaknesses in policies, procedures, or practices annually to the Office of Management and Budget. Recommendations A.1, B.2, C.1 and C.2 in this report address corrective actions needed to improve the effectiveness of security for computer networks. In our opinion, the material weaknesses identified meet the requirement for establishing an Air Force Plan of Action and Milestone. In addition, we will consider these weaknesses for inclusion in our annual FISMA input to the Secretary of the Air Force and the DoD Inspector General.



DERRICK D. H. WONG
Associate Director
(Information Systems Security and Communications Division)

JUDITH L. SIMON
Assistant Auditor General
(Financial and Systems Audits)

Table of Contents

BACKGROUND

MCCCs, NOSC, and ROSCs provide and manage command-wide network operations and security for the Air Force enterprise network. These activities maintain situational awareness to ensure the network is available and protected through security scans and patches. NCCs manage the installation-level computer network and associated infrastructure (or enterprise) providing the communications and computing resources needed for day-to-day operations.

Air Force Instruction (AFI) 10-208, *Continuity of Operations (COOP) Program*, 1 December 2005, requires all levels of command develop a COOP plan. COOP plans ensure capability exists to continue mission essential functions across a wide range of potential emergencies, including physical threats such as acts of nature (for example, floods and hurricanes) and logical threats such as technological attack (for example, viruses, denial-of-service attacks, program bugs). The AFI also requires a risk assessment to include an analysis of mission, threats and vulnerabilities, and development of exercise programs to evaluate the readiness of the continuity plans. In addition, this program should include personnel, equipment, systems, processes, and procedures necessary to respond in a crisis. Finally, it details how plans must be validated and updated every 2 years, or more frequently as needed.

Federal Emergency Management Agency (FEMA) Federal Preparedness Circular (FPC) 65, *Federal Branch Continuity of Operations (COOP)*, 15 June 2004, provides federal agencies guidance and a template for preparing COOP plans. The FPC also recommends performing risk assessments to support plan preparation. The following publications provide guidance applicable to information technology systems.

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, July 2002, provides detailed guidance on how to conduct risk assessments for information technology systems and determine suitable technical, management, and operational security controls.

- NIST SP 800-34, *Contingency Planning Guide for Information Technology (IT) Systems*, June 2002, provides a narrative description of COOP plan contents for information technology systems.

AUDIT RESULTS 1 – COOP PREPARATION

Condition. Communication squadron personnel did not properly prepare COOP plans. Specifically, 128 (88 percent) of 146 active duty, Air National Guard (ANG), and Air Force Reserve Command (AFRC) MCCCs, NOSC, ROSCs, or

NCCs reviewed did not prepare plans.[1] Further, the 18 prepared plans (see footnote 1) were incomplete. The plans did not include one or more essential elements, including risk assessments, alternate facilities, staffing and equipment requirements, or maximum time to re-establish network operations.

Cause. This condition occurred because the Secretary of the Air Force Chief, Warfighting Integration and Chief Information Officer (SAF/XC) did not develop or provide guidance for COOP plan requirements to communications personnel. Thus, communications personnel were not aware of the requirement to prepare or how to prepare a plan.

Impact. As a result, communications squadron personnel were not prepared to respond to contingencies and mitigate the impact on Air Force computer networks. This lack of capability could disrupt communications vital to accomplishing the supported installation and Air Force mission.

Recommendation A.1. SAF/XC, in coordination with the Deputy Chief of Staff for Operations, Plans and Requirements (AF/A3/5), should develop guidance to:

a. Require communications personnel at MCCCs, NOSC, ROSCs and NCCs conduct a periodic risk assessment and prepare COOP plans.

b. Explain the process for preparing a COOP plan. As a minimum, the guidance should include information from NIST SP 800-30 on conducting risk assessments and information from NIST SP 800-34 on plan contents.

c. Require communications personnel validate and update COOP plans every 2 years, or more frequently as needed.

Management Comments A.1. SAF/XC concurred and stated:

a. "SAF/XC will release communications to the field requiring communications personnel at MCCCs, NOSC, ROSCs and NCCs to conduct a periodic risk assessment and prepare COOP plans in accordance with AFI 10-208. Estimated Completion Date: 30 November 2007.

b. "SAF/XC will release communications to the field requiring COOP plans follow guidance as established in Chapter 2 of AFI 10-208. Estimated Completion Date: 30 September 2007. Additionally, SAF/XC will work in conjunction with AF/A3 to make

[1] Specific locations not shown due to security classification concerns. Locations were provided to management during the audit.

changes to AFI 10-208 to include detailed information for COOP plans for Air Force network systems. Estimated Completion Date: 31 December 2007."

c. "SAF/XC will release communications to the field requiring compliance with Paragraph 2.5 of AFI 10-208, which states 'All organizations are required to validate and update their COOP plan every 2 years'. Estimated Completion Date: 30 November 2007."

Evaluation of Management Comments. Management comments addressed the issues raised in the audit results, and management actions planned should correct the problem.

This Page Intentionally Left Blank

BACKGROUND

DoD Directive 3020.26, *Defense Continuity Program (DCP),* 8 September 2004, and AFI 10-208 require exercising COOP plans annually. Exercising a plan involves establishing procedures, roles, and responsibilities in the event network operations are compromised. Although exercising a plan does not prevent interim or extended service interruption, it does support a more rapid response that could minimize impact.

NIST SP 800-34 defines COOP exercises as announced or unannounced and suggests exercises include the worst-case incident or an incident most likely to occur, and system recovery simulation on an alternate platform from backup media. The guidance also notes that an exercise must never disrupt normal operations.

AUDIT RESULTS 2 – COOP EXERCISES

Condition. Communications squadron personnel at MCCCs and NCCs did not effectively exercise their COOP plans. Specifically, 13 (72 percent) of 18 locations with plans did not exercise, and 5 (28 percent) did not effectively exercise their plans (see footnote 1 on page 2). For example, exercises did not include system recovery simulation on an alternate platform using backup media. To illustrate, communications squadron personnel at two locations considered a telephone inquiry into their supportability or a building evacuation exercise as COOP plan exercises.

Cause. This condition occurred because SAF/XC neither provided guidance nor referred communications personnel to exercise requirements in AFI 10-208. As a result, communications personnel were not aware of the requirement to exercise plans, what constituted an effective exercise, or how to accomplish exercises without disrupting network users.

Impact. COOP plans must be exercised annually to identify, mitigate, and resolve shortfalls in procedures or resources (such as alternate facilities, staffing, equipment, or training) needed to timely restore network operations to support mission essential functions during or following a contingency.

Recommendation B.1. SAF/XC, in coordination with the Air Force Network Operations Commander (AFNetOps/CC), should establish a method for exercising COOP plans without disrupting network users.

Management Comments B.1. SAF/XC concurred and stated: "SAF/XC will coordinate with AFNetOps/CC to ensure the establishment of a method for exercising COOP plans with minimal disruption for network users. Estimated Completion Date: 31 December 2007."

Recommendation B.2. SAF/XC should develop guidance to:

a. Require communications personnel exercise their COOP plan at least annually.

b. Provide communications personnel criteria on actions that constitute an effective exercise, methods for conducting exercises, and procedures for documenting and addressing lessons learned and mitigating or resolving shortfalls and limiting factors.

Management Comments B.2. SAF/XC concurred and stated:

a. "SAF/XC will release communications to the field requiring communications personnel exercise their COOP plan at least annually and meet criteria for effective exercises in accordance with AFI 10-208. Estimated Completion Date: 30 November 2007."

b. "SAF/XC will work in conjunction with AF/A3 to make changes to AFI 10-208 to include detailed information for exercising COOP plans for AF network systems. Estimated Completion Date: 31 December 2007."

Evaluation of Management Comments. Management comments addressed the issues raised in the audit results, and management actions planned should correct the problem.

BACKGROUND

AFI 10-208 requires Air Force personnel to classify COOP plans based on content according to applicable security guidance. Classification is required when a plan includes highly sensitive or critical continuity information, such as information on alternate facilities and shortfalls in equipment and staffing.

DoD *Defense Continuity Program (DCP) Security Classification Guide,* 15 December 2005, provides guidance on classifying COOP plans, including information technology network plans. The guide also provides tables to determine when and how to classify plans.

AUDIT RESULTS 3 – COOP CLASSIFICATION

Condition. Communications squadron personnel did not properly classify COOP plans. Specifically, only 2 (11 percent) of 18 plans (see footnote 1 on page 2) reviewed were marked classified. However, other plans contained possible classified information such as alternate facilities and schematic diagrams of their NIPERNET and SIPERNET networks, but were not marked classified. For example, the COOP plans for MCCCs at three locations (see footnote 1 on page 2) identified alternate facilities, but were not properly classified.

Cause. This condition occurred because SAF/XC neither provided guidance nor referred communication personnel to classification requirements in AFI 10-208 or classification guidance in the DCP Security Classification Guide. Therefore, communication personnel were not aware of the requirement to classify plans or how to determine the appropriate classification.

Impact. COOP plans must be properly classified to ensure sensitive information concerning network operations is not compromised.

Recommendation C.1. SAF/XC, in coordination with AFNetOps/CC, should require communication squadron personnel evaluate and classify existing COOP plans using the DCP Security Classification Guide.

Management Comments C.1. SAF/XC concurred and stated: "SAF/XC will release communications to the field requiring communications squadron personnel evaluate and classify existing COOP plans using the DCP Security Classification Guide in accordance with AFI 10-208. Estimated Completion Date: 30 November 2007."

Recommendation C.2. SAF/XC should develop guidance requiring communications squadron personnel evaluate and classify all future COOP plans using the DCP Security Classification Guide.

Management Comments C.2. SAF/XC concurred and stated: "SAF/XC will release communications to the field requiring communications squadron personnel evaluate and classify all future COOP plans using the DCP Security Classification Guide in accordance with AFI 10-208. Estimated Completion Date: 30 November 2007."

Evaluation of Management Comments. Management comments addressed the issues raised in the audit results, and management actions planned should correct the problem.

AUDIT SCOPE

Audit Coverage. We performed audit work at 7 MCCCs and 20 randomly selected active duty NCCs. Additionally, we visited Headquarters AFRC and ANG to review COOP plans for all 119 Reserve Component MCCCs, NOSC, ROSCs and NCCs (Appendix II). We also discussed COOP plans with SAF/XC and AF/A3/5. We performed the review from May through December 2006, and evaluated plans dated 5 August 2003 through 5 June 2006. We provided a draft report to management in May 2007.

- Preparation. We reviewed COOP plans to determine whether communications squadron personnel identified contingencies that could disrupt operations. We also reviewed plans for risk assessments and whether the assessments identified both physical and logical vulnerabilities. We also compared information in the plans to NIST 800-34 on plan preparation and content for information technology systems to determine whether plans identified all actions required to restore network operations.

- Exercises. We interviewed communications squadron personnel and requested and reviewed supporting documentation to determine whether COOP plans were effectively exercised.

- Classification. We compared information in COOP plans to classification guidance in DoD DCP *Security Classification Guide* to determine whether plans were properly classified.

Sampling Methodology.

- Sampling. We used random sampling to select 20 of the 93 active duty Air Force NCCs for review. We judgmentally selected all 7 MCCCs, the ANG NOSC, all 6 ANG ROSCs, all 95 ANG NCCs, the AFRC MCCC, and all 16 AFRC NCCs to ensure comprehensive coverage.

- Computer-Assisted Auditing Tools and Techniques (CAATTs). We did not use CAATTs to analyze data.

Data Reliability. We did not rely on computer-generated data to support audit conclusions.

Auditing Standards. We conducted this audit in accordance with generally accepted government auditing standards and, accordingly, included tests of key internal and management controls associated with preparing, exercising, and classifying COOP plans.

PRIOR AUDIT COVERAGE

We did not identify any Air Force Audit Agency, DoD Inspector General, or Government Accountability Office reports issued within the past 5 years that addressed the same or similar objectives as this audit.

Air Combat Command (ACC)

HQ ACC Langley AFB VA	NONE
2d Bomb Wing Barksdale AFB LA	NONE
5th Bomb Wing Minot AFB ND	NONE
9th Reconnaissance Wing Beale AFB CA	NONE
20th Fighter Wing Shaw AFB SC	NONE

Air Education and Training Command (AETC)

HQ AETC Randolph AFB TX	NONE
42d Air Base Wing Maxwell AFB AL	NONE
314th Airlift Wing Little Rock AFB AR	NONE
325th Fighter Wing Tyndall AFB FL	NONE

Air Force Materiel Command (AFMC)

HQ AFMC Wright-Patterson AFB OH	NONE
95th Air Base Wing Edwards AFB CA	NONE
311th Human Systems Wing	NONE

Brooks City-Base TX

Air Force Reserve Command (AFRC)

HQ AFRC Robins AFB GA	NONE

Air Force Space Command (AFSPC

HQ AFSPC Peterson AFB CO	NONE
153d Air Wing Cheyenne Mountain AFB CO	NONE

Air Mobility Command (AMC)

HQ AMC Scott AFB IL	NONE
62d Air Wing McChord AFB WA	NONE
305th Air Mobility Wing McGuire AFB NJ	NONE
319th Air Refueling Wing Grand Forks AFB ND	NONE
437th Air Wing Charleston AFB SC	F2006-0075-FDM000 12 September 2006

Air National Guard (ANG)

HQ ANG Washington DC	NONE

Pacific Air Forces (PACAF)

HQ PACAF Hickam AFB HI	NONE
36th Air Expeditionary Wing Andersen AFB, Guam	NONE
354th Fighter Wing Eielson AFB AK	NONE

United States Air Forces in Europe (USAFE)

HQ USAFE Ramstein AB, Germany	NONE
31st Fighter Wing Aviano AB, Italy	NONE
39th Air Base Wing Incirlik AB, Turkey	NONE
423d Air Base Group RAF-Alconbury AB, United Kingdom	NONE
426th Air Base Squadron Stavanger AB, Norway	NONE

This Page Intentionally Left Blank

Information Systems Security and Communications Division (AFAA/FSS)
Financial and Systems Audits Directorate
5023 4th Street
March ARB CA 92518-1852

Derrick D. H. Wong, Associate Director
DSN 447-4929
Commercial (951) 655-4929

LeeRoy H. Waugh, Program Manager

John Panzullo, Audit Manager

We accomplished this audit under project number F2005-FB4000-0072.000.

This Page Intentionally Left Blank

SAF/OS
SAF/US
SAF/FM
SAF/IG
SAF/LL
SAF/PA
SAF/XC, AF/A6
AF/CC
AF/CV
AF/CVA
AF/A3/5
AF/A8
AF/RE
NGB/CF
NGB/IR

AU Library
DoD Comptroller
OMB

ACC
AETC
AFCA
AFMA
AFMC
AFNetOps
AFOSI
AFRC
AFSOC
AFSPC
AIA
AMC
ANG
PACAF
USAFA
USAFE
Units/Orgs Audited

FREEDOM OF INFORMATION ACT

The disclosure/denial authority prescribed in AFPD 65-3 will make all decisions relative to the release of this report to the public.

This Page Intentionally Left Blank

To request copies of this report or to suggest audit topics for future audits, contact the Operations Directorate at (703) 696-7913 (DSN 426-7913) or E-mail to reports@pentagon.af.mil. Certain government users may download copies of audit reports from our home page at www.afaa.hq.af.mil/. Finally, you may mail requests to:

Air Force Audit Agency
Operations Directorate
1126 Air Force Pentagon
Washington DC 20330-1126