CENTERS for MEDICARE & MEDICAID SERVICES
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

ESG
Enterprise Information
Security Group
Risk Management, Oversight,
And Monitoring

Risk Management Handbook
Volume II
Procedure 4.4
Contingency Plan Development

FINAL
Version 1.0
November 6, 2014

Document Number: CMS-CISO-2014-vII-pr4.4

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CONTINGENCY PLAN DEVELOPMENT* PROCEDURE, VERSION 1.0, DATED NOVEMBER 6, 2014

1. Baseline version. This document, along with its corresponding Risk Management Handbook (RMH), Volume III Standard, replaces *CMS Information Security (IS) Application Contingency Plan (CP) Procedures*, dated November 14, 2008, and its associated *CMS Information Security (IS) Contingency Plan (CP) Template*, Version 1.0, dated November 14, 2008.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

The purpose of the Centers for Medicare & Medicaid Services (CMS) *Contingency Plan (CP) Development Procedure* is to provide CMS Business Owners, Information System Security Officers (ISSOs) and Contingency Plan Coordinators (CPCs) a systematic guide to coordinating, developing, and maintaining CPs. Additionally, this procedure will provide a contingency planning methodology that is integrated with the CMS eXpedited Life Cycle (XLC).

Specifically, this procedure will provide guidance for consistently performing the following steps:

- Determining IT recovery requirements in the form of Recovery Time Objectives (RTOs)[1] and Recovery Point Objectives (RPOs)[2].
- Determining the most effective recovery strategies.
- Developing and maintaining complete and executable CPs.

1.2 BACKGROUND

CMS is reliant on its information systems[3] for mission fulfillment. Information systems are susceptible to a wide variety of events and threats that may affect their ability to process, store and transmit raw data and information. Contingency planning is one method of reducing risk to CMS' operations by providing prioritized, efficient, and cost effective recovery strategies and procedures for the organizations' Information Technology (IT) infrastructure.

Contingency planning refers to the interim measures taken to recover an information system and IT services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate or replacement equipment, or implementation of manual methods as a substitute for functions performed by that information system.

[1] RTO *(Recovery Time Objective)* is the overall length of time an information system's components can be in the recovery phase before negatively affecting the organization's mission or mission/business processes. (SP 800-34).

[2] RPO is the point in time to which data must be recovered after an outage. SP 800-34 (R1) dated May 2010. RPO is the requirement for data currency and validates the frequency with which backups are conducted and off-site rotations performed.

[3] An *information system* is defined as *"A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"* in the CMS Risk Management Handbook (RMH), Volume I, Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms*. *available at* http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Through this procedure CMS promulgates and operationalizes this requirement and reiterates the importance of contingency planning. Each system must have a CP and test that CP annually to maintain compliance with the Federal Information Security Management Act (FISMA).

This procedure provides the instructions to develop a CP. The processes provided in this procedure require action on the part of the CMS business owners.

In order to support FISMA requirements as well as requests from FISMA auditors and the Department of Health and Human Services (DHHS) Inspector General (IG) CMS requires that business owners have documentation available for review. Note: System Developers/Maintainers and Information System Security Officers (ISSOs) will assist in meeting these reporting requirements[4]. An effective way to support this requirement is to upload completed copies of current versions of the following to the CMS FISMA Controls Tracking System (CFACTS):

- Contingency Plan,
- Contingency Plan Exercise Plan, and
- Contingency Plan Exercise After Action Report (AARs).

1.3 HOW TO USE THIS PROCEDURE

This procedure is broken down into two columns: *Procedure* and *Principle*. The *Procedure* column specifically addresses the steps to perform in order to complete the process. The *Principle* column provides additional applicable information about the specific procedural step to aid understanding. However, it is assumed that the user possesses a minimal working understanding of the subject-matter.

1.4 RELATED PROCEDURES

Other relevant Risk Management Handbook (RMH) documents include:

- RMH Volume I, Chapter 1, *Risk Management in the XLC.* This chapter provides information required to understand the interrelation of information security, risk management, the CMS XLC, and the system life cycle.
- RMH Volume II, Procedure 1.1, *Accessing the CFACTS*. This procedure is required to gain access to, and log into the CFACTS.
- RMH Volume II, Procedure 2.3, *Categorizing an Information System*. This procedure explains how to establish the system's security category in CFACTS.
- RMH Volume II, Procedure 2.6, *Information System Description*. This procedure is required to create or update system information in CFACTS.

[4] For Contingency Plan Exercise Procedures see the Risk Management Handbook Volume II Procedure 4.5 *Contingency Plan Exercise available at* http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

- RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*. This procedure is required to document security controls in CFACTS and is a prerequisite for documenting testing of the applicable security control(s).
- RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS*. This procedure is required to document security control testing, and directs the documentation of identified weaknesses.
- RMH Volume II, Procedure 6.2, *POA&M Management*. This procedure is required to ensure that weaknesses are properly documented and managed in CFACTS.
- RMH Volume II, Procedure 6.3, *Security Information Review*. This procedure provides a systematic guide to review and ensure the accuracy and completeness of security related information for systems in CFACTS.
- RMH Volume II, Procedure 7.8, *Key Updates*. This procedure explains how to ensure that Weaknesses are properly documented and managed in CFACTS. This procedure is required to ensure that all information in CFACTS is updated to reflect recent events.
- RMH Volume III Standard 4.4 *Contingency Planning Standard*. This standard provides the overarching CP policies.

Other relevant procedures that are not yet incorporated into the *Risk Management Handbook* include:

- *CMS System Security Plan (SSP) Procedure*.
- *CMS Information Security Risk Assessment (IS RA) Procedure*.
- *CMS CP Exercise Procedure*.

All applicable RMH procedures are available on the CMS information Security website, in the Information Security Library at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

2 PROCEDURES

PROCEDURE

PRINCIPLE

2.1 CONTINGENCY PLAN DEVELOPMENT

2.1.1 PROCEDURE USERS

1. CMS Business Owners.

2. CMS System Developers/Maintainers.

PROCEDURE	PRINCIPLE
3. CMS ISSOs.	
4. CMS Contingency Plan Coordinators (CPCs).	

2.1.2 INITIAL CONDITIONS

1. The system has been categorized in accordance with RMH Volume II, Procedure 2.3, *Categorizing an Information System*.	*Each system will be categorized in accordance with Federal Information Processing Standards (FIPS) 199. RMH Volume II, Procedure 2.3,* Categorizing an Information System *contains the CMS instructions to accomplish this activity.*
2. A system description has been developed and approved.	*The system description includes the system boundary. Well-defined boundaries establish the scope of protection for organizational information systems and include the people, processes, facilities, and information technologies.*
3. The system has been registered in the CMS Enterprise Architecture.	*Information system registration, in accordance with organizational policy, uses information in the system identification section of the security plan to inform the parent or governing organization of: (i) the existence of the information system; (ii) the key characteristics of the system; and (iii) any security implications for the organization due to the ongoing operation of the system.*

PROCEDURE **PRINCIPLE**

2.1.3 DETERMINE CRITICAL PARAMETERS

Key characteristics of the business process and system must be identified as the first step in developing a Contingency Plan. Many methods can be used to generate the information, including a focused risk assessment and a Business Impact Analysis (BIA).

1. Determine four (4) critical timing factors.

a. Maximum Tolerable Downtime (MTD) of the mission/business process.

The MTD is the amount of time mission/ business process can be disrupted without causing significant harm to the organization's mission. [NIST SP 800-34]

b. Recovery Time Objective (RTO) of the system.

RTO is the overall length of time an information system's components can be in the recovery phase before negatively affecting the organization's mission or mission/business processes. [NIST SP 800-34]

c. Recovery Point Objective (RPO) of the data.

The RPO is the point in time to which data must be recovered after an outage. [NIST SP 800-34]

d. Work Recovery Time (WRT).

The WRT (Work Recovery Time) is the time it takes to get critical business functions back up-and-running once the systems (hardware, software, and configuration) are restored to the RPO. This includes the manual processes necessary to verify that the system has been restored to the RPO, and all necessary processes to address the remaining lost, or out-of-synch, data or business processes. See RMH Vol 1, Chapter 1 Risk Management in the XLC *for information on the Information System Description and requisite information.*

PROCEDURE	**PRINCIPLE**
2. Identify any *Single Points of Failure* (SPOFs) that need to be mitigated.	*An SPOF can be any resource, service, or person without backup that is critical to operations.*
a. Examine personnel skill sets to determine if any one person is critical to operations and to the recovery of the system and does not have a viable replacement.	
b. Examine system hardware and identify all system devices that do not have immediately available backup hardware should the primary devices fail.	
c. Coordinate with the infrastructure provider to determine if the points at which the infrastructure is vulnerable to failure for the loss of a single device or telecommunications path.	*Although the infrastructure is under the purview of the Enterprise Data Center (EDC) provider, it is incumbent upon each business owner to understand vulnerabilities and SPOFs of their systems within the current architecture.*
3. Identify all systems that provide critical data feeds to your system.	*It may be necessary to develop a Service Level Agreement (SLA) with the infrastructure provider or another business owner to ensure the upstream dependencies of your system can be recovered within the identified recovery time of your system.*
4. Determine all customers of your services/ products and data from the system for which you are developing a CP to ensure the identified recovery metrics meet their recovery requirements.	*System owners may need to develop an SLA to ensure your system is recovered quickly enough to ensure the recoverability of their system within that system's RTO.*

2.1.4 RECOVERY STRATEGY ANALYSIS

PROCEDURE	PRINCIPLE
1. Identify personnel to staff the Recovery Team.	*The recovery team must have enough persons assigned to effectively conduct a damage assessment and then implement the recovery strategies for system hardware, software, and data.* *A second consideration is the geographical separation between the primary and alternate facility (if applicable).* *Damage assessment may not be complete before a disaster is declared. Should this occur the team must be split between completing damage assessment at the primary facility and implementing recovery at the alternate facility.*
a. Identify a team leader and at least one alternate.	*The team leader should be the business owner.*
(1) The Team leader and alternate both must have the authority to declare a system disaster.	
b. Identify the Contingency Plan Coordinator (CPC).	*The CPC will normally be the ISSO who will have technical responsibility for all system recovery for a given Line Of Business (LOB).* *One of the primary responsibilities of the CPC is to ensure a recovered system meets FISMA requirements for that system.*
c. Identify the technical team who will implement the recovery strategies.	*The technical team must be able to implement the recovery strategies for the system hardware, software, and data.* *The technical team will also be called upon to validate the data prior to the users accessing the system*

PROCEDURE	**PRINCIPLE**
2. Coordinate with the infrastructure business owner to determine if the data center recovery agreements/contracts include or should include the system.	
3. If the system is not to be included within the data center's DRP, determine the most applicable and cost effective strategies.	*Recovery strategies will need to be identified for hardware, software, and data.* *The overarching characterization of recovery strategies is that as recovery times become shorter, there are fewer strategies to choose from, and those available strategies become more expensive.*
4. When determining data recovery strategies, a "best practice" is to consolidate them with backup strategies.	*Data backup and recovery strategy costs are impacted by several factors, including:* ● *The frequency with which backups are conducted.* ● *The media on which backups are stored.* ● *The availability of backups (i.e. how easily backups may be retrieved and transported to either the primary or alternate processing facilities).*
5. Software and Data backup and recovery strategies include, but are not limited to:	
a. Automatic active-active failover. Supports near-zero RTOs and RPOs.	*Automatic failover to an alternate, online system that does not require manual intervention or implementation.*
b. Active-passive failover.	*The backup system allows for automatic replication. In the event of a primary system failure, some manual intervention is required to bring the backup system fully online.*
c. Data Mirroring.	*Data is written to an alternate data repository (e.g. Storage Area Network [SAN]) as it is being written to the primary system. Recovery still requires loading software and then the stored data.*
d. Data Vaulting.	*Data is written to an offline data repository. As with data mirroring recovery requires loading the software and then the stored data.*

PROCEDURE	PRINCIPLE
e. Backup tapes.	*The least expensive and most ubiquitous strategy. System recovery requires the most intervention and delivery of the tapes to the alternate facility.*
6. Determine the most applicable and cost effective strategies for hardware replacement.	
7. Hardware strategies include but are not limited to:	*Hardware recovery strategy contracts must be crafted clearly and specifically. Only the equipment identified in any contract will be provided.* *Ad hoc additions at the time of a disaster will incur premium rates.*
a. Redundant systems.	*Redundant systems include hot sites, cloud recovery services, and self-owned data centers (to include Virtual Data Centers [VDCs]).* *Each of the above examples supports specific RTOs and therefore greater care must be taken when determining the most applicable strategy for the systems with the shortest RTOs.* *Regardless of the mode selected (i.e. active-active or active-passive), redundant hardware will be required.*
b. Drop-ship or Quick-ship contracts.	*Drop-ship is an agreement with the current hardware vendor(s) to provide specific replacement hardware within specified delivery times or Service Level Agreements (SLAs).*
c. Internal swap-out.	*Internal Swap-out is the planned replacement of critical hardware with lesser critical hardware.* *This strategy transfers the risk of an outage to lesser critical systems and therefore requires an agreement between Business Owners.*

PROCEDURE	PRINCIPLE
d. Wait out the disaster.	*Waiting out the disaster until the organization has recovered all other, more critical systems is a viable strategy for IT systems that support routine business functions.* *When implementing this strategy it must be clear that disaster recovery may take up to 30 days or longer.*
8. Determine an estimate for the aggregated cost estimate for all strategies.	*Costs must include one-time start up as well as recurring costs.*
9. Obtain approval for the overall recovery solution comprised of the individual recovery strategies.	*System recovery strategies are to be approved by the business owner.*

2.1.5 CP DEVELOPMENT

1. The purpose of a CP is to establish thorough pre-approved policies, procedures, and technical measures a capability that facilitates the recovery of system operations quickly and effectively following a service disruption.[5]	*Using a CP to reference and/or provide links to other documents that provide the specific recovery procedures will impede system recovery and not provide the level of detail for recovery necessary to meet recovery requirements.* *Referencing other documents for administrative information such as system description and past CP exercises will not detract from the effectiveness of a CP.*
2. Each plan will be divided into the following six (6) Sections which will be described in subsequent sections of this procedure.	

[5] SP 800-34 revision 1 *Contingency Planning Guide for Federal Information Systems*

PROCEDURE	PRINCIPLE
3. Section 1 - Introduction.	*This section is to provide short sections that synopsize the scope of the CP and any assumptions or limitations that were considered in the development of the CP.*
a. Scope.	*The scope of the CP will be clearly identified, limiting the applicability to the single system for which the plan has been developed and the personnel who have been identified to implement it.*
b. Assumptions.	*This section of the CP will clearly identify any planning limitations or expectations over which the business owner has no control.*
4. Section 2 - Concept of Operations (CONOPS) will consist of a system description, overview of the three recovery phases and recovery team roles and responsibilities.	*Each CP will have a CONOPS section that provides, at a minimum:* *Section that identifies the recovery prioritization of the system* *Overview of the three (3) Phases; (1) Activation and Notification, (2) Recovery and (3) Reconstitution* *An overview of the approved recovery strategies for which procedures are provided in the "Recovery Phase" Section.* *Disaster declaration criteria based on the recovery metrics for the system.* *Roles and Responsibilities for developing, maintaining, exercising the plan, and conducting training.*
a. The system description should include the physical location, operating environment, recovery prioritization, system architecture, and functionality, general location of users and partnerships with external organizations and system interdependencies.	*The system description should be available from the applicable security plan.*

PROCEDURE	PRINCIPLE
b. Overview of the three phases.	*Each CP should be developed using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize effectiveness and minimize system outage.* *The Preparedness Phase is the step in the planning cycle that focuses on developing the plan, conducting initial exercises, and training. Since this phase occurs before any disaster, this phase is not included in the CP itself.* *The CONOPS needs only to provide a high level introduction to each of the three phases. Each phase will have its own section later in the plan.*
(1) Activation and Notification Phase.	*High level explanation of what actions will be covered in the Activation and Notification Phase.*
(2) Recovery Phase.	*The explanation provided in the CONOPS of this phase should introduce the approved recovery strategies for system recovery.*
(3) Reconstitution Phase.	*The explanation provided in the CONOPS of this phase should provide for the overall criteria for deactivating the plan and resuming normal operations.*
c. Roles and Responsibilities.	*Describe each team and role responsible for executing or supporting system recovery and reconstitution.* *Include responsibilities for each team/role, leadership role, and coordination with other recovery and reconstitution teams as applicable.*
(1) Business Owner.	*The Business Owner has overall management responsibility for the plan, executability of the plan and system disaster declaration authority.*

PROCEDURE	PRINCIPLE
(2) CPC.	*The CPC is responsible for oversight of all recovery and reconstitution progress, initiates any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.*
5. Section 3 - Activation and Notification Phase.	*The Activation and Notification Phase will provide: The initial actions taken to triage an incident; Activate initial response personnel; Conduct damage assessment; and declare a disaster if necessary; and the initial relocation of personnel, if necessary, to affect recovery.*
a. All personnel with recovery responsibilities should provide contact information to include after-hours.	
b. The initial actions to be taken must include damage assessment procedures for the hardware, software, and data.	
c. The disaster declaration criteria will be the length of time the impact(s) of the event is/are expected to persist (disruption period) when compared to system RTOs.	*The clock for reestablishing functions and IT systems within their RTOs and MTDs begins at the time of the event, not from the completion of the damage assessment or the formal disaster declaration.*
(1) If the disruption period exceeds the RTO, the disaster declaration criterion is met and a disaster should be declared.	
(2) If the disruption period does not exceed the RTO, the decision to "wait out" the incident would be viable.	
(3) If access to the facility is denied beyond the RTO (e.g. first responders have ordered an evacuation), then a disaster would be declared based on the *Denial of Facility* impact.	

PROCEDURE	PRINCIPLE
(4) If a cyber-security event occurs such as intrusion or malware infection, the incident response team would have to provide timing estimates to the declaration authority. If the disruption period including all time while gathering all forensic evidence exceeds the system RTO, a disaster should be declared.	
d. If personnel are required to relocate to an alternate facility, driving directions should be included as well as any additional guidance for personnel transportation.	*Contingencies should consider impassible traffic routes and shutdown of air transportation.*
e. Procedures for physical security access and alternate location Points of Contact (POC) should be included in this section.	*If security badges or other access tokens need to be distributed to relocating personnel, thorough coordination and clear procedures will reduce confusion and facilitate check in procedures.*
6. Section 4 - Recovery Phase.	*The recovery phase will provide the detailed procedures for implementing and sustaining the approved recovery strategies outlined in the CONOPS section.* *Also in this phase are included the procedures for notifying higher authority, functional partners and system users.*
a. Provide the step-by-step procedures for the hardware and software recovery.	*Assume the CP is the only document available to you at the time of the disaster. Additionally, assume the network is unavailable for online retrieval.*
(1) Include the procedures for loading the application software onto recovery hardware.	*This may include having to update security configurations and settings since the last backup was taken.*
(2) Provide procedures for updating the software to accommodate any patches or revisions to those in place when the system became unavailable.	*This procedure must be specific enough to provide accurate guidance but generic enough to accommodate any updates or patches that may have been installed throughout the system lifecycle.*

PROCEDURE	PRINCIPLE
(3) Provide procedures for contacting the alternate storage facility POC(s) and contact information for access after normal business hours as well as access during normal working hours must be included.	
b. Ensure accurate technical step-by-step procedures are included.	*The assumption must be that other documents such as Operations and Maintenance (O&M) Manuals are not available and access to the network has been curtailed as a result of the disaster.*
(1) Include procedures for updating the data from the last backup to the time of the disaster.[6]	*It may be necessary to maintain hardcopy records or other method of transaction tracking to ensure the capability to update the system from the last backup to the time of the disaster.*
(2) The final step before allowing users' access is to validate the data.	*Ensure procedures are in place to obtain the recovery management team approval prior to authorizing system access to the users.*
(3) Include procedures for communicating with the user community and higher authority.	*Communications must include; the initial report that the system is down, expected time of recovery, any updates that may be required, and finally reporting the system is available and any configuration changes that may be required (e.g. IP address changes to reflect the alternate facility).*
(4) Provide system users with information regarding reaching customer service for resolving access issues.	

[6] This is where WRT comes into play and could make-or-break the ability to recover functionality, even if system recovery has gone smoothly up to this point.

PROCEDURE	PRINCIPLE
7. Section 5 Reconstitution Phase.	*The Reconstitution Phase will provide the detailed procedures for salvage operations, validating the system and data, normalizing operations, and terminating contingency operations.*
a. Salvage operations.	*Salvage operations must include hardware, software as well as hardcopy documentation.* *It is strongly recommended that each plan include certified restoration companies' contact information so that information may be retrieved from damaged hard drives as well as freeze drying damaged critical paper files.*[7]
b. System functionality validation.	*The system functionality must be verified by the system administrator and developer/maintainer.*
c. Data validation.	*Once the data has been restored from backups, and with any transactions processed during the recovery phase any backlogged transactions may be processed.*
d. Backlog processing.	*As soon as the backlog has been cleared, the business owner must be notified to report to the user community and higher authority as appropriate.*
e. Attaining normal operations.	*Normal operations are achieved when the system has been recovered, all data has been loaded and validated, and finally all backlogs have been processed.*
f. Terminating contingency operations.	*Once normal operations have been achieved, contingency operations are terminated.* *It is highly recommended that when authorized to relocate IT functionality to the permanent facility, the recovery procedures should be used for the final migration to that permanent facility.*

[7] For a list of certified restoration companies in a given state go to: http://www.restorationindustry.org/

PROCEDURE	**PRINCIPLE**
8. Section 6 Appendices.	*There will be a minimum of six (6) Appendices for each CP.* *The below listed appendices meet the requirements set forth in SP 800-34 (R1*
a. Appendix A: Personal Contact Information	*This appendix will contain all of the pertinent contact information for disaster declaration, succession of leadership and all personnel with recovery responsibilities for the system for which the CP was written.* *This appendix should include contact information for both during and after working hours.*
b. Appendix B: Vendor Contact Information	*This appendix will contain all of the points of contact and contact information for all vendors who may be needed for system recovery.* *This appendix should include contact information for both during and after working hours.*
c. Appendix C: Damage Assessment, Recovery and Reconstitution procedures	*This appendix **MUST** provide the detailed, key stroke by key stroke procedures for conducting damage assessment, implementing all of the approved recovery strategies and any variations on those procedures that may be necessary to return processing to the primary facility.* *The damage assessment report must include a disaster declaration recommendation based on the comparison between the Estimated Time to Repair (ETR) and the system RTO.* *These procedures must also include extending the recovered system to the user community even when that community may be dispersed across multiple alternate operating locations.* *It is not sufficient to reference other manuals, publications or documents in the CP, in the event those documents or access to those documents is not available at the time of a disaster.*

PROCEDURE	**PRINCIPLE**
d. Appendix D: System Description and Diagrams, Hardware and Software Inventories	*The information for this section may be copy/ pasted directly from the applicable security plan. However, it best to reproduce it here than to rely on other documentation that may or may not be available at the time of a disaster.*
e. Appendix E: Interconnections Table and Points of Contact	*Interconnection information will be critical for system restoration.* *Connections must be restored, per the BIA.* *Considerations must be made to recover connectivity from any alternate processing facility approved in the recovery strategies analysis for the system to be recovered as well as an alternate processing facility to which the other systems may have migrated as a result of the incident that caused the disaster declaration.*
f. Appendix F: Exercises and Plan Maintenance	*An ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities. Each CP will be exercised at least annually (e.g. every 365 days) to ensure plan accuracy and executability.*[8]
g. Appendix G: Critical Recovery Metrics	*The recovery metrics to be included are: WRTs and MTDs of all functions supported by the system, RTO of the system, RPO of the data processed, stored, or transmitted by the system.*

[8] See ARS control CP-4 and RMH Vol II procedure 4.5 for CP Exercise procedures.

3 APPROVED

Teresa Fryer

Digitally signed by Teresa Fryer
DN: cn=Teresa Fryer, o, ou, email=teresa.fryer@cms.hhs.gov, c=US
Date: 2014.11.13 13:44:23 -05'00'

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at mailto:ciso@cms.gov.

The signature of the CMS Chief Information Security Officer (CISO) constitutes approval of this procedure and does not infer that the CISO must sign off on each individual CP Exercise.

(This Page Intentionally Blank)