Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS INFORMATION SECURITY (IS) CERTIFICATION & ACCREDITATION (C&A) PACKAGE GUIDE

August 25, 2009

Version 1.0 – Draft

SUMMARY OF CHANGES

The Summary of Changes in the *CMS Information Security (IS) Certification & Accreditation (C&A) Package Guide* version 1.0, dated August 20, 2009 is provided below:

1. This document replaces in its entirety the *CMS Information Security (IS) Certification & Accreditation (C&A) Template*, v1.0, dated May 12, 2005 with the *CMS Information Security (IS) Certification & Accreditation (C&A) Package Guide*, v1.0, dated July 16, 2009.

2. The structure throughout the document is modified to reflect the current requirements for assembling information security artifacts in a universal manner to facilitate certification/accreditation reviews of the C&A package. The required sections of the C&A package are identified to provide the Business Owners and System Developers/Maintainers with this standard CMS approach.

3. Formatting modifications were made throughout the document to support compliance to Section 508.

EXECUTIVE SUMMARY

The *CMS Information Security (IS) Certification & Accreditation (C&A) Package Guide* hereinafter known as "The Guide" replaces in its entirety the *CMS Information Security (IS) Certification & Accreditation (C&A) Template*, v1.0, dated May 12, 2005.. The Guide supports the *CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedure*, and is provided to standardize the submission of C&A packages from CMS Business Owners and System Developers/Maintainers.

The CMS IS C&A Program Procedure covers six (6) distinct phases to form a continuous security management practice for all CMS systems/applications. Business Owners of systems that are already in production, or are currently accredited, may only need to address the final phase of the C&A Program, which defines activities performed during maintenance of the system and for periodic re-accreditation.

The C&A package submitted by Business Owners and System Developers/Maintainers is comprised of distinct elements positioned in a distinct sequence. This guide provides the elements and sequence for a certified C&A package submitted to the CMS Chief Information Officer (CIO) for accreditation of a CMS system. Each C&A package shall contain the following elements:

- C&A Package Cover Memo
- Table of Contents
- Executive Summary
- Security Certification Form
- System Security Plan (SSP)
- Information Security Risk Assessment (IS RA)
- Contingency Plan (CP)
- Test of the CP
- Security Test & Evaluation (ST&E) Report
- Plan of Action and Milestones (POA&M)
- Supporting Documentation

The Guide is comprised of sequence instructions, boiler plate samples, and reference pointers to the CMS information security procedures and templates that support elements of the C&A package. The Business Owner and System Developer/Maintainer are expected to follow the corresponding procedures and templates prior to the submission of the C&A package for certification and accreditation.

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1 PURPOSE 1
1.2 BACKGROUND 1
1.3 SCOPE 1
1.4 HOW TO USE THIS DOCUMENT 1

2. OVERVIEW 2
2.1 C&A PACKAG ELEMENTS AND TAB LOCATIONS 2
2.2 C&A PACKAGING 2
2.3 C&A PROGRAM DOCUMENTS 3

3. C&A PACKAGE ELEMENTS 3
3.1 CERTIFICATION COVER MEMO 3
3.2 EXECUTIVE SUMMARY 5
3.3 TABLE OF CONTENTS 5
3.4 TAB A – SECURITY CERTIFICATION FORM 6
3.4.1 Required Signatures 6
3.4.2 Boilerplate Security Certification Form 7
3.5 TAB B – SYSTEM SECURITY PLAN 11
3.6 TAB C – INFORMATION SECURITY RISK ASSESSMENT 11
3.7 TAB D – CONTINGENCY PLAN 11
3.8 TAB E – TEST OF THE CONTINGENCY PLAN 11
3.9 TAB F – SECURITY TEST & EVALUATION 11
3.10 TAB G – PLAN OF ACTION AND MILESTONES 12
3.11 TAB H – SUPPORTING DOCUMENTATION 12

1. INTRODUCTION

1.1 PURPOSE

The *Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Certification & Accreditation (C&A) Package Guide* hereinafter known as "The Guide" provides CMS Business Owners and System Developers/Maintainers with the necessary information and instructions for assembling and submitting a CMS C&A package for system certification/accreditation (or recertification/reaccreditation).

1.2 BACKGROUND

The CMS is responsible for implementing and administering an IS program to protect its information resources in compliance with applicable laws, regulations, and Executive Orders. The *CMS Information Security (IS) Certification & Accreditation Program Procedure* provides a high-level overview of this program and covers six (6) distinct phases to form a continuous security management practice for all CMS systems/applications. Business Owners of systems that are already in production, or are currently accredited, may only need to address the final phases of the C&A Program, which defines activities performed during maintenance of the system and for periodic re-accreditation. This document replaces in its entirety the *CMS Information Security (IS) Certification & Accreditation (C&A) Template,* v1.0, dated May 12, 2005. The Guide supports the CMS IS C&A Program and is provided to standardize the submission of C&A packages from CMS Business Owners and System Developers/Maintainers.

1.3 SCOPE

The Guide applies to all CMS Business Owners and System Developers/Maintainers that own, develop, and/or maintain a CMS System or a system performing work on behalf of CMS. All personnel tasked with submitting a C&A package for certification/accreditation (or recertification/reaccreditation) should read this document to become familiar with the CMS C&A package elements and pre-defined Tabular (TAB) sequence for package acceptance and further submission to the CMS Chief Information Officer (CIO) through the CMS Chief Information Security Officer (CISO).

1.4 HOW TO USE THIS DOCUMENT

The Guide provides instruction for each element of the C&A package and is described and presented in the required sequence. In some instances, sample letters and forms are provided that must be tailored to meet the specifics for the system that is being proposed for certification/accreditation.

2. OVERVIEW

The CMS IS C&A Program is an essential part of the CMS enterprise-wide IS Program. A CMS IS C&A package is submitted by the Business Owner to the CIO through the CISO for making an accreditation decision also known as an Authority to Operate. The authorization, in writing by the CIO, is required for the operation of an information system prior to full implementation and whenever significant changes in the system are affected. This is a key component of the CMS IS C&A Program. The CMS IS C&A Program Procedure provides the Business Owner and System Developer/Maintainer with a high-level overview for preparing the necessary documentation to demonstrate and to validate that appropriate security controls exist to safeguard the system.

2.1 C&A PACKAG ELEMENTS AND TAB LOCATIONS

The C&A package submitted by Business Owners and System Developers/Maintainers is comprised of distinct elements with a pre-defined sequence. Each C&A package submitted for acceptance and further submission for certification/accreditation will contain the elements in the defined sequence described in Table 1.

Table 1: CMS C&A Package Elements and Sequence

Sequence	TAB	C&A Package Elements
1st		Certification Cover Memo
2nd		Executive Summary
3rd		Table of Contents
4th	**A**	Security Certification Form
5th	**B**	System Security Plan (SSP)
6th	**C**	Information Security Risk Assessment (IS RA)
7th	**D**	Contingency Plan (CP)
8th	**E**	Test of the Contingency Plan
9th	**F**	Security Test & Evaluation (ST&E) Report
10th	**G**	Plan of Action and Milestones
11th	**H**	Supporting Documentation

2.2 C&A PACKAGING

The C&A package should be submitted using file dividers to separate the package. Three ring binders, preferably white, should be used to contain the C&A package and, when multiple binders are needed, the binders need to be labeled by Books (e.g., Book 1 of 3, Book 2 of 3, and Book 3 of 3) and include the name of the system on the cover and spine of each book. The table of contents included as part of the C&A package will delineate the contents of each book submitted. The Business Owner and System Developer/Maintainer are also required to submit an electronic copy (i.e., CDs) of the C&A package elements. (It should be noted that due to the size of the baseline configurations that must be submitted as part of the SSP, this information only needs to be submitted in electronic format and not in hardcopy.)

2.3 C&A PROGRAM DOCUMENTS

To manage a risk-based IS Program; Business Owners are responsible for executing the processes defined in detail in the CMS IS C&A Program documents which can be located at the **Info Security Library** navigation key of CMS IS "Virtual Handbook" website, http://www.cms.hhs.gov/informationsecurity/. The Business Owner and System Developers/Maintainers are expected to have followed the relevant IS procedures and templates prior to the submission of the C&A package. The procedures and templates are provided below.

C&A Package Element	IS Program Procedure	IS Program Template
SSP	*CMS System Security Plan (SSP) Procedure*	*CMS System Security Plan (SSP) Template*
IS RA	*CMS Information Security Risk Assessment (IS RA) Procedure*	*CMS Information Security Risk Assessment (IS RA) Template*
CP	*CMS Information Security (IS) Application Contingency Plan (CP) Procedure*	*CMS Information Security (IS) Application Contingency (CP) Plan Template*
Test of the CP	*CMS Contingency Planning Tabletop Test Procedure*	*Appendix B – CP Tabletop Test Plan Template*
ST&E	*CMS Information Security (IS) Assessment Procedure*	*CMS Information Security (IS) Assessment Plan Template*
ST&E Report	*CMS IS Assessment Reporting Procedure*	*Application Assessment Findings Report Template* *Infrastructure Data Center Assessment Findings Report Template*
POA&M	*CMS Information Security (IS) Plan of Actions & Milestones (POA&M) Guide*	*Attachment A – CAP Management Worksheet* *Attachment D – CMS Information Security Policy/Standard Risk Acceptance Template*

3. C&A PACKAGE ELEMENTS

The elements of the C&A package are detailed in the sections that follow. The Business Owner and System Developer/Maintainer should follow the instructions for each element when assembling and submitting the C&A package for system certification/accreditation.

3.1 CERTIFICATION COVER MEMO

The certification cover memo is the first element of the C&A package and is completed by the Business Owner and submitted to the CMS CIO through the CMS CISO. The sample cover letter provided below contains boilerplate language as well as information that must be completed and customized for the system. The Business Owner can obtain a clean version of the Certification Cover Memo from the **Info Security Library** navigation key of the CMS IS "Virtual" Handbook located at http://www.cms.hhs.gov/informationsecurity/.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

[*Department/Organization*]

TO: Ryan Brewer, CMS Chief Information Security Officer (CISO)

FROM: [Business Owner]

SUBJECT: Certification & Accreditation (C&A) Package for [system name (system acronym)] -- ACTION

The [*Business Owner*] has completed the certification evaluation of [*system name*]. An accreditation decision for [*system name*] is requested prior to [*date*]. The attached Certification & Accreditation (C&A) Package provides to the best of my knowledge current and accurate information to facilitate an informed, risk-based accreditation decision by the Chief Information Officer.

Please find within the attached C&A Package a copy of the Certification Form, the [*system name*] SSP, IS RA, CP, Test of the CP, POA&M, the CAP, and the final Security Test & Evaluation Report dated [mm\dd\yyyy] prepared by [*CMS C&A Evaluator*]. I am available to discuss any questions regarding our compliance with the *CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedure* including the ST&E. Please contact [*name*] of [*organization*] at [*phone number*] if you require a meeting.

Attachment

cc: Director, Enterprise Architecture & Strategy Group, OIS

3.2 EXECUTIVE SUMMARY

The Executive Summary is the second element of the C&A package. The C&A package Executive Summary is completed by the Business Owner and submitted as the next page following the Certification Cover Memo. The Business Owner provides summary information of each component of the C&A package that will assist in the certification & accreditation decision for the System. Once the Executive Summary information is developed, the Business Owner should delete the italicized wording prior to submission for certification and accreditation of the system. The C&A package Executive Summary contains summary descriptions of the following:

- The summary description of the System Security Plan (SSP) under **Tab B** is provided in this section. If more than one, provide a description of all in the Major Application (MA) family.
- The summary description of the Information Security Risk Assessment (IS RA) under **Tab C** is provided in this section. There should be one for each application in the MA family.
- The summary description of the Contingency Plan (CP) under **Tab D** is provided in this section. There should be one for each application in the MA family.
- The summary description of the Tests of the Contingency Plans under **Tab E** is provided in this section. There should be one for each application in the MA family.
- The summary description of the Security Test and Evaluation (ST&E) under **Tab F** is provided in this section. There should be separate tests for each application in the MA. If one test covered more than one application, clearly state the applications to which the test applies.
- The summary description of the Plan of Action & Milestones (POA&M) under **Tab G** is provided in this section. Provide information regarding whether the ST&E findings have been entered into the CMS POA&M database tool known as the CMS Contractor Integrated Security Suite (CISS) Tool.
- The summary description of the Supporting Documentation under **Tab H** is provided in this section. Provide information detailing the supporting documentation used to assist in the certification/accreditation of the system.

3.3 TABLE OF CONTENTS

The Table of Contents is the third element of the C&A package and will list the elements and TAB references. The format of the table of contents provided in the C&A package should be presented in tabular format and contains the C&A package element and associated TAB reference. Table 2 is a sample table of contents that is created manually and contains the required elements.

Table 2 - Sample Table of Contents

CMS C&A PACKAGE ELEMENTS	TAB REFERENCE
INFORMATION SECURITY CERTIFICATION PACKAGE COVER MEMO	
EXECUTIVE SUMMARY	
CMS INFORMATION SECURITY CERTIFICATION FORM	A
SYSTEM SECURITY PLAN (SSP)	B
INFORMATION SECURITY RISK ASSESSMENT (IS RA)	C
CONTINGENCY PLAN (CP)	D
TEST OF THE CONTINGENCY PLAN (CP)	E
SECURITY TEST & EVALUATION (ST&E)	F
PLAN OF ACTION & MILESTONES (POA&M)	G
SUPPORTING DOCUMENTATION	H

3.4 TAB A – SECURITY CERTIFICATION FORM

The Business Owner must position the CMS Certification Form as **TAB A** of the C&A package. It should be noted that the certification form is for the entire contents of the C&A package and individual certifications for each element is not required, A sample Security Certification Form is provided with boilerplate language and placeholders for information that should be completed and customized to support the system for certification/accreditation. The Security Certification Form should be completed as follows:

1. Select the reason(s) certification is required.
2. Indicate the name of the System.
3. Indicate the CMS Component.
4. Provide the printed Name, Date, and Signature of the CMS Component Information System Security Officer (ISSO).
5. Include the boilerplate language.
6. Provide the printed Name, Date, and Signature of the Certification Official (Executive).
7. Provide the printed Name, Date, and Signature of the Business Owner.
8. Provide the printed Name, Date, and Signature of the System Developer/Maintainer.
9. Complete the Security Certification Restrictions section and indicate any restrictions.
10. Complete the Security Certification Actions section and indicate any actions.

3.4.1 REQUIRED SIGNATURES

The signature titles identified on the Security Certification Form shall not be altered. The titles and only those titles listed in Table 3 shall be indicated on the Security Certification Form.

Table 3 – Security Certification Form Required Signature Titles

REQUIRED SIGNATURE TITLE	DESCRIPTION
Certification Official (Executive)	CMS Office or Center Director of the business function.
Business Owner	CMS Group Director for the business function.
System Developer/Maintainer	CMS Division Director that does this activity whether through a contract or with CMS staff.
CMS Component ISSO	CMS individual in the Business Owner's component.

3.4.2 BOILERPLATE SECURITY CERTIFICATION FORM

The Business Owner must ensure the Security Certification Form is completed to support the system being considered for certification/accreditation and recertification/reaccreditation. The Business Owner should retrieve a clean Security Certification Form from the **Info Security Library** navigation key of the CMS IS "Virtual" Handbook located at http://www.cms.hhs.gov/informationsecurity/. A boilerplate Security Certification Form is provided on pages 8 through 10.

CMS Security Certification Form

Certification is required for the following reason(s):	Selected Reason(s)
• New System • Major system modification • Increased system data sensitivity level • Serious security violation • Changes in the threat environment • Expired Accreditation	

Name of System

CMS Component

(printed name)_____ (signature) _____
CMS Component Information System Security Officer (ISSO) **Date**

The signatures below attest that the appropriate technical certification evaluations have been conducted successfully.

I, the Business Owner/Manager, have examined the controls implemented for this system and consider them adequate to meet agency policy and the relevant business requirements. I also understand and accept the risk inherent in processing on a network or at the installation(s) that supports this system, particularly where the support system is operated outside of my management control. This certification is based on the documented results of the design reviews, system test, and the recommendations of the testing teams.

(printed name)_____ (signature) _____
Certification Official (Executive) **Date**

(printed name)_____ (signature) _____
Business Owner **Date**

(printed name)_____ (signature) _____
System Developer / Maintainer **Date**

Security Certification Restrictions
Certification is granted with the following restrictions (use additional pages if necessary):

Security Certification Actions
The following specific actions are to be completed by the dates indicated (use additional pages if necessary):

3.5 TAB B – SYSTEM SECURITY PLAN

The Business Owner must position the System Security Plan (SSP) as **TAB B** of the C&A package. If more than one system, provide all that are included for this submission. The Business Owner will follow the *CMS System Security Plan (SSP) Procedure* for completing the *CMS System Security Plan (SSP) Template.*

3.6 TAB C – INFORMATION SECURITY RISK ASSESSMENT

The Business Owner must position the Information Security Risk Assessment (IS RA) as **TAB C** of the C&A package. The Business Owner will follow the *CMS Information Security Risk Assessment (IS RA) Procedure* in completing the *CMS Information Security Risk Assessment (IS RA) Template.*

3.7 TAB D – CONTINGENCY PLAN

The Business Owner must position the Contingency Plan (CP) as **TAB D** of the C&A package. The Business Owner will use the *CMS Information Security (IS) Application Contingency Plan (CP) Procedure* in completing the *CMS Information Security (IS) Application Contingency (CP) Plan Template.* General Support Systems shall follow the Contingency Plan procedures and template identified in the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems.*

3.8 TAB E – TEST OF THE CONTINGENCY PLAN

The Business Owner must position the Test of the Contingency Plan (CP) as **TAB E** of the certification package. The Business Owner will use the *CMS Contingency Planning Tabletop Test Procedure* and complete *Appendix B – CP Tabletop Test Plan Template.* General Support Systems shall follow the CP procedure and template identified in NIST SP 800-34.

3.9 TAB F – SECURITY TEST & EVALUATION

The Business Owner must position the results of the Security Test & Evaluation (ST&E) as **TAB F** of the C&A package. After completing the certification evaluation, the CMS C&A Evaluator shall produce an ST&E Report, which will form part of this C&A package. The test findings shall be documented in the report after the onsite and, if required, offsite testing has been completed. The ST&E Report shall be made available to the CMS Government Task Lead and the Business Owner for review prior to final assembly of the C&A package. The Business Owner will ensure the C&A Evaluator is provided with the CMS procedures and templates to perform and document the ST&E. Specifically, the C&A Evaluator will use the *CMS Information Security (IS) Assessment Procedure, CMS Information Security (IS) Assessment Plan Template, CMS IS Assessment Reporting Procedure,* and as applicable either the *Application Assessment Findings Report Template or Infrastructure Data Center Assessment Findings Report Template.*

- Determine the actual level of effort to perform the ST&E
- Identify specific resources needed for the ST&E effort

- Prepare a detailed work and test plan for the ST&E activities

3.10 TAB G – PLAN OF ACTION AND MILESTONES

The Business Owner must position the POA&M as **TAB G** of the C&A package. The POA&M and its supporting processes enhance CMS' ability to identify, assess, prioritize, and monitor the progress of corrective actions pertaining to information security weaknesses found within programs and systems. Any identified IT finding from any source whether it is an audit, annual security control testing (SCT), ST&E, accreditation actions or any other test that identifies an IS weakness must be entered into the POA&M reporting and corrective action process. The Business Owner will use the *CMS Information Security (IS) Plan of Actions and Milestones Guide in completing Attachment A – Corrective Action Plan Management Worksheet and Attachment D – CMS Information Security Policy/Standard Risk Acceptance Template* for entering into the CMS Integrated Security Suite (CISS) tool.

3.11 TAB H – SUPPORTING DOCUMENTATION

The Business Owner must position any additional Supporting Documentation as **TAB H** of the certification package. The supporting documentation is optional and should contain relevant documents and checklists that the Business Owner believes will assist in the certification/accreditation decision for the system.

C&A Checklist
The C&A Checklist is provided as part of the Supporting Documentation – TAB H. The C&A Checklist is a tool provided to the Business Owner to document the C&A activities for the System. ***This checklist is optional for the Business Owner to complete but can be helpful in providing validation of following the C&A process when audited or reviewed.***

C&A ACTIVITY STEPS	DATE COMPLETED	COMPLETED BY
PHASE 1: PRE-CERTIFICATION		
Task 1-Business Risk Identification		
1. Include C&A resources in IT investment request		
2. Identify anticipated system security level by information type		
3. Initiate IS RA development		
4. Identify business risk		
PHASE 2: INITIATION		
Task 2-Certification Preparation		
1. Prepare C&A project plan indicating proposed schedule, resources and key milestones		
2. Continue IS RA development		
3. Initiate SSP development		
4. Fully characterize the system in the SSP		

C&A ACTIVITY STEPS	DATE COMPLETED	COMPLETED BY
5. Identify system security level by information type		
6. Identify risks in the IS RA		
7. Evaluate controls in the applicable SSP Workbook		
8. Evaluate residual risks		
9. Prepare IS artifacts		
Task 3-ST&E Resource Identification		
1. Determine ST&E required resources 2. Notify ST&E participants		
Task 4-IS Artifacts Analysis, Update and Acceptance		
1. Independent review of the Security Categorization (System Security Level by Information Type)		
2. An independent analysis of the IS artifacts, e.g., IS RA, SSP, CP etc.		
3. Update IS artifacts as needed		
PHASE 3: SECURITY CERTIFICATION		
Task 5-Security Control Assessment		
1. Prepare for the assessment		
2. Negotiate the RoE		
3. Conduct the assessment		
4. Document the results		
Task 6-Security Certification Documentation		
1. Provide the ST&E findings and certification recommendations to the Business Owner		
2. Update the IS artifacts as needed		
3. Prepare the POA&M based on the ST&E findings		
4. Prepare the Business Owner Certification		
PHASE 4: SECURITY ACCREDITATION		
Task 7-Accreditation Decision		
1. Assemble the C&A package according to C&A Template		
2. Determine if the agency-level risk is acceptable		
3. Prepare accreditation recommendations		
4. Submit C&A package to CIO		
5. Business Owner C&A briefing to CIO		
6. Sign Accreditation Letter or IATO		
Task 8-C&A Package Distribution		
1. Distribute the C&A package to the Business Owner		
2. Update the SSP with the latest information from the accreditation decision		
PHASE 5: MAINTENANCE		
Task 9-Continuous Monitoring		
Configuration Management and Change Control		

C&A ACTIVITY STEPS	DATE COMPLETED	COMPLETED BY
1. Authorize and document the proposed or actual changes to the information system		
2. Determine the impact of proposed or actual changes on the security of the system		
3. Submit CAPs in quarterly POA&M		
Security Control Testing		
1. Select an appropriate set of security controls to be tested		
2. Annually assess the selected controls using standard procedures and techniques		
Task 10-Documentation and Status Reporting		
1. Update the IS artifacts		
2. Update the POA&M		
3. Report the C&A metrics to the CISO		
Task 11-Re-Accreditation Triggering		
1. Re-execute tasks 2-8		
2. Submit C&A Package		
PHASE 6: DISPOSITION		
Task 12-Develop System Disposition Plan		
1. Develop a System Disposition Plan		
2. Verify that software/applications have not been compromised		
3. Archive or transfer data, software components, life cycle documents and artifacts		
Task 13-Dispose of Equipment		
1. Ensure that equipment is disposed of in accordance with the System Disposition Plan		
Task 14-Conduct a Disposition Review		
1. Conduct a disposition review		
2. Document the lessons learned from the shutdown and archiving of the terminated system		

End of Document