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

Risk Management, Oversight, And Monitoring

Standard:

CMS Information Security Acceptable Risk Safeguards (ARS),

CMS Minimum Security Requirements (CMSR)

FINAL
Version 2.0
September 20, 2013

Document Number: CMS-CIO-STD-SEC01-2.0

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN ARS VERSION 2.0, SEPTEMBER 20, 2013

1. This version reflects the updates in response to changes required due to:
   a. Changes in National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Revision (R) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

SUMMARY OF CHANGES IN ARS VERSION 1.5, JULY 31, 2012

1. This version reflects the updates in response to changes required due to:
   a) Changes in NIST special publications mandated by Federal Information Processing Standards (FIPS) 200, and changes to the *HHS-OCIO Policy for Information Systems Security and Privacy* and *HHS-OCIO Policy for Information Systems Security and Privacy Handbook*.
   b) Changes mandated under *Federal Risk and Authorization Management Program (FedRAMP)* minimum control requirements, as required by Office of Management and Budget (OMB) Memorandum for Chief Information Officers dated December 8, 2011, *Security Authorization of Information Systems in Cloud Computing Environments*.
   c) Moved remaining e-authentication guidance and direction from Appendix D to Risk Management Handbook (RMH), Volume III, Standard 3.1, *CMS Authentication Standards*.
   d) Updated references to the *CMS Integrated Life Cycle Framework (ILC)* to the new *CMS eXpedited Life Cycle (XLC)*.
   e) Removed specific control *Applicability(s)* from each CMS Minimum Security Requirements (CMSR) control, and removed related discussions within the Acceptable Risk Safeguards (ARS).

SUMMARY OF CHANGES IN ARS VERSION 1.0, APRIL 23, 2010

1. Renumbered to Version 1.0 for consistency with Internet Only Manual (IOM) versioning.
   f) Version 1.0 reflects the updates from the NIST SP 800-53 Revision 3, dated August 2009.

SUMMARY OF CHANGES IN ARS VERSION 4.0, MARCH 19, 2009

1. This document is available at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/ as a clean copy. Because version 4.0 contains significant changes in both format and organization, no redline version of this document is supplied to indicate changes from the prior version.
2. The bulk of the changes in this version of the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) reflect a change in the way the CMS controls are organized. For those familiar with the CMS Core Security Requirements (CSRs) the organization of this document is similar.
   a) Organizationally defined variables and security requirement enhancements are identified. All organizationally defined variables and enhancements (enhancements that included a CMS- in the identifier) are now identified as implementation standards (see Section 5.2.3).
   b) Control requirements were moved from the main body of this document to Appendices A, B, and C. E-Authentication control requirements are based on the CMSR IA-2 with the implementation of the appropriate e-Authentication Standards contained in Appendix D. Security control requirements for each security level are maintained in a separate appendix. Within each appendix, supplementary information for each control requirement (guidance, implementation standards, applicability, references, related security control requirements, and assessment procedures) has been added for each control requirement.

   c) Updated the entire document to change references to the CMS ARS controls to the new CMSR term. Section 2 of this document describes what the CMSR are and the purpose of the minimum security requirements.
   d) Updated the previous E-Authentication appendix references to account for moving the CMS E-Authentication Standards to Appendix D and for document reformatting for 508 compliance.
3. Introduction (Section 1) - Updated to change references to the CMS ARS controls to the new CMSR term.
4. Purpose (Section 2) - Updated to expand and clarify scope, responsibilities, and applicability of this manual.
5. How To Use The Appendices (Section 4) – Reordered this section to precede CMSR structure section. Modified and updated to reflect the new structure and format of the CMSRs.
   a) Updated the How to Use this Document section to incorporate the above changes. Removed the Notes subsection text, which was moved to other sections.
6. CMSR Structure (Section 5) – Modified and updated to reflect the new structure and format of the CMSRs:
   a) Changed “Standards Numbering Schema” section title to “CMSR Structure” and revised the section text
   b) Added and adjusted text to describe additional CMSR elements.
   c) References (Section 6) – Added References section to consolidate all references to a single location.
   d) Removed Control Requirements (ARS version 3.1, sections 1 through 17) and moved to new Appendices A, B, and C. Added supplementary data described in Section 5 and moved E-Authentication standard in Appendix A to Appendix D.
7. Old Appendix A, *e-Authentication Standards*, move to Appendix D: *CMS e-Authentication Standards*. Former Appendices B and C were deleted and replaced with updated Appendices A, B, and C (CMSRs), respectively.
8. Control Requirement Changes:
   a) Added control elements described in Section 5 (including Baseline controls from *CMS Policy for the Information Security Program*, Implementation Standards, Guidance, Applicability, References, related control requirements, and Assessment Procedures.)
   b) Added implementation standards based on CMS management guidance, Health Insurance Portability and Accountability Act (HIPAA), and Internal Revenue Service (IRS) 1075, as indicated below.
   c) Moved all CMS-specific control enhancements (indicated with a “CMS-” in the previous version 3.1) to integrate with applicable baseline controls as “implementation standards”. All text of these requirements was maintained unchanged except as indicated below.
9. Global change - All references to the “*ARS Appendix A for e-Authentication*” have been changed to “the *e-Authentication Standards*” Appendix D.
   a) The following ARS enhancements were removed and/or integrated with other CMSR implementation standards: AU-2(0), CA-6(0), CP-5(0), and IA-4(CMS-2).
10. AC-18
   a) HIGH, MODERATE, and LOW: Added AC-18.Std.2 to provide additional guidance for wireless devices. This was AC-18(DIR-1).
11. AC-20
   a) HIGH and MODERATE: Added AC-20.Std.2 for additional guidance when handling Federal Tax Information (FTI).
12. AU-2
   a) HIGH, MODERATE, and LOW: AU-2.Std.2 (from AU-2(CMS-1)) – Modified for clarity
   b) HIGH, MODERATE, Std.2 Remove duplicate items (d) and (h) and renumbered the bullets.

c) MODERATE: Added AU-2.Std.4 for clarity.

13. AU-6
    a) HIGH and MODERATE: Added AU-6.Std.7 for additional guidance when handling FTI.
14. AU-11
    a) HIGH and MODERATE: Added AU-11.Std.2, AU-11.Std.3, and AU-11.Std.4 for additional guidance when handling Personally Identifiable Information (PII).
15. CA-6
    a) HIGH, MODERATE, and LOW; CA-6(0) removed as it was a duplicate of the base control.
16. CM-2 Std. 1 Changed year to 365 days
17. CP-5 Enhancement (0) removed as it repeats the base requirement.
18. CP-7
    a) HIGH and MODERATE: CP-7.Std.1 (from CP-7(0)) – Modified to read “within one week”.
19. CP-8
    a) HIGH and MODERATE: CP-8.Std.1 (from CP-8(0)) – Modified to read “within one week”.
20. CP-9
    a) HIGH Std.1 changed values “full backups every other day” to “incremental or differential backups daily and a full backup once a week.” This allows effective time utilization for backup completion and is cost effective while protecting CMS systems and data.
    b) HIGH and MODERATE: Added CP-9.Std.2 for additional guidance when handling PII.
21. IA-2
    a) HIGH, MODERATE, and LOW: IA-2.Std.1 (from IA-2(CMS-1)) – Modified for clarity.
22. IA-4
    a) CMS-2 Deleted.
23. IA-5
    a) HIGH, MODERATE, and LOW: IA-5.Std.1 (from IA-5(0)) – Reworded for clarity and adjusted restriction values and periodicity for each level.
24. MA-2
    a) HIGH and MODERATE: Added MA-2.Std.1 for additional guidance when handling PII.
25. MP-1
    a) HIGH and MODERATE: Added MP-1.Std.1 for additional guidance when handling PII.
26. MP-4
    a) HIGH and MODERATE: Added MP-4.Std.1 and MP-4.Std.2 for additional guidance when handling PII.
27. MP-5
    a) HIGH and MODERATE: Added MP-5.Std.1 for additional guidance when handling PII.
    b) HIGH and MODERATE: Added MP-5.Std.2 for additional guidance when handling FTI.
28. MP-5(1)
    a) HIGH and MODERATE: Changed “tamper proof” to “tamper evident.” The change is to more clearly convey that the recipient needs to be able to identify if it had been opened prior to receipt not that it prevents tampering.
29. MP-6
    a) HIGH and MODERATE: Added MP-6.Std.3 for additional guidance when handling FTI.
    b) HIGH and MODERATE: Added MP-6.Std.4 HIGH, MODERATE, and LOW.
30. MP-CMS-1
    a) HIGH and MODERATE: MP-CMS-1.Std.1 (from MP-CMS-1(CMS-0)) – Modified for clarity.

31. PE-2
    a) HIGH and MODERATE: Added PE-2.Std.2 for additional guidance when handling PII.
32. PE-3
    a) HIGH, MODERATE, and LOW: Added PE-3.Std.4 for clarity. Was PE-3(DIR-1)
    b) HIGH and MODERATE: Added PE-3.Std.5 for additional guidance when handling PII.
33. PL-2
    a) HIGH and MODERATE: Added PL-2.Std.1 for additional guidance when handling Personal Health Information (PHI).
    b) HIGH and MODERATE: Added PL-2.Std.2 and PL-2.Std.3 for additional guidance when handling FTI.
    c) HIGH, MODERATE and LOW – Removed PL-2(CMS-1) as it duplicated the requirements of the base CMSR PL-2.
34. PS-3
    a) HIGH, MODERATE and LOW: Modified PS-3.Std.2 (from PS-3(CMS-1)) – Added “appropriate” to text.
35. PS-4
    a) HIGH and MODERATE: PS-4.Std.1 (from PS-4(CMS-1)) – Deleted “and system access” from text.
36. RA-5
    a) HIGH, MODERATE and LOW Std. 2 change from once a year to once every 365 days.
37. SA-1
    a) HIGH and MODERATE: Added SA-1.Std.1 for additional guidance when handling FTI.
38. SA-9
    a) HIGH and MODERATE: Added SA-9.Std.2 for additional guidance when handling PHI.
39. SC-4
    a) HIGH and MODERATE: Added SC-4.Std.2 for additional guidance when handling PII.
40. SC-9
    a) HIGH and MODERATE: Added SC-9.Std.1 for additional guidance when handling PII.
41. SC-10
    a) HIGH, MODERATE, and LOW: SC-10.Std.1 (from SC-10(0)) – Modified parameter to “thirty (30) minutes”.
42. SI-2
    a) HIGH: SI-2.Std.1 (from SI-2(0)) – Modified parameter to “seventy-two (72) hours”.

SUMMARY OF CHANGES IN ARS VERSION 3.1, APRIL 24, 2008

1. This document is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/ as either a clean copy or as a markup copy enabling those individuals who were very familiar with version 3.0 of the ARS to quickly scan for and identify the substantive changes, which have been made to the document in version 3.1.
2. The bulk of the changes in this version of the CMS Information Security (IS) ARS reflect revisions in the organizationally defined variables to align with CMS current processes and to correct typographical errors from version 3.0.
3. Global change – “annually” or “annual” to “every 365 days” to reflect the OMB decision on the definition of the terms.
    a) Section 1, AC-2 changed to the following:,
    b) Control 0 LOW – Review information system accounts every 365 days.

c) Control 0 MODERATE – Review information system accounts every 180 days.

d) Control 0 HIGH – Review information system accounts every 90 days.

e) Control 2 MODERATE and HIGH – Configure the information system to allow emergency account for a period of time Not to Exceed (NTE) 24 hours and to allow accounts with a fixed duration (i.e., temporary accounts) NTE 365 days.

f) Control 3 LOW – Configure the information system to disable inactive accounts automatically after 365 days.

g) Control 3 MODERATE – Configure the information system to disable inactive accounts automatically after 180 days.

h) Control 3 HIGH – Configure the information system to disable inactive accounts automatically after 90 days.

4. Section 1, AC-7 changed to the following:
   a) Control 0 LOW – Configure the information system to disable access for at least five (5) minutes after three (3) failed log-on attempts by a user during a five (5) minute time period.
   b) Control 0 MODERATE – Configure the information systems to lock out the user account automatically after three (3) failed log-on attempts by a user during a fifteen (15) minute time period . Require the lockout to persist for a minimum of one (1) hour.
   c) Control 0 HIGH – Configure the information systems to lock out the user account automatically after three (3) failed log-on attempts by a user during a one (1) hour time period . Require the lockout to persist for a minimum of three (3) hours.
5. Section 1, AC-10, Control CMS -1 changed to -- The requirement and use of more than one (1) application/process session for each user is documented in the System Security Plan.
6. Section 1, AC-11, Control 0 – changed “desktop access” to “local access”.
7. Section 1, AC-12, changed to the following:
   a) Control 0 –”fifteen (15) minutes of inactivity” to “thirty (30) minutes of inactivity.”
   b) Control 1 – Removed from MODERATE and retained only at the HIGH level
8. Section 3, AU-11 Control 0 – for clarity the word “audit” was added in front of “records” and “record”.
9. Section 4, CA-5 Control 0 – the update requirement for the POA&M was changed from “every three (3) months” to “monthly.”
10. Section 5, CM-7 Control 0 changed to “Configure the information system to provide only essential capabilities and services by disabling all system services, ports and network protocols that are not explicitly required for system and application functionality. A list of specifically needed services, ports, and network protocols will be maintained and documented in the security plan; all others will be disabled.”
11. Section 7, IA-4 Control 0 changed to the following:
    a) LOW – Disable user identifiers after 365 days of inactivity and delete disabled accounts during the annual recertification process.
    b) MODERATE – Same as LOW except after 180 days of inactivity.
    c) HIGH – Same as LOW except after 90 days of inactivity.
12. Section 11, PE-2 Control 0 changed to the following:
    a) LOW – Review and approve list of personnel with authorized access to facilities containing information systems at least once every 365 days.
    b) MODERATE -- Review and approve list of personnel with authorized access to facilities containing information systems at least once every 180 days.
    c) HIGH -- Review and approve list of personnel with authorized access to facilities containing information systems at least once every 90 days.
13. Section 13, PS-6 Control 0 changed to “Access agreements are reviewed and updated as part of the system accreditation or when a contract is renewed or extended.”
14. Section 14, RA-5 Control 0 changed “quarterly” to “90 days.”

15. Section 16, SC-5 Control 0 – added URLs for the SANS and NIST references.
16. Section 17, SI 6 Control 0 and 1 – MOVE to HIGH only and state "Not Required" under MODERATE.
17. Section 17, SI-7 changed to the following:
    a) Control CMS-1 removed.
    b) "Not Required" inserted for LOW.
    c) Control 1 – Removed from MODERATE and HIGH language changed to "Perform weekly integrity scans of the system."
    d) Control CMS-2 moved to Section 16, SA-11.

SUMMARY OF CHANGES IN ARS VERSION 3.0, SEPTEMBER 19, 2007

1. This document is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/ as either a clean copy or as a markup copy enabling those individuals who were very familiar with version 2.0 of the ARS to quickly scan for and identify the substantive changes, which have been made to the document in version 3.0.
2. The bulk of the changes in this version of the CMS Information Security (IS) ARS reflect the new standards to which CMS must comply as established by the NIST SP 800-53 Revision 1, Recommended Security Controls for Federal Information Systems, dated December 2006. Additional changes have been made in order to comply with new directives and guidance from the OMB, the Department of Health and Human Services (DHHS) and industry best practices.
3. Global change – "System Owner" is now "Business Owner"
4. Global change – "service category" is now "control family".
5. References to "ARS Category" changed to "ARS Family" for all ARS 3.0 references.
6. The introductory text at the beginning of each control family has been aligned to the definitions for the 17 security-related areas in the FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 9, 2006.
7. The appendices have been rearranged for ease of use.
    a) Appendix A, Standards Category Classification has been moved to Appendix B and renamed "Standards Family Classification".
    b) Appendix B, Standards Redistribution, has been moved to Appendix C and renamed Historical Log of ARS Standards Redistribution.
    c) Appendix C, E-Authentication, has been moved to Appendix A, and renamed E-Authentication Standards
8. Appendix A, E-Authentication Standards, was updated for clarity and to reflect the new standards to which CMS must comply as established by changes to NIST SP 800-63, Electronic Authentication Guideline v1.0.2, dated April 2006
9. The following is a listing of the new control numbers in each control family in the CMS ARS based on the new requirements of NIST SP 800-53 Rev 1 controls.
    a) AC-12.1: Session Termination
    b) AC-17.4: Remote Access
    c) AC-18.1: Wireless Access Restrictions
    d) AC-18.2: Wireless Access Restrictions
    e) AC-20.1: Use of External Information Systems
    f) AT-5: Contacts with Security Groups and Associations
    g) AU-2.3: Auditable Events
    h) AU-5.1: Response to Audit Processing Failures
    i) AU-5.2: Response to Audit Processing Failures

j) AU-7.1: Audit Reduction and Report Generation
k) AU-8.1: Time Stamps
l) CA-4.1: Security Certification
m) CA-5.CMS-1: Plan of Action and Milestones
n) CA-7.1: Continuous Monitoring
o) CM-5: Access Restrictions for Change
p) CM-8: Information System Component Inventory
q) CM-8.1: Information System Component Inventory
r) CM-8.2: Information System Component Inventory
s) CP-2.2: Contingency Plan
t) CP-9.4: Information System Backup
u) IA-2.2: User Identification and Authentication
v) IA-2.3: User Identification and Authentication
w) IA-2.CMS-3: User Identification and Authentication
x) MP-5.1: Media Transport
y) MP-5.2: Media Transport
z) MP-5.3: Media Transport
aa) PE-3.1: Physical Access Control
bb) PE-4.CMS-2: Access Control for Transmission Media
cc) PE-8.2: Access Records
dd) PE-9.CMS-2: Power Equipment and Cabling
ee) PE-18: Location of Information System Components
ff) PE-18.1: Location of Information System Components
gg) PE-19: Information Leakage
hh) PL-6: Security-Related Activity Planning
ii) SA-4.1: Acquisitions
jj) SA-4.2: Acquisitions
kk) SC-7.2: Boundary Protection
ll) SC-7.3: Boundary Protection
mm) SC-7.4: Boundary Protection
nn) SC-20: Secure Name /Address Resolution Service (Authoritative Source)
oo) SC-20.1: Secure Name /Address Resolution Service (Authoritative Source)
pp) SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver)
qq) SC-21.1: Secure Name /Address Resolution Service (Recursive or Caching Resolver)
rr) SC-22: Architecture and Provisioning for Name /Address Resolution Service
ss) SC-23: Session Authenticity
tt) SI-4.5: Information System Monitoring Tools and Techniques
uu) SI-7.1: Software and Information Integrity
vv) SI-7.2: Software and Information Integrity
ww) SI-7.3: Software and Information Integrity

10. The following lists the new CMS standards, which are not based on NIST SP 800-53 Rev 1 controls and their source.
    a) AC-CMS-1: System Boot Access (Industry Best Practices)
    b) MA-CMS-1: Off-site Physical Repair of Systems (Industry Best Practices and NIST SP 800-64 Integrating Security into the System Development Life-Cycle [SDLC])

c) MA-CMS-2: On-site Physical Repair of Systems (Industry Best Practices and NIST SP 800-64 Integrating Security into the SDLC*)*

d) MP-CMS-1: Media Related Records (Industry Best Practices)

e) PS-CMS-1: Review System Access During Extraordinary Personnel Circumstances Industry Best Practices (CMS Master Security Plan and CMS Business Partners Systems Security Manual [BPSSM])

f) PS-CMS-2: Designate an Information System Security Officer (ISSO)/System Security Officer (SSO) (Industry Best Practices and CMS Handbook)

g) SC-CMS-1: Desktop Modems Industry Best Practices (CMS Master Security Plan and CMS BPSSM)

h) SC-CMS-2: Identify and Detect Unauthorized Modems (Industry Best Practices)

i) SC-CMS-3: Secondary Authentication and Encryption (Industry Best Practices)

j) SC-CMS-4: Electronic Mail (Industry Best Practices and CMS Master Security Plan)

k) SC-CMS-5: Persistent Cookies (Industry Best Practices)

l) SC-CMS-6: Network Interconnection (Industry Best Practices)

11. The following lists those former ARS standards, which have been removed as a CMS standard and have been replaced by a NIST SP 800-53 Rev 1 control.
12. CA-CMS-1: Information Sensitivity Assessment (Controls consolidated with RA-3)
    a) IA-CMS-1: Help Desk Support Procedures (Controls moved to IA-2.CMS-3)
    b) PE-CMS-1: Power Surge Protection (Controls moved to PE-9.CMS-2)
    c) PE-CMS-2: Physical Ports (Controls moved to PE-4.CMS-2)
    d) PE-CMS-3: Restrict the Use of Portable Computing Devices, formerly Handheld Personal Computers. (Controls deleted as they are included in AC-19)
13. ARS standard CP-CMS-1 has been removed as it is now covered in current CMS CP Procedures.

SUMMARY OF CHANGES IN ARS VERSION 2.0, MARCH 13, 2006

Items 1 through 5, below, reflect the changes in the CMS requirements to comply with the NIST SP 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (includes updates through 05-04-2005).

1. The following categories and/or standards within the ARS version 1.2 were removed and replaced by policy statements within the CMS Policy for the IS Program, dated May 2005:
    a) Certification and Accreditation Standards
        i) 5.1 – Assign Responsibility for Security within Each System
    b) System Access Security Standards
        i) 7.22 – User Access Administration
2. Numerous standards were added to ARS 2.0 to further comply with NIST SP 800-53 (controls and guidance) and to adhere to the DHHS policies and guidance. CMS has adopted additional standards based on CMS Policies, Procedures and Guidance; other Federal and non-Federal guidance resources and industry best practices. The following lists those standards and their sources.
    a) AC-CMS-1: System Boot Access (Industry Best Practices)
    b) CA-CMS-1: Information Sensitivity Assessment (Industry Best Practices, CMS Information System (IS) Risk Assessment (RA) Methodology and FIPS 199)
    c) CP-CMS-1: Disaster Recovery Plan Industry Best Practices, *CMS Master Security Plan and* Federal Information Security Management Act (FISMA)
    d) IA-CMS-1: Help Desk Support Procedures (Industry Best Practices, *CMS Enterprise Password Standard, and* FISMA

e) MA-CMS-1: Off-site Physical Repair of Systems (Industry Best Practices and *NIST SP 800-64 Integrating Security into the SDLC)*
f) MA-CMS-2: On-site Physical Repair of Systems (Industry Best Practices and *NIST SP 800-64 Integrating Security into the SDLC)*
g) MP-CMS-1: Media Related Records (NIST SP 800-53, Second Public Draft)
h) PE-CMS-1: Power Surge Protection (Industry Best Practices and *CMS Master Security Plan)*
i) PE-CMS-2: Environmental Controls (Industry Best Practices)
j) PE-CMS-3: Physical Ports (Industry Best Practices)
k) PE-CMS-4: Restrict the Use of Portable Computing Devices, formerly Handheld Personal Computers. (Industry Best Practices)
l) PS-CMS-1: Review System Access During Extraordinary Personnel Circumstances (Industry Best Practices, CMS Master Security Plan, and CMS BPSSM core set of security requirements (CSR) 1.1.9
m) PS-CMS-2: Designate an ISSO/SSO (Industry Best Practices and CMS Handbook)
n) PS-CMS-3: Data Ownership and Stewardship (Industry Best Practices)
o) SC-CMS-1: Desktop Modems (Industry Best Practices, *CMS Master Security Plan*, and *CMS BPSSM*
p) SC-CMS-2: Identify and Detect Unauthorized Modems (Industry Best Practices)
q) SC-CMS-3: Secondary Authentication and Encryption (Industry Best Practices)
r) SC-CMS-4: Electronic Mail (Industry Best Practices, *CMS Master Security Plan)*
s) SC-CMS-5: Persistent Cookies (Industry Best Practices)

3. Appendix A, CMS Acceptable Risk Safeguards for e-Authentication, has been added based on NIST SP 800-63 V1.0.1, *Electronic Authentication Guideline*, dated September 2004.
   a) There will be recurring old ARS standards within different categories, due to the applicability of their parts. In cases where standards recur, only the specific portions of the standard, which apply, are included within the new standard.
   b) The old ARS standards are listed in ascending order, within each category, for tracking purposes
4. The standards from the ARS, version 1.2, are redistributed throughout the new categories of this proposed ARS. The table within Appendix B, Historical Log of ARS Standards Redistribution, maps the old standards to their new name and location.
5. An explanation of the numbering scheme for the various controls was added. See the “STANDARDS NUMBERING SCHEMA”.

Items below reflect the changes in ARS version 1.2 from the original version.

6. Section 3.2, [Organizational Practice Security Standards column] “Information Sensitivity Assessment” (ISA) change to “CMS Information Security Business Risk Assessment (RA)”.
7. Section 3.2, Low, Moderate and High, change “an ISA” to “a Business RA”.
8. Section 3.2, Low, Moderate and High, remove “Section 10.5 of the”.
9. Section 3.4, Low, Moderate and High, add “or equivalent,” following “management procedures,”.
10. Section 3.14, Low, Moderate and High, add “and/or CMS SSP Methodology.” following “CMS Roadmap”.
11. Section 4.6, [Security Management Standards column], add “/SSO” following “(ISSO)”.
12. Section 4.6, Low, Moderate and High, add “/SSO” following “ISSO”.
13. Section 6.2, Low, Moderate and High, add “external communications” after “All”.
14. Section 7.3, Low and High, replace in its entirety with “Configure operating system controls to disable public read and write access to files, objects, and directories that may directly impact system functionality or performance, or that contain sensitive information.
15. Section 7.18, Moderate and High, add “highly” after “Encrypt”.

16. Section 8.2, Moderate and High, replace in its entirety with “Implement technical security measures to guard against unauthorized access to sensitive information that is being transmitted over an electronic communications network.”
17. Section 9.1, Moderate, add “and must be encrypted when residing in non-secure areas.” after “controls.”
18. Section 9.1, High, add “when residing in non-secure areas.” after “encrypted.”
19. Section 9.9, High, change “every other day” to “weekly”.
20. Section 10.6, Low, Moderate and High, add “once an incident has occurred” after “forensic evidence”.

SUMMARY OF CHANGES IN ARS VERSION 1.1, APRIL 7, 2004

1) Baseline version.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

The *Centers for Medicare & Medicaid Services (CMS) Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR)* contain a broad set of required security standards based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013, and the *HHS-OCIO Policy for Information Systems Security and Privacy*, dated July 7, 2011, and *HHS-OCIO Policy for Information Systems Security and Privacy Handbook*, dated July 7, 2011, as well as additional standards based on CMS policies, procedures, and guidance, other federal and non-federal guidance resources and industry leading security practices. This document provides guidance to CMS and its contractors as to the minimum level of required security controls that must be implemented to protect CMS' information and information systems.

Incorporating controls cataloged in this document will ensure that all CMS systems meet a minimum level of information security and privacy assurance. However, many CMS systems, particularly those that are mission-critical, or that are available to Internet users, will require additional technical security protections as part of CMS' implementation requirements such as the *CMS Technical Reference Architecture (TRA)* or any applicable *TRA Supplements.* These documents describe architecture standards that must be in place for CMS systems. Business Owners should refer to http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html to ensure that all CMS information system development architecture, design, and lifecycle requirements are met.

A system may be required to meet additional, higher-level, or more rigorous, information protection requirements as mandated by specific federal, legal, program, or accounting sources. For example, the CMSR control "Audit and Accountability" (AU) *AU-11 Audit Retention*, states that for all systems *"the audit records will be retained for ninety (90) days and then archived for one (1) year."* However, the *National Archives and Records Administration (NARA)* has determined that *"Documents relating to periodic audits of teaching facilities nationwide by carriers to recover overpayment"* (NC1-440-78-1, Item B) be retained for four (4) years after completion of an audit. Therefore, if these logs were utilized as part of such an audit, the NARA requirements would take precedence. The CMS system must be developed to meet these higher-level standards where applicable. **The ARS shall not be construed to relieve or waive these other standards.**

It is also important to note that the ARS does not address specific *business-process* requirements that ensure business requirements are fulfilled. The goal of the CMSRs is to provide a baseline of minimal internal/external information security and privacy assurance controls. It is the responsibility of the Business Owner of CMS systems, with direction provided by the Office of Information Services (OIS), to ensure that all applicable internal/external information security and privacy assurance controls are incorporated into CMS systems. Business Owners must document and certify the incorporated controls in their respective security plan and identify any risks in the corresponding risk assessment for their system.

2 PURPOSE

Protecting and ensuring the confidentiality, integrity, and availability (CIA) for all of CMS' information and information systems is the primary purpose of the information security and privacy assurance program. The ARS complies with the *CMS Policy for the Information Security and Privacy* and the *CMS Policy for the Information Security and Privacy Program*[1] by providing a defense-in-depth security structure along with a least-privilege, need-to-know basis for all information access.

The CMSRs within the ARS are not intended to be an all-inclusive list of security controls nor are they intended to replace a Business Owner's due diligence to incorporate additional controls to mitigate risk. The CMSRs are the minimum security requirements to be considered and employed where applicable throughout the risk management process and the *CMS eXpedited Life Cycle (XLC).*

3 SCOPE

All CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions and performing work on behalf of CMS shall observe the baseline policy statements described in the *CMS Policy for the Information Security and Privacy Program* and the complementary controls defined in the ARS as the minimum security requirements for all CMS information and information systems.

The Business Owner, assisted by the System Developer/Maintainer, has primary responsibility for evaluating the ARS and determining the appropriateness of the CMSRs for their system and ensuring their proper implementation.

A Business Owner may choose to strengthen the control beyond its system security level requirement to provide the best possible protection of CMS' information and information systems. In some cases, a Business Owner may not need to directly implement some specific controls as long as they can adequately demonstrate (and document) that the requirement is satisfied by a parent system.

Sometimes security controls cannot be implemented even at the minimum level due to resource issues such as funding restrictions, personnel constraints, or hardware/software limitations. Alternative or compensating controls can be implemented to reduce the risk to CMS: its information, information systems, assets, and reputation. This must be considered as part of risk management process though the CMS security assessment and authorization (SA&A) program. The alternative or compensating controls must be documented in the security plan, any remaining risk must be documented in accordance with current risk assessment procedure, and

[1] The *CMS Policy for the Information Security and Privacy Program* can be found at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

approved by the Chief Information Officer (CIO) or his/her designated representative, using appropriate policy waiver mechanisms.

4 HOW TO USE THE APPENDICES

The CMSRs provided in Appendices A, B, and C are a detailed resource for understanding all aspects of the CMS defined security controls.

4.1 CMSR APPENDICES

Each CMSR Appendix is a set of security controls based on a CMS System Security Level (i.e., High, Moderate, and Low) as established by Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Each Business Owner is required to determine their system's security level according to *Risk Management Handbook (RMH),* Volume II, Procedure 2.3, *Categorizing an Information System*, and use that designation to select the appropriate CMSR appendix for defining their minimum set of required security controls. The CMSRs Appendices are:

- Appendix A: *CMS Minimum Security Requirements for High Impact Level Data*
- Appendix B: *CMS Minimum Security Requirements for Moderate Impact Level Data*
- Appendix C: *CMS Minimum Security Requirements for Low Impact Level Data*

Each Appendix includes baseline and enhancement controls, and associated amplifying information, for the indicated security level. The CMSRs include:

- Control text (Baseline and Enhancement Controls)
- Additional CMS or data-type specific standards (e.g., CMS defined variables) to which the control must meet (Implementation Standards)
- Additional guidance for clarifying the control (Guidance)
- The specific laws, standards, or mandates from which the control originated (Reference)
- Related controls (Related Control Requirements)
- Recommended objects and methodologies for assessing compliance with each control. (Assessment Procedure)

While each CMSR contains a significant amount of associated information, it should be noted that this information is provided to the user in order to maximize understanding of, not only the controls, but also the expectations for reaching compliance and the methodologies that will be used to verify compliance.

4.2 AUTHENTICATION AND E-AUTHENTICATION

CMSR IA-2 is the baseline control for organizational user authentication requirements. IA-8 is the baseline for non- organizational user authentication requirements (i.e., "e-Authentication".) Included with the baseline are the enhancements establishing the minimum authentication

control requirements. The specific implementation of local and remote authentication and e-Authentication controls are described in *RMH,* Volume III, Standard 3.1, *CMS Authentication Standards*.

5 CMSR STRUCTURE

5.1 CMSR FAMILY NUMBERING AND DESCRIPTION

The security controls have a well-defined organization and structure. They are organized into 26 control families for ease of use in the security control selection and specification process. The families are established by NIST SP 800-53, and are in alignment with the 18 security-related areas specified in FIPS 200[2], *Minimum Security Requirements for Federal Information and Information Systems,* and 8 privacy families listed in Appendix J[3] of the NIST SP 800-53.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each of the 18 security control families and 8 privacy control families. Table 1 summarizes the 26 security control families and the applicable two-character identifier used in the CMSRs.

Table 1 CMSR Security Control Family Descriptions

Family (and Identifier)	Description
Access Control (AC)	The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
Awareness and Training (AT)	The standards listed in this section focus on how the organization shall: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.

[2] Of the eighteen security control families in NIST Special Publication 800-53, seventeen families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS Publication 200. One additional family (Program Management [PM] family) provides controls for information security programs required by FISMA. This family, while not specifically referenced in FIPS Publication 200, provides security controls at the organization level rather than the information system level.

[3] Privacy controls listed in Appendix J, have an organization and structure similar to security controls, including the use of two-character identifiers for the eight privacy families.

Family (and Identifier)	Description
Audit and Accountability (AU)	The standards listed in this section focus on how the organization shall: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
Security Assessment and Authorization (CA)	The standards listed in this section focus on how the organization shall: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management (CM)	The standards listed in this section focus on how the organization shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
Contingency Planning (CP)	The standards listed in this section focus on how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Incident Response (IR)	The standards listed in this section focus on how the organization shall: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
Maintenance (MA)	The standards listed in this section focus on how the organization shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	The standards listed in this section focus on how the organization shall: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
Physical and Environmental Protection (PE)	The standards listed in this section focus on how the organization shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Family (and Identifier)	Description
Planning (PL)	The standards listed in this section focus on how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
Personnel Security (PS)	The standards listed in this section focus on how the organization shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Risk Assessment (RA)	The standards listed in this section focus on how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
System and Services Acquisition (SA)	The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security and privacy assurance considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection (SC)	The standards listed in this section focus on how the organization shall: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security and privacy assurance within organizational information systems.
System and Information Integrity (SI)	The standards listed in this section focus on how the organization shall: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.
Program Management (PM)	The PM family provides controls for information security programs required by Federal Information Security Management Act (FISMA). This family, while not specifically referenced in FIPS 200, provides security controls at the organization level rather than the information system level.
Authority and Purpose (AP)	This family furthers compliance with the Privacy Act by ensuring that organizations: (i) identify the legal bases that authorize a particular Personally Identifiable Information (PII) collection or activity that impacts privacy; and (ii) specify the purpose(s) for which they collect PII in their notices.
Accountability, Audit, and Risk Management (AR)	This family is intended to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that an organization is complying with all applicable privacy protection requirements and minimizing its overall privacy risk.

Family (and Identifier)	Description
Data Quality and Integrity (DI)	This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the public notice.
Data Minimization and Retention (DM)	This family assists organizations in implementing the data minimization and retention elements of the Privacy Act, which requires organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a NARA-approved record retention schedule.
Individual Participation and Redress (IP)	This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.
Security (SE)	This family supplements the security controls in Appendix F to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with Office of Management and Budget (OMB) policies and guidance. The controls in this family are implemented in coordination with information security personnel using the existing NIST Risk Management Framework.
Transparency (TR)	This family implements Sections 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization's information practices and the privacy impact of government programs and activities.
Use Limitation (UL)	This family is intended to assist organizations in complying with the Privacy Act, which prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the Controls in this Family will ensure that the scope of PII use is limited accordingly.

Some *Controls, Enhancements, Implementation Standards* and *Guidance,* or portions thereof, only pertain to narrowly-defined types of data, such as Protected Health Information (PHI), PII or Federal Tax Information (FTI). Additionally, some requirements may only apply within specific implementation scenarios. The approved migration of data into a Federal Risk and Authorization Management Program (FedRAMP)-approved *Cloud Service Provider (CSP)* for instance, may require the unique application of specific *Controls, Enhancements, Implementation Standards* or *Guidance* that are only applicable in this specific scenario. These specialized requirements will be indicated with a "(For *XXX* only)" in the text immediately preceding the applicable section within the ARS—where "*XXX*" will serve as an acronym or short description to indicate the type of data or scenario where that portion of the applicable text uniquely applies.

All other text, where no "(For *XXX* only)" is indicated, are CMS-wide control elements that shall be implemented at the designated system security level for *all* CMS information, information systems, and scenarios.

5.2 CONTROL REQUIREMENTS

The CMS security control structure consists of the *Baseline* or *Enhancement* section, *Guidance* section, *References* section, *Related Requirements* section and *Assessment Procedures* section. In addition, the baseline and enhancements controls may have a sub-section for *Implementation Standards* that will be associated with that baseline or enhancement.

The CMS-tailored security controls serve as the starting point for organizations in determining the appropriate controls and countermeasures necessary to protect their information systems.

The term *organization* is utilized throughout the control requirements and associated CMSR elements. NIST SP 800-53 defines an *organization* as: *…an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).* CMS extends and clarifies this to include applicable *supporting organizations* (that is, *"…operational elements"*)—including contractor organizations. When directing and assigning minimum roles and responsibilities within control requirements, CMSRs may refer to organizational leaders such as the *CIO*. For the purposes of CMSR control requirements, understanding of these terms are to be interpreted as follows:

- For roles preceded by the term *CMS*, such as …*approved by the CMS CIO…*; these roles and responsibilities are to be interpreted to refer to the *CMS agency official* that holds that role or title. In this case, the *CIO for the Centers for Medicare & Medicaid Services*.
- For roles ***not*** preceded by the term *CMS*, such as …*approved by the CIO…*; these roles and responsibilities are to be interpreted to refer to the *local official* that holds that *equivalent* role or title. In the case of a contractor organization, the *CIO* might refer to a corporate *Chief Information Officer*, *Chief Technology Officer*, or *Director of Information Technology for Medicare Programs*; whatever corporate/organizational role is the equivalent of the "Chief Information Officer" within the applicable organizational structure and scope. Within federal government organizational structures, CIO will always refer to the *CMS* CIO.

5.2.1 BASELINE CONTROL

The *Baseline* control is the concise statement specifying the capability needed to protect a particular aspect of the CMS information or information system at the applicable system security level.

Baseline ARS controls are identified by security control Family ID and convey CMS policy, which are based on *minimum* Federal requirements, and:

- Employ, and correlate directly to, NIST 800-53 numbering (e.g., AC-1, AC-2, AC-3…)
- Use CMS designators for additional requirements where a direct NIST correlation is not made (e.g., AC-*CMS*-1.)
- Ordered such that the CMS designators always follow the complete set of NIST designators and always restart the numbering of the CMS designator at 1 (e.g. AC-1, AC-2, AC-3, AC-4, AC-5, …AC-CMS-1.)

The baseline section includes the following:

- *Control Requirement*
- *Implementation Standards* (may not exist for all Baseline controls)
- *Guidance* (may not exist for all Baseline controls)
- *References*
- *Related Control Requirements*
- *Assessment Procedure*
  - *Assessment Objectives*
  - *Assessment Methods and Objects*

5.2.2 ENHANCEMENTS

Enhancements supplement baseline controls to achieve the overall required level of protection in accordance with the system security level. *Enhancements* may only be required for higher system security level baselines, but may be used to strengthen the level of protection provided in lower system security level systems if deemed appropriate by the Business Owner.

The enhancement controls are structured the same as the baseline controls. Each enhancement section is as follows:

- *Control Requirement*
- *Implementation Standards* (may not exist for all Enhancements)
- *Guidance* (may not exist for all Enhancements)
- *References*
- *Related Control Requirements*
- *Assessment Procedure*
  - *Assessment Objectives*
  - *Assessment Methods and Objects*

5.2.3 IMPLEMENTATION STANDARD

When an implementation standard is indicated, it is associated with a baseline control or enhancement. The purpose of the implementation standard is to provide CMS tailored controls for implementation of the associated baseline.

Some standards may contain specific CMS definitions or event values (such as "90 days") to be implemented as the compliance standard for a given control. Other implementation standards are based on specific types of data such as *Protected Health Information (PHI)*, *Personally Identifiable Information (PII)*, or *Federal Tax Information (FTI)*.

For example, AC-20's second implementation standard, at the High system security level states:

> *"(For PII only) Only organization owned computers and software can be used to process, access, transmit, and store PII."*

This particular implementation standard is used by organizations responsible for PII information.

Similar implementation standards exist and apply for organizations responsible for PHI or FTI data, or for scenarios where FedRAMP-approved CSPs are used. All other implementation standards, where no "(For *XXX* only)" is indicated, are CMS implementation controls that shall be implemented at the designated system security level for all CMS information and information systems.

Table 2 shows an example of a possible implementation standard associated with CMSR AC-20. *Implementation Standard* item 1[4] is a CMS-specified control that applies to all CMS information and information systems. Item 2 is specifically designated for those organizations responsible for PII and must be followed for implementation, assessment, and audit.

Table 2 Example Implementation Standards for CMSR AC-20

Implementation Standard(s) *[Example]*
1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees. 2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII.

The RMH, Volume III, Standard 7.1, *Incident Handling*, provides definitions for PII, PHI and FTI. Organizations responsible for these types of information must provide the additional safeguards as defined in the applicable implementation standards.

5.2.4 GUIDANCE

The CMSRs may include additional *Guidance* to explain the intent of the control. In some cases, these include specific CMS desires or recommendations, or may refer to other CMS or NIST publications for further guidance. It is a recommended security practice to refer to the guidance and procedures for additional information to have a clearer and more detailed understanding of specifics of the requirement to assist the organization meeting the CMS security requirements.

5.2.5 REFERENCES

The references section identifies the source documents and section or paragraph designations that are the basis or source for the applicable CMSR. For example, an Internal Revenue Service (IRS) reference may look like this: *IRS-1075: 5.6.3.2#1*. From this example:

- The IRS-1075 is the publication.
- The 5.6.3.2#1 portion is the section with sub-paragraphs leading to the applicable reference used for the control requirement—where the numbers *before* the "#" represent the actual

[4] When referenced outside of the context of the specific CMSR, implementation standards may be referred to (more specifically) as *AC-20.Std.1, AC-20.Std.2,* etc.

numbered Section within the reference document, and the number *after* the "#" represent the unnumbered paragraph within the referenced Section.

5.2.6 RELATED CONTROL REQUIREMENTS

Many, but not all, CMSRs may be *related* to one or more other CMSRs. When addressing some CMSRs, it may be important that their implementation documentation during an assessment or audit be consistent with one or more *related* CMSRs. At the very least, organizations shall take care to ensure that related CMSR implementations do not conflict. While every effort was made to identify related CMSRs, other unidentified relationships may exist that are unique to a particular system, contract type, or organization.

5.2.7 PRIORITY

The priority value listed on the right side of the Control or Enhancement title provides the recommended priority codes used for sequencing decisions during security control implementation. Organizations can use the priority code designation associated with each security control to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control, a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the security control is not selected (or has been withdrawn) for any baseline). This recommended sequencing prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all of the security controls in the security plan have been implemented. The priority codes are intended only for implementation sequencing, not for making security control selection decisions.

5.2.8 ASSURANCE

Two fundamental components affecting the trustworthiness of information systems are *security functionality* and *security assurance*. Security functionality is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system—thus possessing the capability to accurately mediate and enforce established security policies. Security controls address both security functionality and security assurance. Some controls focus primarily on security functionality (e.g., PE-3, *Physical Access Control*; IA-2, *Identification and Authentication*; SC-13, *Cryptographic Protection*; AC-2, *Account Management*). Other controls focus primarily on security assurance (e.g., CA-2, *Security Assessment*; SA-17, *Developer Security Architecture and Design*; CM-3, *Configuration Change Control*). Finally, certain security controls can support security functionality and assurance (e.g., RA-5, *Vulnerability Scanning*; SC-3, *Security Function Isolation*; AC-25, *Reference Monitor*). Security controls related to functionality are combined to develop a security

capability with the assurance-related controls implemented to provide a degree of confidence in the capability within the organizational risk tolerance.

The CMSRs specify assurance-related controls with an "A" in the controls header to identify the security controls that have assurance-related characteristics or properties (i.e., assurance-related controls). Assurance-related controls are discussed in greater detail in NIST SP 800-53 (as amended), Appendix E, *Assurance and Trustworthiness*, to include the allocation of such controls to security control baselines. There is no summary table provided in the NIST SP 800-53 Appendix E for the *Program Management (PM)* family or the *Privacy* families since PM and Privacy controls are not associated with any particular security control baseline.

5.3 ASSESSMENT PROCEDURES

The *Assessment Procedures*, including *Assessment Objectives*, and *Assessment Methods and Objects*, help determine if the security control implementations in the information system are effective (i.e., implemented correctly, operating as intended, and producing the desired outcome). They provide a foundation to support the security assessment and authorization process. The "*Assessment Procedure*" consists of a set of procedural steps that are designated to achieve one or more objectives by applying methods to assessment objects.

5.3.1 ASSESSMENT OBJECTIVE

The "*Assessment Objectives*" include a set of *determination statements* (*"Determine if…"*) related to the particular security control under assessment. The determination statements are closely linked to the content of the security control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

Assessment Objectives establish the expectations for security control assessments based on the assurance requirements defined in the security control. The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Each of the *Assessment Objective determination statements* is either traceable to requirements within the baseline or enhancement security control. This ensures that all aspects of the security control are fully assessed and that any weaknesses or deficiencies in the control can be identified, and corrective actions taken (usually in the form of a Plan of Actions and Milestones [POA&M]).

5.3.2 ASSESSMENT METHODS AND OBJECTS

The assessment methods define the nature of the assessor's actions and include *Examine*, *Interview*, and *Test*. The assessment object identifies the specific item being assessed including specifications, mechanism, activities, and individuals. The application of an assessment procedure to a security control produces assessment findings. These assessment findings are subsequently used in helping to determine the overall effectiveness of the control.

6 REFERENCES

The CMS information security and privacy assurance program and ARS were developed in accordance with Federal mandates and CMS requirements for the handling and processing of CMS' information and information systems. A list of applicable laws across the program is provided below:

- Public Law 74-271, *Social Security Act*, as amended
  http://www.ssa.gov/OP_Home/ssact/ssact.htm.
- Public Law 93-579, *The Privacy Act of 1974*, as amended
  http://www.justice.gov/opcl/privstat.htm
- Public Law 104-13, *Paperwork Reduction Act of 1995*, as amended
  http://www.fws.gov/policy/library/rgpl104-13.pdf
- Public Law 108–173, *Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA*), SEC. 912: Requirements for Information Security for Medicare Administrative Contractors
  http://www.gpo.gov/fdsys/pkg/BILLS-108hr1enr/pdf/BILLS-108hr1enr.pdf
- *Code of Federal Regulations (CFR),* Regulation 5 CFR Part 731 – Suitability,
  http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=5:2.0.1.1.7&idno=5
- United States Code Title 44 Chapter 33—*Disposal of Records*
  http://www.archives.gov/about/laws/disposal-of-records.html
- GAO-09-232G, *Federal Information System Controls Audit Manual (FISCAM),* February 2, 2009
  http://www.gao.gov/new.items/d09232g.pdf
- OMB Circulars can be found at the CMS web site or at:
  http://www.whitehouse.gov/omb/circulars/index.html
- Homeland Security Presidential Directives can be found at:
  http://www.dhs.gov/xabout/laws/.
- Executive Orders can be found at:
  http://www.archives.gov/federal-register/executive-orders/disposition.html
- A list of NIST special publications and FIPS publications can be found at:
  http://csrc.nist.gov/publications/
- The most recent Internal Revenue Service publication 1075 can be found at:
  http://www.irs.gov/pub/irs-pdf/p1075.pdf
- *HHS-OCIO Policy for Information Systems Security and Privacy*, dated July 7, 2011
  http://www.hhs.gov/ocio/policy/index.html#Security
- *HHS-OCIO Policy for Information Systems Security and Privacy Handbook*, dated July 7, 2011 (available upon request via mailto:ciso@cms.hhs.gov)

Additional CMS documents were used as references in the development of this manual. The CMS information security web site at http://www.cms.gov/Research-Statistics-Data-and-

Systems/CMS-Information-Technology/InformationSecurity/ provides a list of applicable CMS documents across the information assurance program.

7 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2013.10.17 12:20:15 -04'00'

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 CMS 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.hhs.gov.