



**OFFICE OF INFORMATION SERVICES**

---

**CIO DIRECTIVE 09-03**

**DATE:** June 15, 2009

**TO:** CMS Center/Office Directors and Regional Administrators  
CMS Business Component Owners/Certification Officials for CMS Systems

**FROM:** Julie Boughn /s/  
CMS Chief Information Officer (CIO) &  
Director, Office of Information Services (OIS)

**SUBJECT:** CIO Directive 09-03 – CIO Designated Representatives for Information Security Requirements--**INFORMATION**

**Purpose**

The purpose of this directive is to provide operational guidance delegating authority to designated representatives to approve or disapprove exception requests on behalf of the CMS CIO. This directive authorizes the CMS CIO representative to act on behalf of the CMS CIO in the specified instances as defined in the CMS Policy for the Information Security Program (PISP) and the CMS Information Security (IS) Acceptable Risk Safeguards (ARS).

**Background**

The CMS PISP and ARS contain a limited number of requirements that allow exceptions to the basic controls if granted by the CIO designated representative. In these instances, the justification and approval for the exception must be controlled, documented and monitored. Both the PISP and the ARS indicate the individual authorized to make the decision on the exception request. Essentially, as written the language envisions two scenarios:

1. The PISP/ARS language that states “must be approved in writing by the CIO or his/her designated representative” refers to the CIO of the entity that is responsible for implementing the required CMS IS controls. For example, for the Baltimore Data Center and CMS facilities at Central Office (CO) and the Regional Offices (ROs), this is the CMS CIO or his/her designated representative. For systems located at external locations, this means the CIO of the entity or organization hosting the system. If the organization does not have an individual titled as their CIO, the executive fulfilling those functions would assume this authority.

2. Three other policy/controls use similar language and state that the exception “must be approved in writing by the CMS CIO or his/her designated representative.” This means that regardless of where the control is implemented, exceptions must be approved by the CMS CIO or his/her designated representative

### **Policy Designations**

The following **Table 1** provides the policy/control statements from the PISP and/or ARS which allows the CIO to delegate his/her responsibilities and the individual(s) assigned the respective delegation. For the CMS Data Center and CMS facilities at CO and the ROs, the identified roles are hereby authorized to act on behalf of the CMS CIO in reviewing and approving in writing exceptions to the specified controls. In the event that the designee is not available either on-site or by electronic means, their Deputy may act on their behalf.

<b>Policy Title</b>	<b>Policy (ARS) Number</b>	<b>CIO Designated Representative(s)</b>
<b>Remote Access</b>	4.1.17 (AC-17)	CMS Chief Technology Officer (CTO)
<b>Access Control for Portable and Mobile Devices</b>	4.1.19 (AC-19)	CMS Chief Information Security Officer (CISO)
<b>Use of External Information Systems</b>	4.1.20 (AC-20)	CMS CISO
<b>System Boot Access</b>	4.1.21 (AC-21)	Director, EDCG
<b>Remote Maintenance</b>	4.9.4 (MA-4)	CMS CTO
<b>Media Labeling</b>	4.10.3 (MP-3)	Director, EDCG
<b>User Installed Software</b>	4.15.7 (SA-7)	CMS CISO
<b>Collaborative Computing</b>	4.16.15 (SC-15)	CMS CTO

**Table 1**

The following **Table 2** provides the three policy/control statements from the PISP and/or ARS which allows the CMS CIO to delegate his/her responsibilities to the individual(s) assigned the respective delegation for all entities or hosted environments operating on behalf of CMS. In the event that the designee is not available either on-site or by electronic means, their Deputy may act on their behalf.

<b>Policy Title</b>	<b>Policy (ARS) Number</b>	<b>CIO Designated Representative(s)</b>
<b>Wireless Access Restrictions</b>	4.1.18 (AC-18)	CMS CISO
<b>External Information Systems Services</b>	4.15.9 (SA-9)	No Delegation
<b>Voice Over Internet Protocol</b>	4.16.19 (SC-19)	CMS CTO

**Table 2**

In order for an exception (risk acceptance) to be granted for an individual policy/control, the attached risk acceptance form must be submitted and signed by the Business Owner, System ISSO, and CIO delegated representative.

In addition to the PISP and ARS delegated designations, I am delegating the responsibility for approving and signing the Plan of Action and Milestones (POA&M) Risk Acceptance forms to the CISO. In the absence of the CISO, the Deputy CISO is authorized to sign the risk acceptance forms. The Risk Acceptance process is used as part of the POA&M process to provide Business Owners the vehicle to document new compensating controls or business risks that may lead to “Low” risk weaknesses being accepted by CMS. These risk acceptance requests should be directed to the CISO and must be approved by the CISO before they can be closed. The POA&M Guideline has been modified to reflect the new delegation and new risk acceptance form. I have also included the new risk acceptance form with this directive.

I ask your support in disseminating this CIO Directive to your staff.

If you have any questions concerning this directive, please contact Ryan Brewer, CISO, at [Ryan.Brewer@cms.hhs.gov](mailto:Ryan.Brewer@cms.hhs.gov) or (410) 786-2614. Staff may contact Mike Mellor, Deputy CISO, at [Michael.Mellor@cms.hhs.gov](mailto:Michael.Mellor@cms.hhs.gov) or (410) 786-2983.

Attachment

cc:

Charlene Frizzera, CoO  
Michelle Snyder, Deputy CoO  
CMS Business Owners of CMS Systems  
CMS Developer/Maintainers of CMS Systems  
Henry Chao, CTO, OIS  
Robert Vacarro, Director, OIS/EDCG  
Sally Good-Burton, OIS/EASG  
Ryan Brewer, CISO, OIS/EASG  
Michael Mellor, Deputy CISO, OIS/EASG  
Maria McMahon, Technical Advisor, OIS/EASG

## CMS Information Security Policy/Standard Risk Acceptance

<b>Component:</b>	<b>System Name:</b>	<b>Subsystem:</b>	<b>Date:</b>
<b>CMS System Security Level</b> (FIPS-199 Categorization of information system):  <b>High</b> <input type="checkbox"/> <b>Moderate</b> <input type="checkbox"/> <b>Low</b> <input type="checkbox"/>		<b>Requestor:</b>	<b>Phone Number:</b>
<b>Overview of the Risk Acceptance Request</b> (explain what is being requested):			
<b>Applicable Policy/Standard Affected</b> (include brief description):			
<b>Finding from Audit: Not Applicable</b> <input type="checkbox"/> 1) Finding title and finding #:  2) Risk level: High <input type="checkbox"/> Moderate <input type="checkbox"/> Low <input type="checkbox"/>  3) Source of finding:  4) Copy finding text in quotes:   5) Recommendation (copy recommendation text from source text in quotes):   6) Business Risk (describe the exposure to CMS business):			
<b>Business Justification for the Risk Acceptance</b> (What is the business impact to CMS of not accepting the request):			
<b>Justification for Request</b> (Explain why compliance with this policy/standard is not possible due to technical limitations, conflict with mission requirements, or other circumstances):			
<b>Risk Mitigation:</b> 1) Describe the compensating controls that will be implemented and, if applicable, the control number from NIST SP 800-53 to reduce the risk of otherwise complying with the policy/standard:   2) Describe how the compensating controls in step 1 provide an equivalent security capability or level of protection for the information system:			
<b>Additional Comments:</b> Describe any additional information that may be needed or reference any attachments:			

