Revoked CIO Directives

The document you are trying to access is obsolete. CIO Directive 12-04 – *Revocation/Re-Affirmation of Legacy CIO Directives* contains the complete list of current and revoked directives. A summary of the directives that were **Revoked** and where to find current related information follows.

1) **CIO Directive 07-01**—*Transporting Sensitive Information: Encryption Requirements for Data Leaving CMS Data Centers*
   a) *Media Transport* requirements are now fully-addressed in the *CMS Acceptable Risk Safeguards (ARS)* manual Appendices (A, B, or C, as appropriate for the security categorization of the information), control MP-5: *Media Transport*, and other relevant security controls and enhancements within the ARS.
2) **CIO Directive 07-02**—*CMS Chief information Security Officer (CISO) Forum for Information System Security Officers (ISSO)*
   a) While the *CMS Chief Information Security Officer (CISO) Forum* will continue to occur, the training requirements for *Information System Security Officers (ISSOs)* are now fully-addressed in CIO Directive 12-03, *Annual Role-Based Information Security Training Requirements* below.
3) **CIO Directive 07-03**—*Mandatory Encryption on all Removable Storage Devices*
   a) *Whole-disk encryption* requirements are fully-addressed in the *ARS* control AC-19: *Access Control for Mobile Devices*.
   b) Additional *data encryption* and *media access* requirements are addressed in other relevant security controls (and their *Enhancements*) within the ARS (including but not limited to: AC-3, AC-17, AC-18, AC-19, MP-4, MP-5, SC-4, SC-7, SC-19, and SC-CMS-1.
   c) *PointSec™* is currently being phased-out at CMS to be replaced by other FIPS 140-2 compliant solutions. Usage of encryption and access to external storage devices will be governed through network-level *Group Policies,* and set through appropriate CMS Office of Information Services (OIS) management and security standards.
   d) Use of *personally-owned* equipment is fully-addressed in the *ARS* control AC-20: *Use of External Information Systems*, and other relevant security controls and enhancements within the ARS.
4) **CIO Directive 07-05**—*FY 2008 Annual Security Controls Testing*
   a) *Annual Controls Testing* requirements are fully-addressed in the *ARS* control CA-2: *Security Assessments*.
   b) *Reporting* of annual testing requirements are now fully-addressed in the *CMS Risk Management Handbook (RMH)*, Volume II, Procedure 7.3, *CMS Annual Attestation Procedure*. Additional guidance, and associated changes to this process, will be managed by the CMS CISO, through further issuances and updates to the RMH.
5) **CIO Directive 07-06**—*Software for Encryption of Agency Information -- Portable Media and E-mail Attachments*
   a) *Electronic Mail* requirements are addressed are fully-addressed in the *ARS* control SC-CMS-1: *Electronic Mail.*

b) Legal requirements for the handling of *Privacy Information* can be found on the CMS *Privacy* website at: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html or by emailing the *CMS Privacy Office* at mailto:Privacy@cms.hhs.gov.

c) *Data encryption* and *media access* requirements are addressed in other relevant security controls (and their *Enhancements*) within the ARS (including but not limited to: AC-3, AC-17, AC-18, AC-19, MP-4, MP-5, SC-4, SC-7, SC-19, and SC-CMS-1.

d) *PointSec*™ is currently being phased-out at CMS to be replaced by other FIPS 140-2 compliant solutions. Usage of encryption and access to external storage devices will be governed through network-level *Group Policies,* and set through appropriate CMS Office of Information Services (OIS) management and security standards.

6) **CIO Directive 08-01**—*Annual Role-Based Information Security (IS) Training Requirements*

a) This Directive was *superseded* by CIO Directive 12-03— *Annual Role-Based Information Security Training Requirements*

7) **CIO Directive 12-02**—*Minimum Security Configuration Standards*

a) This Directive was *superseded* by CMS CISO Memorandum—*Minimum Security Configuration Standards,* dated May 3, 2012. Additional guidance, and associated changes to this process, will be managed by the CMS CISO, through further issuances and updates to the ARS and the RMH.