

§ 164.308(a)(7)(i). Modified language to state that two implementation specifications, “Applications and data criticality analysis” and “Testing and revision procedures,” are addressable.

- Removed “Formal mechanism for processing records” (proposed § 142.308(a)(4)) since this requirement was determined to be in part intrusive into business functions and in part redundant.

- Moved proposed § 142.308(a)(5), “Information access control,” to § 164.308(a)(4)(i) and renamed as “Information access management.” Removed the word “formal” from description. Modified language to state that two implementation specifications (“Access Authorization” and Access Establishment and Modification”) are addressable.

- Moved proposed § 142.308(a)(6), “Internal audit,” to § 164.308(a)(1)(ii)(D) as an implementation specification under the “Security management process” standard since this was determined to be a more logical placement of this item. Retitled, for clarity, “Information system activity review.”

- Moved proposed § 142.308(a)(7), “Personnel security,” to § 164.308(a)(3)(i) and retitled “Workforce security.” Modified language to state that implementation specifications are addressable.

- Combined proposed § 142.308(a)(7)(i), and § 142.308(a)(7)(iii) (“Assuring supervision of maintenance personnel by an authorized, knowledgeable person” and “Assuring that operations and maintenance personnel have proper access authorization,”) under § 164.308(a)(3)(ii)(A) and renamed to “Authorization and/or supervision.” Modified description for clarity.

- Moved proposed § 142.308(a)(7)(iv), “Personnel clearance procedure,” to § 164.308(a)(3)(ii)(B), renamed to “Workforce clearance procedure,” and modified description for clarity.

- Removed proposed § 142.308(a)(7)(v), “Personnel security policies and procedures,” as this feature was determined to require redundant effort.

- Removed proposed § 142.308(a)(7)(vi), “Security awareness training.” Information concerning this subject has been incorporated under § 164.308(a)(5)(i), “Security awareness and training.”

- Removed proposed § 142.308(a)(8), “Security configuration management,” and all implementation features, except “Documentation” (hardware and/or software installation, Inventory, Security testing, and Virus checking),

since this requirement was determined to be redundant. “Documentation” has been made a discrete standard at § 164.316.

- Moved proposed § 142.308(a)(9), “Security incident procedures,” to § 164.308(a)(6)(i) and reworded for clarity. Combined “Report procedures” and “Response procedures” features into a single required implementation specification, named “Response and Reporting” at § 164.308(a)(6)(ii).

- Moved proposed § 142.308(a)(10), “Security management process,” to § 164.308(a)(1).

- Moved proposed § 142.308(a)(10)(i), “Risk analysis,” to § 164.308(a)(1)(ii)(A).

- Moved proposed § 142.308(a)(10)(ii), “Risk management,” to § 164.308(a)(1)(ii)(B).

- Moved proposed § 142.308(a)(10)(iii), “Sanction policy,” to § 164.308(a)(1)(ii)(C).

- Removed proposed § 142.308(a)(10)(iv), “Security policy,” since this requirement was determined to be redundant.

- Moved proposed § 142.308(a)(11), “Termination,” to § 164.308(a)(3)(ii)(C) as an addressable implementation specification under the “Workforce security” standard, and renamed as “Termination procedures”. Removed “Termination” implementation features (changing locks, removal from access lists, removal of user accounts, turning in of keys, tokens, or cards) since these were determined to be too specific.

- Moved proposed § 142.308(a)(12), “Training,” to § 164.308(a)(5)(i) and renamed as “Security awareness and training.” Language modified to incorporate all training information under this one standard. Revised and made addressable all implementation specifications under this standard.

- Moved proposed § 142.308(b), “Physical safeguards to guard data integrity, confidentiality and availability,” to § 164.310 and renamed as “Physical safeguards.” Removed specific reference to locks and keys.

- Moved proposed § 142.308(b)(1), “Assigned security responsibility requirement,” to § 164.308(a)(2) since this has been determined to be an administrative procedure. Modified language to clarify that responsibility could be assigned to more than one individual.

- Moved proposed § 142.308(b)(2), “Media controls,” to § 164.310(d)(1) and renamed as “Device and media controls.” Removed the word “formal.” Added “Media re-use” as a required implementation specification at § 164.310(d)(2)(ii).

- Removed proposed § 142.308(b)(2)(i), “Access control,”

implementation feature as it was determined to be redundant.

- Moved proposed § 142.308(b)(2)(ii), “Accountability” implementation feature to § 164.310(d)(2)(iii), and made it an addressable implementation specification.

- Combined proposed § 142.308(b)(2)(iii), “Data backup,” implementation feature with proposed § 142.308(b)(2)(iv), “Data storage” implementation feature, renamed as “Data backup and storage”, moved to § 164.310(d)(2)(iv), and made it an addressable implementation specification.

- Moved proposed § 142.308(b)(2)(v), “Data disposal,” implementation feature to § 164.310(d)(2)(i) and made it a required implementation specification.

- Moved proposed § 142.308(b)(3), “Physical access controls,” to § 164.310(a)(1) and renamed as “Facility access controls.” Removed word “formal.”

- Moved proposed § 142.308(b)(3)(i), “Disaster recovery,” implementation feature to § 164.310(a)(2)(i). It is now part of the “Contingency operations” implementation specification.

- Moved proposed § 142.308(b)(3)(ii), “Emergency mode operations,” implementation feature to § 164.310(a)(2)(i). It is now part of the “Contingency operations” implementation specification.

- Removed proposed § 142.308(b)(3)(iii), “Equipment control (into and out of site),” as this information is now covered under § 164.310(d)(1), “Device and media controls.”

- Moved proposed § 142.308(b)(3)(iv), “A facility security plan,” to § 164.310(a)(2)(ii).

- Moved proposed § 142.308(b)(3)(v), “Procedure for verifying access authorizations,” to § 164.310(a)(2)(iii) and renamed as “Access control and validation procedures.” Removed the word “formal” from text.

- Moved proposed § 142.308(b)(3)(vi), “Maintenance records,” to § 164.310(a)(2)(iv).

- Moved proposed § 142.308(b)(3)(vii), “Need to know procedures for personnel access,” to § 164.310(a)(2)(iii) and renamed as “Access control and validation procedures.”

- Moved proposed § 142.308(b)(3)(viii), “Procedures to sign in visitors and provide escort, if appropriate,” to § 164.310(a)(2)(iii) and renamed as “Access control and validation procedures.”