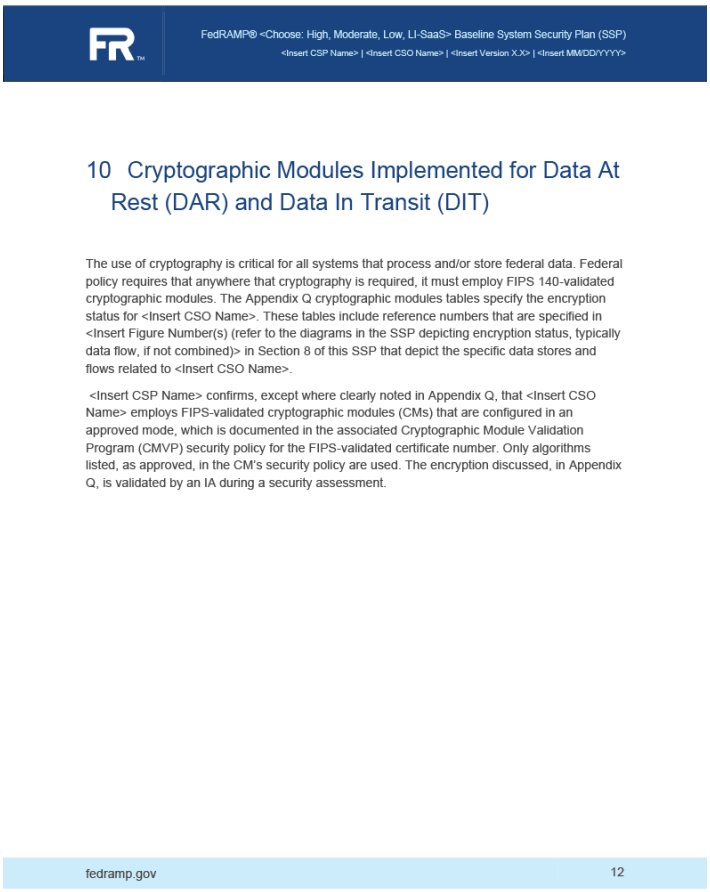
10. Cryptographic Modules Implemented for DAR and DIT



10 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)

The use of cryptography is critical for all systems that process and/or store federal data. Federal policy requires that anywhere that cryptography is required, it must employ FIPS 140-validated cryptographic modules. The Appendix Q cryptographic modules tables specify the encryption status for <Insert CSO Name>. These tables include reference numbers that are specified in <Insert Figure Number(s) (refer to the diagrams in the SSP depicting encryption status, typically data flow, if not combined)> in Section 8 of this SSP that depict the specific data stores and flows related to <Insert CSO Name>.

<Insert CSP Name> confirms, except where clearly noted in Appendix Q, that <Insert CSO Name> employs FIPS-validated cryptographic modules (CMs) that are configured in an approved mode, which is documented in the associated Cryptographic Module Validation Program (CMVP) security policy for the FIPS-validated certificate number. Only algorithms listed, as approved, in the CM's security policy are used. The encryption discussed, in Appendix Q, is validated by an IA during a security assessment.

This is address in Appendix Q: Cryptographic Modules.

Revision #1
Created 2026-03-13 18:47:17 UTC by Brian Ruf
Updated 2026-03-13 18:50:00 UTC by Brian Ruf