National Institute of Standards and Technology

Cryptographic Module Validation Program

NIST Special Publication 800-57 Part 1 Transition Plan for the Use of Key Sizes and Security Strengths by Federal Agencies

NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General*, was published August 2005. Within this document, specifications in Table 4 provide recommendations that may be used to select an appropriate suite of algorithms and key sizes for Federal Government unclassified applications. A minimum of 80 bits of security strength shall be provided until the end of 2010. Between 2011 and the end of 2030, a minimum of 112 bits of security strength shall be provided. Thereafter, a minimum of 128 bits of security strength shall be provided.

The Cryptographic Module Validation Program (CMVP) **800-57 Part 1 Transition Plan addresses the use of key sizes and strengths by Federal agencies**, which are implemented in cryptographic modules validated to FIPS 140-1 or FIPS 140-2. Prior to the publication of SP 800-57 Part 1, there were no recommendations or requirements for any particular key size or strength other than industry *best practices*. FIPS 140-2 **AS07.19** provided a requirement of equivalent strength for key establishment methods, but no explicit sizes or strengths were indicated. The CMVP did not recommend or require any particular key sizes as part of the testing and validation to FIPS 140-1 and FIPS 140-2. With the release of FIPS 140-2 IG 7.5 – *Strength of Key Establishment Methods*, the CMVP stated the requirements for annotating the equivalent security strength of implemented key establishment methods. With the release of SP 800-57 Part 1, this minimum-security transition plan was developed to allow Federal agencies and vendors to smoothly transition to the NIST set of minimum required security strengths.

1. Effective immediately: Federal agencies may continue to use industry *best practice* key strengths in a FIPS Approved mode of operation in FIPS 140-1 or FIPS 140-2 validated cryptographic modules for a period ending on May 19, 2007. This provides a transition period to migrate to the minimum requirement of 80-bits of security strength.

    a. Cryptographic modules validated to FIPS 140-1 or FIPS 140-2 must continue to follow the requirements of FIPS 140-2 IG 7.5.

    b. Agencies must understand that NIST strongly recommends against any continued use of security strengths less than 80-bits. Agencies must accept the security risks of the continued use of strengths less than 80-bits during the transition phase. In short, security strengths less than 80-bits do not provide adequate protection for data whose confidentiality must be assured for more than near-transitory implementations.

2. After the transition period ending on May 19, 2007:

    a. The use of keys of less than 80-bits of security strength shall not be allowed for use in a FIPS Approved mode of operation for use by Federal agencies.
    b. A minimum of 80-bits of security strength shall be required through 2010.
    c. From 2011 through 2030, a minimum of 112 bits of security strength shall be required.
    d. Thereafter, at least 128 bits of security strength shall be required.

The point of contact for this transition plan is Allen Roginsky (CMVP). Please contact Allen at allen.roginsky@nist.gov regarding any questions.