CNSS Advisory Memorandum
Information Assurance/02-04
Revised
March 2005

Advisory Memorandum
on the
Retirement of Data Encryption Standard (DES) Based Cryptography to Protect National Security Systems

Committee on National Security Systems

National Manager

FOREWORD

1. This Advisory Memorandum provides guidance to U.S. Government departments and agencies regarding a "sunset date" for the use of the Data Encryption Standard (DES) cryptographic algorithm for the protection of national security systems and/or information.

2. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this Advisory Memorandum from the CNSS web site (www.cnss.gov) or by contacting the Secretariat at the address below. U.S. Government contractors are to contact their appropriate government agency Contracting Officer Representative regarding distribution of this document.

/s/
MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Secretariat (I01C) . National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716
(410) 854-6805 . UFAX: (410) 854-6814
cnss@radium.ncsc.mil

Advisory Memorandum on the Retirement of Data Encryption Standard (DES) Based Cryptography to Protect National Security Systems

SECTION I - APPLICABILITY

1. This Advisory Memorandum applies to all Executive departments and agencies and to all U.S. Government contractors who own, procure, use, operate, or maintain national security systems as defined in CNSS Instruction No. 4009, "National Information Assurance Glossary," dated May 2003.

SECTION II - BACKGROUND

2. All cryptographic algorithms have fixed operational life-cycles. Advances in technology can shorten the expected life-cycle of a cryptographic algorithm. The security of national security systems is partially predicated on the periodic assessment and replacement of aging cryptographic algorithms. As a result of such assessments, the National Security Agency will no longer evaluate or approve any DES-based security implementation for the protection of national security systems and/or related information.

SECTION III - GUIDANCE

3. The purpose of this Advisory is to alert all Departments and Agencies that currently use DES-based systems to protect national security information that the National Security Agency plans to discontinue supporting such systems. Consequently, the following guidance is provided with respect to continued use of legacy DES-based cryptography in national security applications.

a. Use of the cryptographic algorithm DES or Triple DES[1], in a single key mode, is no longer acceptable to protect information in national security systems. Organizations

[1] Note: There are three keying options for Triple DES: 1. The three keys may be identical (one key TDES), 2. The first and third key may be the same but different from the second key (two key TDES), or 3. All three keys may be different (three key TDES), therefore, one key Triple DES like DES is no longer acceptable to protect information in national security

must take immediate action to remove equipment using single key DES from their national security systems inventory.

b. Departments and Agencies should take action now to replace any systems employing Triple DES in a two key mode. It is NSA's goal to have these systems retired by 2008.

c. By 2015, NSA anticipates that it will no longer provide cryptographic key-generation support for systems employing any Triple DES implementation, unless there are compelling reasons why certain programs will require ongoing support. All such systems should be removed from national security system architectures by that time.

4. Based on this guidance, it is imperative that Departments and Agencies currently using DES-based security solutions to protect national security systems start programming their resources now to upgrade those systems. The NSA Cryptographic Modernization Office (CMO) can provide guidance on suitable replacement algorithms/systems, based on key generation modernization support plans (i.e., key discontinuation). Contact the CMO via NSA IA Customer Service at 1.800.688.6115.

Note: Contact Mr. William Barker (301) 975-8443, wbarker@nist.gov, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-893 for guidance for using DES on other Federal Information Systems.

systems. ("Cryptographic Standards and Guidance: Status Report," National Institute of Standards and Technology, http: //www.itl.nist.gov/lab/bulletns/bltnsep02.htm//)