INFORMATION ASSURANCE

"Confidence in Cyberspace"

INFORMATION ASSURANCE
ADVISORY NO. IAA U/OO/800624-17

Date: 11 April 2017

SUBJECT: Establishing NSA's position on the use of Trusted Platform Modules in National Security Systems - DECISION

Advisory Memorandum
Deployment of Trusted Platform Modules (TPMs) as Cryptographic Components in National Security Systems

APPLICABILITY:

This Advisory Memorandum is issued under the authority defined in Reference A, and applies to all Executive Departments and Agencies, and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in Reference B.

BACKGROUND:

Cryptographic components manufactured to conform to the Trusted Computing Group's (TCG)®[1] Trusted Platform Module (TPM) specification have been widely deployed in commercial computing devices including personal computers, servers, and tablets.

For the purpose of this guidance, a Trusted Platform Module is defined as any hardware or firmware that has been TCG Compliance tested against either the International Organization for Standardization (ISO)®[2] or TCG TPM specification. Compliance testing is functional testing that is self-conducted using any TCG approved automated TPM Compliance Test Suite.

GUIDANCE:

1. Per *Committee on National Security Systems Policy #11*, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, all COTS IA and IA-Enabled IT products acquired for use to protect information on NSS shall comply with the requirements of the NIAP program. For TPMs, only FIPS 140-2 Level 1 is required for NSS acquisition, because there is not a NIAP-approved Protection Profile for this technology. This position statement will be re-evaluated when a Protection Profile or collaborative Protection Profile is available for TPM evaluations. TCG Security Evaluation Certification against the TCG's PC Client TPM 1.2/2.0 protection profile is **not** required for NSS acquisition.
2. The Trusted Computing Group recently published *TCG TPM v2.0 Provisioning Guidance*, which provides guidance to TPM Manufacturers, Platform Manufacturers and Platform Administrators regarding how the

[1] Trusted Computing Group is a registered trademark of Trusted Computing Group
[2] ISO is a registered trademark of International Organization for Standardization

TPM should be enabled when it arrives at the Enterprise. Platforms containing TPM 2.0 which are acquired for use in NSS should be configured to meet this guidance, as described in Reference D, in order to promote manageability and ease of use of the TPM by applications running on the platform.

REFERENCES:

For additional information, please see the following:

A. National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” dated July 5, 1990.

B. CNSS Instruction No. 4009, “National Information Assurance Glossary,” dated April 26, 2010.

C. CNSS Policy 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology (IT) Products” dated, June 10, 2013

D. “TCG TPM v2.0 Provisioning Guidance”, Version 1.0, Revision 1.0, dated March 15, 2017.

DISCLAIMER OF ENDORSEMENT:

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

FOR FURTHER INFORMATION, PLEASE CONTACT:

Industry Inquiries
410-854-6091
email: bao@nsa.gov

Client Requirements And General Information Assurance Inquiries
IA Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov