National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

NIAP Policy Letter #23

19 November 2014

SUBJECT: NIAP evaluation of IEEE 802.11 wireless products

REFERENCES: NIAP Policy #5
Committee for National Security Systems Policy #11
NIST Federal Information Processing Standard 140-2
NIST Special Publication 800-38C
IEEE 802.11-2012

PURPOSE: This policy specifies an interim approach for IEEE 802.11-2012 wireless products to be compliant with the NIAP Wireless Local Area Network (WLAN) Client PP and the NIAP Mobile Device Fundamentals PP.

BACKGROUND: NIAP-compliant IEEE 802.11-2012 wireless products are required to implement CCMP (Counter with CBC-Message Authentication Code Protocol), which is an IEEE-defined protocol based on the AES-CCM encryption mode, as defined in NIST SP 800-38C. CCMP can be implemented in software or in hardware by a wireless chipset in wireless-capable products.

NIAP evaluations demonstrate that relevant cryptography is mapped to a valid NIST Cryptographic Algorithm Validation Program (CAVP) or Cryptographic Module Validation Program (CMVP) certificate. Presently, most consumer wireless client devices lack NIST CAVP/CMVP certificates for the AES-CCM algorithm used by the devices' wireless chipset.

NIAP acknowledges device vendors must address this issue with their wireless chipsets and further acknowledges achieving NIST AES-CCM certification may not be a quick process. Thus, NIAP is publishing this policy to provide an interim approach for evaluation of CCMP implementations in products evaluated against the Wireless Local Area Network (WLAN) Client PP and the Mobile Device Fundamentals PP.

POLICY: All products using a wireless chipset submitted to NIAP CCEVS for evaluation against the NIAP WLAN Client PP or the NIAP Mobile Device Fundamentals PP on or after 1 January 2016 must provide a valid NIST certificate reference for AES-CCM used in CCMP. For products submitted prior to 1 January 2016, if the AES-CCM used in IEEE 802.11-2012 applications does not have a NIST CAVP certificate, the

product must implement Wi-Fi Protected Access® 2 (WPA2) Enterprise and be Wi-Fi CERTIFIED™ by the Wi-Fi Alliance®. The Security Target must include a statement to this effect, which is to be verified by the CCTL during the evaluation.

This policy does not apply to products that implement CCMP in software or to products, such as Access Points and Wireless Controllers, being evaluated against the WLAN Access Systems Protection Profile. These products must present a valid NIST CAVP certificate reference for AES-CCM, as well as undergo the AES-CCM tests specified in the Assurance Activity.

EFFECT: The primary intent of this policy is to provide an interim period for vendors to secure NIST CAVP/CMVP validations for chipsets implementing AES-CCM in order to comply with the NIAP Wireless Local Area Network (WLAN) Client PP and the NIAP Mobile Device Fundamentals PP.

EFFECTIVE DATE: All relevant evaluations submitted to NIAP on or after 1 January 2016 must have a NIST CAVP/CMVP certificate demonstrating AES-CCM compliance.

Original Signed By

JANINE S. PEDERSEN
Director, NIAP