Five Criteria for 802.1AEbk – Media Access Control (MAC) Security Amendment: GCM-AES-256 Cipher Suite

*1. Broad Market Potential *

*a. Broad sets of applicability *

This amendment is applicable to all networks that are currently using or planning to use IEEE 802.1AE, MACsec.

The addition of this cipher suite will broaden the applicability of IEEE 802.1AE
to appeal to those customers desiring the use of the stronger cipher suite.

*b. Multiple vendors and numerous users ***

A number of major equipment providers have indicated support for this amendment.

*c. Balanced costs (LAN versus attached stations) ***

There is no imbalance of cost created by this amendment.

*2. Compatibility ***

This will be fit within the framework in IEEE 802.1AE-2006. There are no changes
to the frame formats. There is no change to the conformance clause.

*3. Distinct Identity ***

*a. Substantially different from other IEEE 802 standards ***

IEEE 802.1AE is already a recognized and established standard, applicable to
security not covered by other 802 standards and currently lacking a 256-bit Cipher Suite, although the future need for such a Cipher Suite was recognized in
the development of 802.1AE-2006 and in 802.1X-2010.

*b. One unique solution per problem (not two solutions to a problem) ***

This project enhances IEEE 802.1AE to meet emerging and additional needs, it
does not duplicate existing capabilities.

*c. Easy for the document reader to select the relevant specification ***

IEEE Std 802.1AE is already an established reference for MAC Security.

*4. Technical Feasibility *

*a. Demonstrated system feasibility *

Characteristics of GCM-AES are already well known. GCM-AES 256 has already been
referenced by RFC 2116.

*b. Proven technology, reasonable testing ***

Technology for testing cryptographic modes of operations is well advanced.

*c. Confidence in reliability ***

GCM-AES has been adopted by NIST. GCM-AES-256 is expected to pose no new reliability challenges.

*d. Coexistence of 802 wireless standards specifying devices for unlicensed operation ***

Not applicable.

*5. Economic Feasibility *

*a. Known cost factors, reliable data ***

The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.

*b. Reasonable cost for performance ***

Experience with AES at all block sizes has met customer needs for cost of perceived value.

*c. Consideration of installation costs ***

No differences expected. The key agreement protocol designed in IEEE 802.1X-2010 was designed to support a cipher with longer key lengths. No changes in the installation practice are anticipated.