

January 16, 2008  
Captain Richard J. Duncan  
Joint Interoperability Test Command  
Fort Huachuca, Arizona

Letter of Conformance – Amended – March 24, 2008

## Host/Workstation Requirements

### **IPSec**

- ❑ RFC 2401 Security Architecture for the Internet Protocol
- ❑ RFC 2406 IP Encapsulating Security Payload (ESP)
- ❑ Part RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
  - Null Encryption
  - AES-CBC
  - 3DES-CBC
  - HMAC-SHA-1
  - HMAC-MD5
- ❑ RFC 2407-09 IKEv1 protocol
- ❑ RFC 4109 Algorithms for Internet Key Exchange version 1 (IKEv1) - Added

## Network Server Requirements (Simple and Advanced Server)

### **IPSec**

- ❑ RFC 2401 Security Architecture for the Internet Protocol
- ❑ RFC 2406 IP Encapsulating Security Payload (ESP)
- ❑ RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
  - Null Encryption
  - AES-CBC
  - 3DES-CBC
  - HMAC-SHA-1
  - HMAC-MD5
- ❑ RFC 2407-09 IKEv1 protocol
- ❑ RFC 4109 Algorithms for Internet Key Exchange version 1 (IKEv1) - Added

### **Additional Services beyond MUST Support**

- ❑ Deleted RFCs 3261 and 2911