



Copyright © 2018 Knoxen, LLC. All Rights Reserved.















ClA Document

# CIA Document

## Network Operations Division Cryptographic Requirements<sup>1</sup>

Section 2.4, 19

Any transport layer encryption<sup>2</sup> **must** be layered over the cryptography<sup>3</sup> discussed in this document. Because this outer layer may be decrypted by an attacker (e.g., SSL Man-in-the-Middle) any transport encryption **must** be used for traffic blending<sup>4</sup> only and not for secrecy.

1. Top-secret classified document obtained by Wikileaks through Shadow Brokers

2. TLS (e.g. HTTPS)

3. Application level security

4. Request metadata leaks no information

# Scenario