FIPS 140-3 (Second Draft) Sections Submitted for Comments

-Guidelines for Reviewers -

NIST is requesting additional comments only on the following sections and sub-sections to resolve gaps and inconsistencies between the comments.

4.2.2 Trusted Channel – the comments suggested that NIST should not mandate the implementation of a trusted channel at Security Level 3 and 4 for all modules. NIST is proposing deletion of the requirement, but to allow for adequate, comparable security, is proposing the addition of an optional "Remote Control Capability." The proposed Remote Control Capability section would specify requirements addressing the module's ability to process logons, send service requests to, and receive service responses from a remote module without compromising security. If the Remote Control Capability is supported, this section would mandate the use of a Trusted Channel at Security Level 3 and 4. NIST would appreciate comments on the proposed approach.

4.3.1 Trusted Role – the comments raised a variety of different concerns, reflecting different interpretations of the purpose of the Trusted Role. To address these concerns NIST is proposing the deletion of the Trusted Role and replacement with a *Self-initiated Cryptographic Capability*, configured and activated by the Crypto Officer that would be preserved over rebooting or power cycling of the module. The capability would provide the module with the ability to perform cryptographic operations including *Approved and Allowed* security functions without external operator request. NIST would appreciate comments on the proposed approach.

4.7 Physical Security – Non-Invasive Attacks – the comments received suggest substantial changes that would either weaken or strengthen the impact of these requirements. Comments received included stronger security requirements for Security Level 3 and 4, making the section mandatory for all cryptographic modules, including the Security Level for this section as part of the overall Security Level, while other comments suggested not addressing non-invasive attacks within the standard. NIST would appreciate general and specific comments on the requirements to address non-invasive attacks.

4.8.4 Sensitive Security Parameter (SSP) Entry and Output – the comments received raised a variety of different concerns, reflecting different interpretations of the requirements on SSPs that are entered into or output from a module. SSP entry and output requirements depend on whether the SSP is entered or output manually or electronically, and whether the SSP is distributed manually or electronically. New technologies have called into question this taxonomy of SSP entry and output methods. NIST would appreciate comments on the most appropriate way to categorize these methods, and the appropriate requirements for each method.

Annex B, Section: Operator Authentication Mechanisms – the comments received indicated that the specification for the strength of the operator's authentication method was incomplete, particularly with respect to biometrics. For biometric authentication, NIST proposes the use of a *Liveness Detection* method associated with the *Session False Match Rate* for one attempt and the *Generalized False Accept Rate* for multiple attempts in one minute. NIST would appreciate comments on the proposed approach.