Department of State comments on NIST SP 800-38D, July 2007 draft

Organization/ Division/Branch/Section Designation	Name of Commentor and Organization	Comment Number	Comment Type (G-General, E-Editorial, T-Technical)	Section or Page Number	Comment(Include rationale for comment)	Suggested change
Dept of State		1	T	Section 8.1	Deterministic construction: the Recommendation should require the leading 32 bits of the IV hold the fixed field, and the trailing 64 bits hold the counter field; standardizing ensures that devices can interoperate and limits the number of configured options required for interoperation.	Recommendation requires require the leading 32 bits of the IV hold the fixed field, and the trailing 64 bits hold the counter field
Dept of State		2	G	All	While this document does reference that this is the AES algorithm, it fails to define what level of information may be protected by this algorithm.	A statement should be added in either the purpose or the introduction to make it clear that this algorithm is NOT for classified information.
Dept of State		3	G	All	Similarly to the above comment (3), the document uses the phrase "confidential data" several times, which coiuld lead a reader to believe that this is an encryption algorithm for the protection of classified information.	Since this algorithm is only for the protection of SBU, a different phrase should be used to describe this data. A phrase such as "sensitive data" wold be more appropriate.