Security Function: Encryption.

Error Propagation: Finite, $n/8$ (=NSB) sub-blocks are correlated together.

Synchronization: Any cryptosystem that uses 2DEM must ensure that the block structure remains intact, either by framing or by storing data in multiple-block-sized chunks.

Parallelizability: fully parallelizable.

Keying Material Requirements: one key (that of the underlying block cipher)

Counter/IV/Nonce Requirements: BPR should be generated randomly. It is encrypted and sent with ciphertext. (Counters, IVs, and nonces could be used with 2DEM, but none is required in our specification)

Memory Requirements: Just memory required for underlying block cipher, input plaintext, and output ciphertext, and the value of BPR (an integer).

Pre-processing Capability: None. (Subkeys, if any, could be computed only once).

Message Length Requirements: arbitrary length messages could be encrypted, and padding is necessary if ciphertext stealing (or some other alternative) is not used.

Ciphertext Expansion: none (besides that required for padding).

Other Characteristics: See specification document.