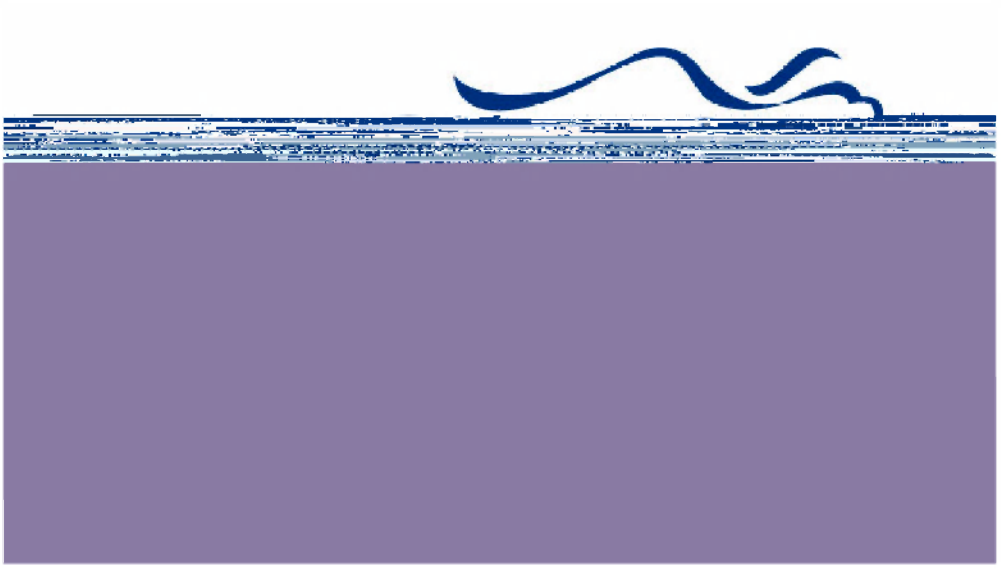
National Security Agency
Central Security Service



(U) Cryptographic Modernization (CryptoMod) Classification Guide
3-9

Effective Date: 1 February 2010

CLASSIFIED BY: [redacted]
Director, Information Assurance

REASON FOR CLASSIFICATION: 1.4 (c) (g)
DECLASSIFY ON: 25 years*

ENDORSED BY: [redacted]
Deputy Associate Director, Policy and Records

Description of Information	Classification/ Markings	Reason	Declass Date	Remarks
B.9 (U) The use of Suite A and Suite B algorithm names and/or cover names used in the CryptoMod.	UNCLASSIFIED	N/A	N/A	
B.10 (U) The fact that NSA is migrating many of its cryptographic products to modern crypto-algorithms within CMI.	UNCLASSIFIED	N/A	N/A	(U) CMI specifies the use of multiple suites of crypto-algorithms.
B.11 (U) The fact that a named CryptoMod product will incorporate multiple suites of crypto-algorithms.	UNCLASSIFIED	N/A	N/A	(U) For example, the KIV-7M employs multiple suites of crypto-algorithms.
B.12 (U) The fact that the next generation US DoD Key Management Infrastructure (KMI) will support products using multiple suites of crypto-algorithms and will be using these algorithms to protect KMI information.	UNCLASSIFIED	N/A	N/A	
B.13 (U//FOUO) CryptoMod Program planning information such as schedules or milestones that show when the entire U.S. cryptographic inventory will transition to modern crypto-algorithms.	SECRET (See remarks for releasability.)	1.4 (c) g)	25 years*	(U//FOUO) Program planning information on cryptographic products is normally REL TO USA, AUS, CAN, GBR, NZL. See following remark. (U//FOUO) Information related to Nuclear Command and Control or Space systems is generally not releasable. **However:** (U) There may be occasions when this information is shared with select Allied national security authorities. Such determinations will be made by the IAD Technical Director in conjunction with the IAD Office of Foreign Affairs after consideration of need-to-know. (U) Refer to Service or program-specific classification guidance.

Description of Information	Classification/ Markings	Reason	Declass Date	Remarks
B.14 (U) Key lengths of unclassified algorithms used in CryptoMod products.	UNCLASSIFIED	N/A	N/A	(U) Unclassified algorithms, when used as part of Suite A, are UNCLASSIFIED//FOUO.
B.15 (U//FOUO) Documentation for classified crypto-algorithms that define or imply symmetric key lengths before operational use.	SECRET	1.4 (c) (g)	25 years*	(U) See remark for item B.5 regarding foreign releasability.
B.16 (U//FOUO) Documentation for classified crypto-algorithms that define or imply symmetric key lengths after operational use.	CONFIDENTIAL	1.4 (c) (g)	25 years*	(U) See remark for item B.5 regarding foreign releasability.
B.17 (U//FOUO) The fact that UNCLASSIFIED public crypto-algorithms may be used in NSA-certified products.	UNCLASSIFIED	N/A	N/A	(U) No association on the use within the product is defined.
C. (U) Positive Access Control (PAC) and Software Signing				
C.1 (U//FOUO) Any EnPAC parameters and software signing parameters generated by the U.S.	TOP SECRET	1.4 (c), (g)	25 years*	(U//FOUO) The U.S.-generated operational EnPAC parameters are not releasable under any circumstances.
C.2 (U//FOUO) The fact that CryptoMod cryptographic products may contain PAC.	UNCLASSIFIED//FOUO	N/A	N/A	
C.3 (U) Identification of the specific algorithm, by cover name, that is used for PAC.	UNCLASSIFIED//FOUO	N/A	N/A	
C.4 (U) Any detailed explanation or documentation of PAC functions.	SECRET//REL TO USA, AUS, CAN, GBR, NZL	1.4 (c) (g)	25 years*	(U//FOUO) Information as documented in EKMS 322.
C.5 (U//FOUO) Operational DePAC parameters and operational software verification parameters (the actual parameters) that are contained in equipment in production.	SECRET//REL TO USA, AUS, CAN, GBR, NZL	1.4 (c) (g)	25 years*	(U//FOUO) These DePAC parameters and operational software verification parameters are classified to guarantee the integrity of these parameters during production. (U//FOUO) Specific release of U.S. DePAC parameters should be based upon need-to-know.
C.6 (U) Operational DePAC parameters and operational software verification parameters that have been installed in a modern product.	UNCLASSIFIED//FOUO	N/A	N/A	(U) Once installed, there is no inherent sensitivity to these values.

Description of Information	Classification/ Markings	Reason	Declass Date	Remarks
C.7 (U) Test DePAC parameters and test software verification parameters.	UNCLASSIFIED	N/A	N/A	
D. (U) Miscellaneous				
D.1 (U//FOUO) The use of named public crypto-algorithms, not part of Suite B, with an NSA-certified product.	SECRET//REL TO USA, AUS, CAN, GBR, NZL	1.4 (c) (g)	25 years*	(U//FOUO) The association is classified for all references to the public cryptographic algorithms. (U//FOUO) The use of public cryptographic algorithm names can be used as cover for any classified algorithm. (U//FOUO) For example, using PGP for the protection of classified information within the KG-### would be classified SECRET//REL TO USA, AUS, CAN, GBR, NZL.
D.2 (U//FOUO) The association of crypto-algorithms or equipments with LYOU identified. .	SECRET//REL TO USA, AUS, CAN, GBR, NZL	1.4 (c) (g)	25 years*	
D.3 (U//FOUO) Any list which associates crypto-algorithms and equipment with Critical Year (CY) identified.	TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL (See remarks for releasability.)	1.4 (c) (g)	25 years*	(U//FOUO) The "*Assessment of Type 1 Cryptographic Products*" provides a compiled listing of algorithms and equipments with the associated LYOU and CY data. Only the equipment name, Strategic LYOU, Tactical LYOU, clarifying remarks and algorithms may be extracted and shared at the SECRET//REL FVEY level with individuals with a need-to-know.

*** 25 years: Declassification in 25 years indicates that the information is classified for 25 years from the date a document is created or 25 years from the date of this original classification decision, whichever is later.**