NISTIR 7298
Revision 2

Glossary of Key Information Security Terms

Richard Kissel, Editor

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7298
Revision 2

Glossary of Key Information Security Terms

Richard Kissel, Editor
Computer Security Division
Information Technology Laboratory

May 2013

U.S. Department of Commerce
Rebecca Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency or Internal Report 7298r2
222 pages (May 2013)

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: secglossary@nist.gov

Cryptographic Alarm –	Circuit or device that detects failures or aberrations in the logic or operation of crypto-equipment. Crypto-alarm may inhibit transmission or may provide a visible and/or audible alarm. SOURCE: CNSSI-4009
Cryptographic Algorithm –	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. SOURCE: SP 800-21; CNSSI-4009
Cryptographic Ancillary Equipment –	Equipment designed specifically to facilitate efficient or reliable operation of cryptographic equipment, without performing cryptographic functions itself. SOURCE: CNSSI-4009
Cryptographic Binding –	Associating two or more related elements of information using cryptographic techniques. SOURCE: CNSSI-4009
Cryptographic Boundary –	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. SOURCE: FIPS 140-2
Cryptographic Component –	Hardware or firmware embodiment of the cryptographic logic. A cryptographic component may be a modular assembly, a printed wiring assembly, a microcircuit, or a combination of these items. SOURCE: CNSSI-4009
Cryptographic Equipment –	Equipment that embodies a cryptographic logic. SOURCE: CNSSI-4009
Cryptographic Hash Function –	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and 2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output. SOURCE: SP 800-21
Cryptographic Ignition Key (CIK) –	Device or electronic key used to unlock the secure mode of crypto-equipment. SOURCE: CNSSI-4009