
DEPARTMENT OF DEFENSE

MILITARILY CRITICAL TECHNOLOGIES LIST

SECTION 17: INFORMATION-SECURITY TECHNOLOGY



October 2003

Defense Threat Reduction Agency
Ft. Belvoir, VA

PREFACE

The Militarily Critical Technologies List (MCTL) Program provides a systematic, ongoing assessment and analysis of goods and technologies to identify those that are critical to the Department of Defense (DoD). It characterizes the technologies (including quantitative values and parameters) and assesses worldwide technology capabilities.

The MCTL is a compendium of goods and technologies that DoD assesses would permit significant advances in the development, production, and use of the military capabilities of potential adversaries. It includes goods and technologies that enable the development, production, and employment of weapons of mass destruction (WMD). Goods and technologies are considered critical if their acquisition and exploitation by a potential adversary would either significantly negate or impair a major military capability of the United States or significantly advance a critical military capability of the adversary. A leading edge technology that has a high potential for advanced military application can be included even if it is not currently embedded in a U.S. system.

Technologies are identified through the deliberation and consensus of Technology Working Groups (TWGs) whose members are subject matter experts from government, industry, and academia. TWG chairpersons continually screen technologies and nominate items to be added or removed from the MCTL. Working within an informal structure, the TWGs strive to produce precise and objective analyses across the technology areas and to update these assessments periodically.

The legal basis of the MCTL stems from the Export Administration Act (EAA) of 1979, which assigned responsibilities for export controls to protect technologies and weapons systems. It established the requirement for DoD to compile a list of militarily critical technologies. The EAA and its provisions, as amended, have been extended by Presidential Directives.

The MCTL is not an export control list. Items on the MCTL may not be on an export control list, and items on an export control list may not be on the MCTL. The MCTL is designed to be used as a reference for evaluating potential technology transfers and for reviewing technical reports and scientific papers for public release. Technical judgment must be used when applying the information. The MCTL should be used to determine whether the proposed transaction would result in a transfer that would give potential adversaries access to technologies whose specific performance levels are at or above the characteristics identified as militarily critical. It should be used with other information to determine whether a transfer should or should not be approved.

An Index of MCTL Technology Data Sheets is provided with each MCTL section. Separate documents contain a Glossary and a list of Acronyms and Abbreviations.

This document, MCTL Section 17: Information Security Technology, supersedes MCTL Part I, Section 8.5: Information Security, June 1996.

SECTION 17—INFORMATION-SECURITY TECHNOLOGY

Scope

17.1	Cryptologic Technology	MCTL-17-15
17.2	Digital Steganographic Technology	MCTL-17-35
17.3	Identity-Management Technology	MCTL-17-43
17.4	Network Firewall Technology	MCTL-17-65

Highlights

- In the Information Age, a universal military requirement exists for information-system security to (1) conceal intentions while military operations are in the planning and preparation phase and (2) achieve surprise, conceal execution orders, and protect situation reports during the execution phase of operations.
- Strong personnel, facilities, equipment, standardization, training, and test and evaluation security programs, as well as defensive Information Operations and Operation Security (OPSEC) are key components of secure militarily critical information and infrastructure assurance systems.
- Commercial information-security technologies, techniques, and products are widely available in world markets with capabilities that are adequate for the protection of some militarily critical information systems; these are also available in commercial-off-the-shelf (COTS) versions, many of which can be customized by rogue states, subnational groups, terrorists, criminals, and international crime syndicates.
- Significant progress is being made toward the development of open, market-based information-security products. These products include commercial public key infrastructures (PKI) and cryptographic, steganographic, and biometric systems, many of which are now covered by national and international standards.
- In the Information Age, few computers are not connected to the Internet. Single-channel signaling and operating systems that can be hacked make firewalls between computers and the Internet a necessity.
- Open worldwide information-security research and development (R&D), which is producing technologies that have undergone scientific peer review, is enabling the development of sound militarily critical information-security products.
- Both commercial and government information-security technologies and products are becoming more affordable.
- The potential adversaries of the United States will have the same access to the global commercial industrial base and installed communications base, including most of the same information-security technologies and products that the U.S. military forces have. (*Joint Vision 2020*)

OVERVIEW

The Wassenaar Arrangement defines “information security” as:

All the means and functions ensuring the accessibility, confidentiality, or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes cryptography, cryptanalysis, protection against compromising emanations, and computer security.

The Information Security section, however, is limited to those technologies that meet the Militarily Critical Technologies List criteria, rather than the multitude of technologies that support various information-security functions.

Information-security technologies have been clustered in four subsections: Cryptologic Technology, Digital Steganographic Technology, Identity Management Technology, and Network Firewall Technology. The Cryptologic subsection contains cryptographic, cryptanalytic, and embeddable programmable processor technologies. The Digital Steganographic subsection contains the steganographic and steganalytic technologies. The Identity Management subsection contains the biometric, smart card, and secure identity-management system technologies. The Network Firewall subsection covers packet filtering, application proxy, stateful packet inspection, and hybrid firewall technologies.

We recognize that there is far more to information security than those technologies and products identified in this section. There are many other information-security-related computer software and hardware, facilities, and equipment technologies, all of which are important to the security of militarily critical information systems. However, these are relatively low-tech technologies and techniques that repeatedly appear in public domain technical literature and trade journals and are widely available in the international marketplace. These technologies and techniques also appear in the Common Criteria, which is both an American National Standards Institute (ANSI) and International Standards Organization (ISO) standard. They were not included in the Information Security section because all are widely known and well understood technologies and techniques. This does not mean that they are not of significant value to the security of militarily critical information systems.

Although covered in this section only by insinuation, or only in passing, human frailty still accounts for roughly 80 percent of the information-security system failures, as it has for the last 25 years. Therefore, the key link in any information-security chain is not a technology per se. Rather, it is the people who manage information-security system operations and those who use them. Technology can reduce, but not eliminate, the human frailty risks to trusted information systems. Perhaps the greatest security-risk-reduction requirement is for more carefully selected security-system management, operation, and administration team members with better skill matches for the sensitive positions they occupy in information-security systems. Equally important is more careful selection and training of secure information system end users. In short, all personnel managing, operating, administering, and using secure information systems must be worthy of the high trust and great responsibility. Improvements in the number as well as quality of personnel selected for the management and use of information-security systems must be combined with vigorous security indoctrination, training, standardization, test, exercise, and evaluation programs, including a thorough training in OPSEC. For these reasons, information-security system architects and developers should be sensitive to the great importance of clean, bug-free code and carefully engineered user-system interfaces to system security applications.

Some of the Information Security section technology items are closely related to those in the Information Technologies section because information-security modules, components, and systems must be tightly integrated with, if not an integral component or module of, the basic information-processing hardware and software architecture that is integrated and tested during system development.

Computer operating systems and many applications now incorporate high-performance features and meta-processing techniques that are shortening the cryptanalytic time required for an exhaustive key search, making the Information Processing subsection technologies closely related to the Information Security section.

The time required for cryptanalysis is a function of both knowledge in the field of mathematics and the state of the art in high-performance computing. Cryptanalytic procedures and techniques are dependent on the state of the art in high-performance computing because processing power determines the length of time required to perform an exhaustive key search which, in turn, governs the life cycle for key lengths.

Identity-management technologies are closely related to the access and circulation-control system technologies that protect sensitive facilities, equipment, and data covered in the Information Systems Facilities subsection.

Some telecommunications technologies in the Information Communications subsection are closely related, such as the spread-spectrum and frequency-hopping technologies commonly used in both civilian and military cellular telephone systems, which now normally incorporate cryptographic modules to protect the billing codes. The networks and switching technology items in the links and nodes of information communications systems are also

closely related. For example, link encryption protects the commercial backbone links in the installed base, which is usually some form of stream encryption.

Information Security section technologies are also closely related to the tracking, telemetry, and control (TT&C) encryption and decryption technologies for military systems and items in the Positioning, Navigation, and Time section. The commanding uplinks and mission data downlinks for some civilian and all military satellites such as the Global Positioning System (GPS) are protected by encryption to maintain positive control of the satellite systems and prevent mission data interception, intrusion, and spoofing.

TEMPEST is a code word that relates to specific standards used to reduce compromising emanations. The following declassified definition of compromising emanations appears on the Internet at <http://cryptome.org/ncsc-3.htm>:

Compromising Emanations (CE)—Unintentional intelligence-bearing signals, which, if intercepted and analyzed, disclose the national security information transmitted, received, handled or otherwise processed by any information-processing equipment.

Trade journals and foreign (Turkey, France) research occasionally covers TEMPEST devices (receivers and antennas used to monitor emanations) or TEMPEST attacks (using an emanation monitor to eavesdrop on someone). While the significant USG technical details remain classified, there is a large body of open source information on TEMPEST in the public domain.

The facilities and equipment for highly classified programs must be designed to suppress optical, acoustic and electronic emanations so that they cannot be intercepted and exploited. Computers, printers, monitors, keyboards and other devices may produce electromagnetic radiation. With the right antennas and receivers, these emanations are sometimes intercepted under ideal conditions from remote locations at a considerable distance. Display screens might be redisplayed and printers and keyboards recorded and replayed.

The principles on which TEMPEST is based have been well known and widely understood for decades. In fact a current (11 May 2003) website, <http://www.eskimo.com/~joelm/tempest.html>, is dedicated to explaining TEMPEST. For example, an item on this website explains that on 1 January 2001 John Young received eight more TEMPEST-related documents from his October 1999 NSA FOIA appeal. The printing in some of the documents furnished is so poor that the text is being retyped for posting on the Eskimo website. Currently documents available include: NSTISSAM TEMPEST/2-95, 12 December 1995, *Red/Black Installation Guidance*; NSA Specification No. 94-106, 24 October 1994, *Specification for Shielded Enclosures*; NACSIM 5000, 1 February 1982, *TEMPEST Fundamental*; and NSTISSI 7000, 29 November 1993, *TEMPEST Countermeasures for Facilities*.

Most military information system equipment is designed to suppress TEMPEST/Radio Frequency Interference (RFI)/ Electromagnetic Interference (EMI) electronic emanations at the box or chip level and sometimes both. Endorsed product lists are maintained by NSA. The TEMPEST Endorsement Programs (TEP) consists of three closely related NSA programs: the Endorsed TEMPEST Products Program, the Endorsed TEMPEST Test Services Program and the Zoned Equipment Program. The essence of these programs involves partnerships with industrial companies.

The National Security Agency (NSA) also provides a listing of commercial TEMPEST test services facilities that NSA has endorsed under the auspices of the Endorsed TEMPEST Test Services Program (ETTSP). The listing is for use by U.S. Government departments and agencies, U.S. Government contractors, and eligible TEMPEST product manufacturers to conduct TEMPEST testing related to the development and production of TEMPEST products. See <http://www.nsa.gov/isso/bao/tep.htm>.

BACKGROUND

Symmetric cryptography. The word “cryptography” was derived from two ancient Greek words: *kryptos*, meaning hidden, and *graphia*, meaning writing. Cryptography, the art and science of keeping messages secure, is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking

ciphertext (i.e., seeing through the disguise).¹ A *cipher* is a secret method of writing, whereby plaintext (or cleartext) is transformed into ciphertext (sometimes called a cryptogram). The word cipher has Hindu and Arabic roots. Western scholars turned the Hindu *sifr* into *zephyrus*, originally meaning the new Arabic² number zero. Zero was so important to the new set of numbers that mathematicians started calling all Arabic numerals ciphers. In the 1300s, Italian merchants started using Arabic numerals and even used them to send encrypted messages, which is how *cipher* came to mean “secret code.”³ The process of changing plaintext into ciphertext is called *encipherment*⁴ or encryption.⁵ The reverse process of transforming ciphertext into plaintext is called *decipherment* or decryption. Both encipherment and decipherment are controlled by a cryptographic key or keys.⁶

Symmetric key cryptography, the traditional approach to cryptography, is the basis for the most widely known and accepted cryptographic systems today. Secret-key cryptography (also called a symmetric or one-key system) has been used for centuries. Early forms (i.e., Caesar’s cipher) merely transposed written characters to hide the message. Secret-key systems use a single key, which is shared by two (or more) parties. Since secret-key encryption is typically much faster, it is normally used for encrypting larger amounts of data. A disadvantage of secret-key systems is that the secret key must be conveyed between sender and receiver by courier or some other physical or electronic trusted means, introducing a host of key management vulnerabilities. The plaintext data can be recovered from the ciphertext only by using exactly the same key that was used to encrypt the plaintext data. Unauthorized recipients of ciphertext who know the algorithm but do not have the correct key cannot decrypt the ciphertext data and obtain the original plaintext data.

Asymmetric cryptography. Much newer than symmetric cryptography, public-key cryptographic systems (also called asymmetric or two-key systems) use a pair of keys for each party. One of the keys of the key pair is “public,” and the other is “private.” The private key is not revealed. The public key can be known to the world. The public key of a pair of keys used for encryption and decryption requires the private key of the same pair. For a public-key system to be secure, the private key must be kept confidential—known only to its owner. The public key must also be known to belong to the addressee. Two widely accepted definitions may help understand public key cryptography:

- Public-key cryptography is particularly useful when parties wishing to communicate secretly cannot rely upon each other or do not share a common key. Asymmetric (public key) cryptography is a two-key cryptographic algorithm. The two keys have the property that, given the public key, it is *computationally* infeasible to derive the private key; and
- Public-key cryptography uses pairs of keys: a public key that is widely available, and a corresponding private key known only to the entity (person, application or service) that owns the keys. These key pairs are related in such a way that what is encrypted with the private key can only be decrypted with the public key and vice versa.

Cryptanalysis. In essence, cryptanalysis is the science and art of recovering the plaintext of an encrypted message without access to the key. The Department of Defense (DoD) has a slightly different definition:

¹ Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second Edition, John Wiley & Sons, Inc., 1995, p. 1.

² Our numbers evolved from the symbols that Indians used; by rights they should be called Indian numerals rather than Arabic ones. See Figure 14, p. 68, Seife, Charles, *Zero: The Biography of a Dangerous Idea*, Viking, New York, 2000.

³ Charles Seife, *Zero: The Biography of a Dangerous Idea*, Viking, New York, 2000, pp. 73, 81.

⁴ The International Standards Organization (ISO 7498-2) uses the terms “encipher” and “decipher” because the Romance languages have words derived from the Latin root word *crypta* that are associated more with the unpleasant ideas of death and burial than things hidden.

⁵ The word “encryption” has been coined from the word “cryptography.”

⁶ Dorothy Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, Reading, Mass., reprinted with corrections, January 1983, p. 1.

[Cryptanalysis consists of] the steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption.⁷

In the digital age, the art of encryption is simply about devising ways to hide text behind walls of random binary numbers. The so-called “black art of code-breaking” is all about using mathematics to find patterns in that binary number randomness—to discover order in a universe that is intended to present none.

A review of the terminology to be used in this section is in order. As used in this section, a *code* is defined as substitution at the level of words or phrases, whereas a *cipher* is defined as substitution at the level of letters. The term *encipher* means to scramble a message using a cipher, while *encode* means to scramble a message using code. Similarly, the term *decipher* applies to unscrambling an enciphered message, and *decode* to unscrambling an encoded message. The terms encrypt and decrypt are used more generally to cover scrambling and unscrambling with respect to both codes and ciphers.

Cryptanalysis could not be invented until a civilization had reached a sufficiently sophisticated level of scholarship in several disciplines, including mathematics, statistics, and linguistics. Between A.D. 800 and 1200, Arab scholars enjoyed a vigorous period of intellectual achievement. It was the Arab scholars who invented cryptanalysis. They succeeded in finding a method for breaking the monoalphabetic⁸ substitution cipher, a cipher that had remained invulnerable for several centuries.

Cryptology presents a difficulty not found in all classic academic disciplines: the need for a continuous challenge-and-response interaction between cryptographers and cryptanalysts. This scientific interaction begins with a challenge from cryptographers, which starts each cycle with a new algorithm design, and a response from the cryptanalysts through continuing peer review. During these reviews, the cryptanalysts try to find and expose flaws in the design, which is usually harder to do than designing the cryptographic algorithms. The result of the evolutionary struggle in this scientific peer review method is a healthy, competitive, public testing process that produces strong cryptography (see Figure 17.0-1). Over the centuries, the ongoing battle between cryptographers and cryptanalysts has inspired a whole series of remarkable scientific breakthroughs as cryptographers have striven to construct ever-stronger cryptography and cryptanalysts have continually invented more powerful methods of analysis. The Recording Industry Association of America, Inc.’s case⁹ is a concise explanation of the value of openness and the peer review process to cryptologic evolution:

It should not be surprising, as paradoxical as it may seem at first blush, that researchers and other scientists who study security and privacy customarily embrace and value openness and wide publication even of results that expose vulnerabilities. Such publication represents the natural advance of knowledge in a relatively new field of scientific study.

⁷ Joint Publication (JP) 1–02 *Department of Defense Dictionary of Military and Associated Terms*, as amended through 9 January 2003: available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, p. 135.

⁸ The *monoalphabetic substitution cipher* is the general name given to any substitution cipher in which the cipher alphabet consists of either letters or symbols, or a mix of both.

⁹ Grayson Barber (GB 0034), Grayson Barber, L.L.C., 68 Locust Lane, Princeton, NJ 08540; (609) 921-0391; Frank L. Corrado (FLC 9895); Rossi, Barry, Corrado, & Grassi, 2700 Pacific Avenue, Wildwood, NJ 08260 (609) 729-1333; Attorneys for Plaintiffs. IN THE UNITED STATES DISTRICT COURT, FOR THE DISTRICT OF NEW JERSEY. EDWARD W. FELTEN; BEDE LIU; SCOTT A. CRAVER; MIN WU; DAN S. WALLACH; BEN SWARTZLANDER; ADAM STUBBLEFIELD; RICHARD DREWS DEAN; and USENIX ASSOCIATION. Hon. Garrett E. Brown, Jr., a Delaware non-profit non-stock Case No. CV-01-2669 (GEB) corporation, Civil Action. Plaintiffs. vs. RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.; SECURE DIGITAL MUSIC INITIATIVE FOUNDATION; VERANCE CORPORATION; JOHN ASHCROFT, in his official capacity as ATTORNEY GENERAL OF THE UNITED STATES; DOES 1 through 4, inclusive, Defendants. DECLARATION OF MATTHEW BLAZE. http://www.salon.com/tech/log/2001/08/31/dmca_animals/index.html. 9/22/2001, 8:56 AM.

A basic rule of cryptography is to use published, public, algorithms and protocols. This principle was first stated in 1883 by Auguste Kerckhoffs: in a well-designed cryptographic system, only the key needs to be secret; there should be no secrecy in the algorithm.¹⁰

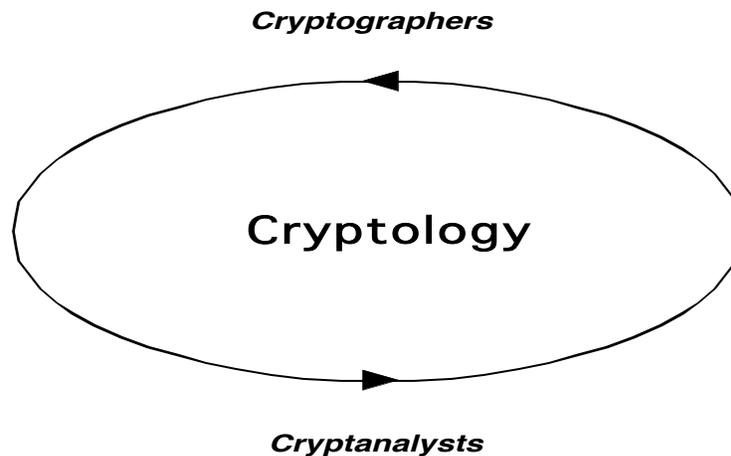


Figure 17.0-1. The Cryptanalytic Testing Process Provides the Insight Necessary for Designing Strong Cryptography

Steganography is that branch of information privacy that attempts to obscure the existence of data through such devices as invisible inks, secret compartments, and use of subliminal channels.¹¹ Steganography is one of the oldest methods used for message security. It was the threat of enemy interception that originally motivated the development of techniques for disguising a message so that only the intended recipient could read it. As early as the 5th century B.C., the Spartans used a *skytale*, the first military cryptographic device (really a form of steganography) for disguising military messages.¹² A somewhat similar device was also in use in China more than 5,000 years ago. Chinese generals sent messages from the battlefield by wrapping a band of silk around a thin pole and then writing on the material. Only someone who had a pole with the same diameter could read the message. To others the message would look like a band of silk with a random pattern of markings. This is one of the earliest documented forms of encryption.¹³ Later examples of steganography are the use of invisible inks and microdots to conceal messages. Steganography has its place in security systems. It is not intended to replace cryptography, but to supplement it. Hiding a message covertly with steganographic methods reduces the chance of the message being detected. However, if that covert message is also encrypted, it requires cryptanalysis to recover the plaintext.

Whereas cryptography may not necessarily hide the presence of a secret message, steganography is intended to conceal the very existence of a message. Examples of steganography are the old methods of invisible inks¹⁴ and

¹⁰ Bruce Schneier, *CRYPTO-GRAM*, Counterpane Internet Security, Inc., schneier@counterpane.com <http://www.counterpane.com>

¹¹ Alfred J. Menezes, et al., *Handbook of Applied Cryptography*, CRC Press, New York, 1997, p. 47.

¹² A skytale consisted of a staff of wood around which a strip of papyrus, leather, or parchment was wrapped. The secret message was written on the strip down the length of the staff. The strip was then unwound and sent on its way. The strip was rewrapped around a staff of the same diameter by the recipient re-forming the message.

¹³ Paul E. Proctor and Christian Byrnes, "The Politics of Cryptography," *Performance Computing*, October 1999.

¹⁴ In an intercepted message from the Japanese naval attaché in Buenos Aires to the Naval General Staff in Tokyo dated Oct. 25, 1942, the attaché says that he is using Gordon's Gin, piramidon, pure prussic acid, and iron chloride. He asks whether the gin has to be Gordon's. No answer was observed. Phyllis Altrogge, McLean, in Letters to the Editor, *Washington Post*, 26 June 2001, p. A16.

microdots.¹⁵ In the digital age, messages can be concealed in graphic images, since most graphics standards specify more gradations of color than the human eye can notice. The steganography algorithm looks for the most complex parts of the image, where neighboring pixels are most different from one another, and adds the data to the least significant bits of the pixels. Without changing the graphical image noticeably, a 64-kilobyte message can be incorporated in a 1,024 × 1,024 gray-scale picture. Programs are available in the public domain for embedding messages in graphics.

There are many forms of steganography. Messages can be hidden in music audio tracks. The hidden meaning of a unique word or phrase embedded in a routine message, which has been designated to execute some preplanned reaction by the recipient, is also considered a form of steganography. Like the one-time pad, this steganographic protocol is, in itself, unbreakable, assuming perfect insider security on both ends. But, like symmetric cryptography, the key (or meaning in this case) must be prepositioned in advance.

Biometrics. Biometric data is derived from a human being and must be processed by a secure biometric identity-management system to verify claimed identity (*authentication*) or discover the individual's true *identity*.¹⁶ A *biometric* is a scale of suitable length and granularity for measuring and objectively specifying the parameters of a human physiological characteristic or personal behavioral trait that can be used to securely *identify*, or *verify* the claimed identity of, an enrollee¹⁷ accredited in a secure biometric identity-management system.

The information-security community generally accepts three ways through which a person can be *positively identified*; that is, prove you are who you say you are, prove you are not who you say you are not, or prove you are not among a group of people already known to the system. This proof can be (1) *something you have* (a credit card or driver's license), (2) *something you know* [a password or personal identification number (PIN)], and (3) *something you are*. Using relatively forge-proof unique identifiers of a human body, which can be objectively measured with biometrics, is a way of specifying *something you are*, which can be used for *authentication* and *identification* purposes, and it has particular value for use as a countermeasure against information-system identity-fraud security exposures. *Something you are* can be determined by objectively measuring a human anatomical or physiological trait that is unique to an individual, such as a fingerprint or iris pattern.¹⁸ Of course, for very small, highly sensitive operations, personal recognition, with trusted third-party introductions, is still the best and most secure system for identification, access, and circulation security.

Smart cards. In most technical references, the term "chip card" covers (1) *smart cards*, featuring embedded complementary metal-oxide semiconductor (CMOS) microcontrollers and memory chips; (2) *memory* or *dumb cards*, featuring embedded, electronically erasable, programmable read-only memory [considered software] (EEPROM) chips; and (3) both *contact* and *contactless* (or *proximity*) cards. *Contact* chip cards conform to ISO 7816 and are easily identified by their standard metallic contact pads. *Contactless* smart cards, which are in conformance with ISO 14443 (Type A, B, or C), do not have power cells but have embedded loop antennas, usually on the back. Contactless cards communicate with this embedded loop antenna by radio-frequency (RF) modulation and are energized by movement within the electromagnetic field produced by the card-reader antennas.

Smart-card applications are increasingly replacing passwords in logical access and circulation control systems, and they are being used for digital signatures. They are now used in most wireless system applications to protect billing codes and provide nominal privacy for the RF links. The use of chip-card technology is encouraged for military applications because the wallet size of the chip-card is convenient. Chip cards are the most widely used and abundant of all the identity-management tools. In addition to being a fairly mature technology that has undergone a

¹⁵ Used by the Germans, who had perfected miniature photography to conceal messages in the periods in sentences. Often cited in histories and popularly used by novelists.

¹⁶ *Frequently Asked Questions, Definitions*, International Biometric Group. See http://bioprivacy.org/faq_main.htm and Michelle C. Frye, *The Body as a Password: Considerations, Uses and Concerns of Biometric Technologies*, A Thesis Submitted to the Faculty of the Graduate School of Arts and Sciences in Georgetown University, Washington, D.C., 27 April 2001.

¹⁷ *1999 Glossary of Biometric Terms*, Association for Biometrics (AfB) and International Computer Security Association (ICSA), see <http://www.afb.org.uk/>

¹⁸ Valene Skerpac, "Got Biometrics?" *Information Security Bulletin 41*, April 2000, p. 41.

long period of extensive tests in actual use, these cards are also the least expensive and therefore most affordable solution for most military system applications. Any of the many existing bar codes, magnetic-stripes, and proximity-card access features that may be required can be integrated within the same multifunction smart card. The card format is preferred for military service over tags and other tokens because it provides a convenient and versatile platform that can house an RF antenna, and because chip cards are the highest volume semiconductor product manufactured worldwide.

Secure identity-management systems. The system architecture for a militarily critical secure biometric identity-management system will usually contain the following seven top-level functional system segments: (1) enrollment (or data collection); (2) transmission (or signal processing); (3) decision; (4) storage; (5) verification; (6) identification; and (7) termination. These are the building blocks for developing a secure integrated information system for processing *biometric data* and maintaining its integrity and security throughout the life cycle of the data.

A biometric system includes all of the hardware, associated software, and interconnecting infrastructure required to enable end-to-end biometric processing. If the biometric process is an integral part of a larger system, then this definition extends to any part of the larger system that holds relevant user data, such as directories, transaction logs, and digital time-stamping where proof of timeliness may be required. In addition, in such a system the process extends to the point after which authentication or identification is complete and no longer required for the larger system to function.

Firewalls. Network firewalls are software or hardware/software systems interposed between assets to be protected, such as workstations; local area or enterprise and larger networks; and external, potentially hostile or uncontrolled networks and systems. Note that all network firewalls are logical single points of failure and bottlenecks and create denial-of-service vulnerabilities as well as manage or reduce other vulnerabilities. There are four generally accepted basic technologies, named for the methods used to protect a network or stand-alone workstation from unauthorized access by Internet “hackers” or “crackers”: packet filtering, application proxy, stateful packet inspection, and hybrid firewalls.

Packet filtering is the most basic form of firewall. When packets do not meet predetermined rules or “policies” set by the network administrator, they are eliminated or filtered by a router or a firewall. Packet filters can be configured to check the source and destination address of the packets and the type of protocol embedded in the packet, rejecting those from untrusted sources and addressed to destinations forbidden by the security policy. The network administrator should be able to set the packet filter so that it will reject any packets coming from an “untrusted” originator on the Internet side of the router (for example, those that contain the “Telnet” protocol), which is a major method of penetration. The Telnet protocol can be used to provide remote control of a workstation, server, or other network device.

Application proxy. An application proxy can be either software or a device that makes software requests on behalf of entities on the network. Most proxy servers are configured to perform Internet browser functions for workstations in the “trusted,” or internal, network. The workstation browser sends its browsing request to the proxy server rather than the destination Web site server on the Internet. The proxy server can then examine the actual application program data and responses from the Internet contained within the packet and reject the packet or pass it on to the originating workstation in accordance with the security policy created by the network administrator. For example, a proxy server might be configured to reject all inbound packets that contain files with .EXE or .COM suffixes. Hackers can use these common executable file types to introduce dangerous virus and work files into a network.

Stateful packet inspection firewalls keep track of all packets associated with specific sessions passing through the firewall. A typical session between two computers will consist of several thousand packets, each of which is identified by a unique source and destination address and a sequence number that allows all of the packets to be reassembled into the correct data file at the destination computer. In very large networks, thousands of sessions may be occurring simultaneously. A stateful inspection firewall keeps track of all the concurrent sessions. Each packet of data is checked to ensure that it belongs to its proper session. Any packets not part of an existing session are rejected. In addition to checking and validating the communication session by the source and destination addresses of the machines in the session and ensuring that all packets belong to the proper session, the firewall further screens the packet at the software port level. (A software port is a unique address extension that the application software uses to communicate with Web sites on the Internet.) Filtering at the software application port level provides an

additional layer of control over the network administrator to ensure that only authorized transactions are allowed through the firewall.

“Hybrid firewalls” is the generally accepted name for the firewalls that blend combinations of firewall methods. There are various advantages and disadvantages in each firewall method outlined above. Hybrid firewalls are the developers’ products that combine the advantages of some or all of the other single-concept firewalls. The one principal disadvantage of hybrids is that they usually require the purchase of additional hardware and software, which is not typically bundled with existing network routers or gateways currently on the market.¹⁹

The sixth row in the data sheet table of each technology item is used to outline the specific factors that result in an affordability issue for that particular technology; however, the cost of the information-security technology applications is decreasing and will continue to decrease for some time. In general, affordability should not be the principal acquisition issue for information-security technologies. In perhaps something of an oversimplification, information-security protection for sensitive data in any storage or transit state can be reduced to cryptography and steganography.

Competitive new general-purpose information-system-security technologies and COTS products that include strong cryptographic functionality, at little or sometimes no apparent additional cost, are appearing in the open national and international markets. However, the cost of suitable additional staffing required to manage and operate the secure information systems can be significant. Providing additional processor power and memory capacity to support the cryptographic functionality for large complex systems is usually also a significant affordability issue. Most of this new cryptographic functionality can be automated, and staff augmentation minimized. However, there is still the persistent, potentially expensive requirement to recruit (or retrain) technically qualified personnel worthy of cryptographic system trust and responsibility to operate and manage the system and to support the required end-user indoctrination, training, standardization, and test and evaluation programs required for optimum information system security.

Several of the major products in COTS network firewalls have been hybrids of proxies and application-level gateways, including Raptor Eagle, NAI/TIS Gauntlet, Harris’ Nighthawk, and SCC’s Sidewinder. Personal firewalls, intended to protect only the PC/workstation they are installed on, are easily configured, effective against many attacks, and widely available at reasonable cost, with trade names such as Black ICE Defender, Personal Firewall, and ZoneAlarm. Another form of firewall, the firewall appliance, is being offered as a low-cost, low-performance integrated hardware/software package to protect simple, small office/home office (SOHO) networks, with reduced configuration difficulties described above.

Competition in the domestic and foreign markets is driving realignments of information-security product lines and consolidation of companies. The information-security industry is still in a period of growth, change, and consolidation. The cryptographic and steganographic manufacturers and distributors listed in the tables of the symmetric key and steganographic technology item data sheets were included as examples of the wide availability of the products of these technologies and are like snapshots that were correct only at the time they were drafted for these technology items. The two Web sites that maintain the product information are noted with the product tables and should be checked for the latest status of these products.

Information system functional areas. The Information Security section organizational concept has been included to maintain the perspective of information security as a functional area (or system segment) of information systems (or technology). Information security is generally regarded as an essential functional area, system segment, or feature of all military information systems.

Because the same secure information systems may be critical to many of the operations defined by DODD 3600.1 (draft), a brief overview of those operations is presented as the context for an explanation of why particular information-security technologies are treated. Figure 17.0-2 illustrates the range of information operations mandated by DODD S-3600.1. The basis for distinguishing, at the highest level, among “pre-hostility” and “post-hostility” operations is that national security cannot be assured in the absence of appropriate pre-hostility DoD operational capabilities. Information-system requirements are often markedly different in pre- and post-hostility scenarios for

¹⁹ See “Firewall Technologies Explained”: www.group1fw.com/fw_tech.html>

secure and covert operations and corresponding capabilities to sustain operations under electronic warfare, physical damage, and chemical, biological, and other threat-driven environments.

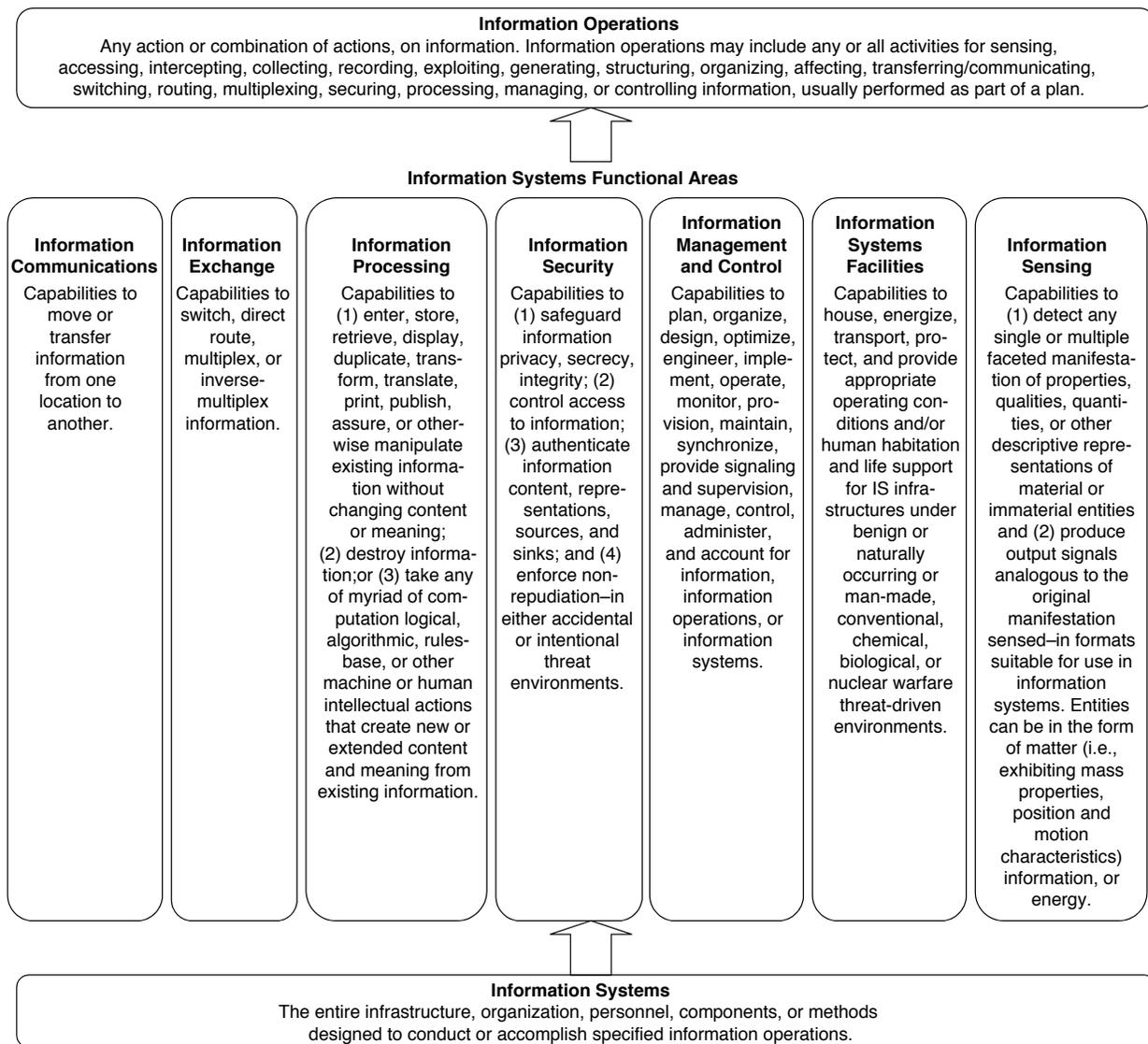


Figure 17.0-2. Information Systems Functional Areas

Explicit reference to the need to support offensive and defensive information operations reflects DODD 3600.1's (draft)²⁰ definitive statement that information operations are actions taken to affect adversary information and information systems while defending one's own information and information systems. *Joint Vision 2010* established the following requirement: "*information superiority will require both offensive and defensive information operations*" (italics added). Offensive information operations will degrade or exploit an adversary's collection or use of information. It will include traditional methods (such as a precision attack to destroy an adversary's command and command-and-control capabilities) and nontraditional methods, such as electronic

²⁰ In formal (final) coordination at this writing (9 May 2003), and while not yet formally approved the information operations concepts defined in the draft.

meaconing, intrusion, jamming, and interception (MIJI) into an information and control network to convince, confuse, or deceive enemy military decision-makers.

Defensive information operations to protect our ability to conduct information operations will be one of the biggest future challenges for U.S. armed forces. Traditional defensive information operations requires all of the information-security disciplines, including disciplined personnel security and background investigations; physical, optical, acoustic, and electronic facility and equipment security measures; encryption; and the full range of OPSEC policies, procedures, and techniques. Nontraditional actions will range from antivirus protection to innovative methods of secure data transmission. In addition, increased strategic-level programs will be required in this critical area.

Historically, a direct relationship has always existed between technologies supporting correlative offensive and defensive military operations. For example, encryption technologies are consummately interrelated to code-breaking technologies and vice versa. Similarly, electronic countermeasure (ECM) techniques essentially may define effective electronic counter-countermeasures (ECCMs). Numerous other examples exist and, despite U.S. non-aggression policies, it is prudent for the DoD, armed forces, and homeland defense organizations to pursue the development and employment of both offensive and defensive information technologies.

From a national security perspective, the most familiar information operations are those invoked after active conflict has commenced. Examples of post-hostility information operations include command, control, and intelligence (C2I) operations; ECMs; psychological warfare; and operations in support of logistics and other military operations associated with conventional and other forms of warfare for recovery and reconstitution.

It must be emphasized that post-hostility does not mean post-military conflict alone—nor does it imply target sets limited to physical entities with military-only value. Targets may include the homeland infrastructure, manufacturing, transportation, utilities, political institutions, and information systems. Economic, political, and offensive information operations battles could be fought and won or lost in the total absence of any traditional physical military conflict.

Pre-hostility information operations are all other information operations that play direct or indirect roles in U.S. national security preparedness to conduct any and all forms of authorized offensive and defensive warfare. From a national-security perspective, this information operations category includes any information operations that help avert hostilities where possible and ensure victory otherwise. Thus, in accordance with DODD 3600.1 direction, prehostility information operations include all operations needed to prepare for conflict or, if possible, to prevent escalation to military or other forms of combat. Some prehostility operations must continue during and after hostilities.

Information technologies are in the design, development, production, and implementation of information systems, which, in turn, are employed to activate or conduct a wide range of information operations.

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Department of Defense Dictionary of Military and Associated Terms, Joint Pub. 1-02.

The enormous range of information operations implied in this definition gives rise to literally hundreds of categorically different information systems and an almost unlimited number of identifiable information technologies.

The selected information-system structural concept is consistent with the industry-wide practice of specifying large information systems in as many as seven functional areas or system segments, which are subsets of information system capabilities that accomplish or support specified categories or subsets of information operations (see Figure 17.0-3). Functional area (or system segment) requirements are normally, and purposefully, defined or specified so that engineers are afforded the greatest possible freedom in making particular hardware or software design choices.

operations types, the danger exists that the same functional area technologies (e.g., “Information Processing”) may be assessed differently by various warfare-operations-specific technical working or author groups, using potentially dissimilar criteria. At best, even if perfectly consistent results are obtained, eliminating the duplication of effort and inefficient use of scarce resources is difficult. Thus, other options for organizing the Information Technology section have been considered but have been determined to be less useful.

SECTION 17.1—CRYPTOLOGIC TECHNOLOGY

Highlights

- Cryptologic technologies and products provide the security to information systems for the required secure, reliable, wideband communications links and information-management nodes that extend through the chain of command and channels of communications from the NCA to the warfighter and that provide information dominance to U.S. forces.
- The worldwide proliferation of encryption has coincided with the explosive growth of the Internet. The civilian sector is now advancing the development, production, and use of civilian commercial cryptologic products.
- For the first time, the symmetric cryptography standard,²¹ which is the standard for the United States and will soon be the standard for most of the world, is based on an algorithm developed outside the United States.
- There are opportunities for the U.S. cryptologic community to influence the future of the information age through cooperation with and participation in the deliberations of international standards bodies.
- There is always the possibility of the discovery of a new attack or a breakthrough in mathematics that makes the solution of the underlying cryptographic problem, which provides the security for a cryptographic system, faster and easier.
- There also is always the possibility of a sudden order-of-magnitude increase in processing power that shortens the time required for an exhaustive key search to the point that the cryptographic algorithm does not provide protection of encrypted data for the originally planned and expected length of time.

OVERVIEW

The cryptologic technologies covered in this section, many of which meet or exceed the minimum threshold requirements for military criticality, are in the public domain. They are widely available in the world market now or will be in 5 years or less. U.S. Government Type 1 cryptologic technology, which falls within the purview of the NSA, is generally classified and therefore not covered in the Information Security section.

The cryptologic technology items in this subsection are closely related to some of the technology items in the Information Technologies section because cryptographic modules, components, and systems must be integrated in, if not an integral component or module of, the basic information-processing system hardware and software architecture during system development and then during production.

Computer operating systems and some applications now incorporate high-performance features and meta-processing techniques that are shortening the cryptanalytic time required for an exhaustive key search, thus making the Information Processing subsection technologies closely related to the cryptanalysis item in this subsection.

The time required for cryptanalyses is a function of both knowledge in the field of mathematics and the state of the art in high-performance computing. Cryptanalytic procedures and techniques are dependent on the state of the art in high-performance computing because processing power determines the length of time required to perform an exhaustive key search, which in turn governs key life cycles, which are a function of key lengths.

Some telecommunications technologies in the Information Communications subsection are closely related, such as the spread-spectrum and frequency-hopping technologies commonly used in both civilian and military

²¹ *Advanced Encryption Standard (AES)*, FIPS PUB 197, 26 November 2001, is based on *Rijndael*, developed by Joan Daemen and Vincent Rijmen of Belgium.

cellular telephone systems, which now normally incorporate cryptographic modules to protect the billing codes and the privacy of conversations over the RF segments. The networks and switching technology items in the links and nodes of information communications systems are also closely related to the cryptography items. For example, link encryption, used to protect most of the commercial backbone links in the installed base, is usually some form of stream encryption.

Cryptologic technology items are also closely related to the TT&C encryption and decryption technologies in the Positioning, Navigation, and Time Technology section. The commanding uplinks and mission data downlinks for both civilian and military satellites, such as the GPS, are increasingly protected by encryption to maintain positive control of the satellites and prevent mission data interception, intrusion, and spoofing.

BACKGROUND

It will help to understand the contents of this subsection, as well as the individual technology items, if the following definitions are kept in mind:

- **Cryptology** is commonly used as a collective term that includes cryptography and cryptanalysis. There are two basic classes of cryptographic systems: *secret key* (also called *symmetric*) and *public key* (also called *asymmetric*).
- **Symmetric** (secret key) cryptography is a form of cryptography in which the key required for encrypting is the same as the key required for decrypting. Secret-key systems use a single key, which is shared by two (or more) parties.
- **Asymmetric** public-key algorithms use two mathematically related keys: a public key and a private key. The two keys have the property that, given the public key, it is *computationally* infeasible to derive the private key. Asymmetric cryptographic technologies are unique enabling elements of secure information systems for key management, authentication, nonrepudiation, and integrity applications.
- **Cryptanalysis** is “The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption.”²²
- **Key recovery** is the generic term for systematic protection of encryption keys to prevent their loss.²³
- **Embeddable programmable cryptographic processors** are very large-scale integrated (VLSI) circuits on CMOS chips that can be embedded in information-system hardware. Encryption algorithm changes and upgrades can be made to embedded programmable cryptographic processors with software, without having to make any changes to the hardware.

The history of cryptology is one of strife between cryptographers who develop codes and cryptanalysts who try to break them. It may come as a surprise that the strength of cryptographic algorithms is like most of the great truths of science. Scientific truths, which are always provisional, must be proven repeatedly with each subsequent identical experiment following a discovery. Later experiments must produce identical results for generations of investigators. Scientific truths are always subject to modification or disproof by the next experiment. Cryptographic algorithms are always subject to modification or disproof by the next cryptanalytic attack. The strength of encryption algorithms is based on assumptions and inferences about the hardness of the underlying problem; encryption therefore can never be proven to be unbreakable or unconditionally secure. An algorithm can only be proven to be insecure by successfully attacking the ciphertext and recovering the plaintext, which does happen from time to time. Until broken, most encryption algorithms are accepted as “strong.”

Cryptography is composed of two basic elements: an algorithm (or cryptographic methodology) and a key. Algorithms are complex mathematical formulae and, in the digital age, keys are strings of binary digits or “bits.” The same algorithm, or algorithms that are designed to work together, must be used for encryption and decryption.

²² Joint Publication (JP) 1-02 *Department of Defense Dictionary of Military and Associated Terms*, as amended through 9 January 2003; available at www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

²³ “Recovery of Encrypted Data,” *ITL Bulletin*, April 2002, p. 3.

The security of a cryptosystem must not depend on keeping the crypto-algorithm secret,²⁴ because sooner or later the secret algorithm will be discovered independently or stolen. The security of strong cryptography must depend only on the length of the key. Generally, the longer the keys, the more secure the cryptography. This is because the longer the key, the more time it will take to perform an exhaustive key search. With the present knowledge of mathematics and processor strength, at some key length an exhaustive key search becomes computationally infeasible.

The longer cryptographic algorithms remain in the public domain under peer review and unbroken, the stronger they are assumed to be. But there is always the possibility of the discovery of a new attack or breakthrough in mathematics that makes the solution of the underlying problem faster and easier. And there is always the possibility of a sudden order-of-magnitude increase in processing power, which shortens the time required for an exhaustive key search to the point that the cryptographic algorithm does not provide protection of encrypted data for the required length of time. Of course, to provide a high level of security for any information system, encryption algorithms (no matter how strong) must be integrated in system implementations that also have sound protocols, authentication, and secure connections to secure nodes.

Projections for cryptologic technologies are difficult because there are so many unknowable variables in mathematics and computer science, both of which control the future of these technologies. The only reasonable generalized projection with respect to the rate of change in these technologies that could be made is that the rate of change in cryptologic technologies might be forecast as “glacial” for the foreseeable future. The following two life histories of cryptographic technologies illustrate this hazy forecast. One of the oldest and most successfully cryptographic systems, the One-time Pad, is still in use and although somewhat awkward and time consuming to use, it is still considered unbreakable by the cryptologic community. After almost 30 years, the useful life of the “Data Encryption Standard” (DES) is still not over, although with the advances in knowledge of mathematics and increasing processing power, the consensus of the cryptologic community is that its life is definitely limited. Since DES was published as a standard on 23 November 1976, it has become the most successful and widely used symmetric block cipher in national and international business and financial applications. With the approaching obsolescence of DES, the U.S. Government made a determination during the summer of 1997 that a symmetric block successor to DES must be developed soon and on 12 September 1997 started the system acquisition process with an announcement of an open international competition for candidate algorithms in the *Federal Register*. It took a little over 4 years of intensive effort, with a great deal of help from the international cryptologic community, to develop the Advanced Encryption Standard (AES) and get it approved and published as a standard on 26 November 2001.

The full key-management life cycle extends from key generation through use, protection, and key destruction. The life of a key is a function of the rate of mathematical discoveries and the rate of processor power development. If the cryptographic algorithm produces strong cryptography and has successfully undergone peer review for a prolonged period, then the cryptanalysts usually must resort to some form of exhaustive key search to recover the plaintext. The time required to perform an exhaustive key search determines the serviceable secure life cycle of a key, which of course is a function of the state of mathematical knowledge and processor power. It may be impractical, or even computationally infeasible, to recover plaintext protected by some forms of strong cryptography. In this regard, one important aspect in the broader subject of cryptographic key life cycles is *key recovery*. Key recovery may be required for two reasons:

- If the keys used to encrypt data with strong encryption are lost, then the data are probably lost; and
- Lost keys may affect continuity of operations.

Encryption keys must be carefully protected during their life cycle. It is vital that they be carefully protected from unauthorized access and also from loss if the “owner” of the key leaves or is unable to perform her or his duties. Since encryption, authentication, and verification keys can affect the continuity of operations, these keys must be copied or archived to allow recovery. It is generally undesirable to implement key recovery for private signing keys because this would weaken a “non-repudiation” claim: the key holders would no longer have sole control of their signing keys. Therefore, it is usually undesirable to use one key for both encryption and digital

²⁴ Simon Singh, *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, New York, 1999, p. 12.

signatures. Key recovery is primarily required for the recovery of stored data that has been encrypted. Copies of the keying material needed to recover data or resume operations should be securely maintained in the custody of a trusted key-recovery facility or officer who is not the normal owner or user of the encrypted data or keying material. Types of keying materials that require backup and secure storage for key recovery are

- Keys used to decrypt data;
- Keys used to decrypt encryption keys that are used to decrypt data;
- Keys used to authenticate data;
- Keys used to verify digital signatures; and
- In unusual operational circumstances, private signing keys.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.1. CRYPTOLOGIC TECHNOLOGY

17.1-1	Symmetric Key Cryptographic Technology	MCTL-17-21
17.1-2	Asymmetric Key Technology	MCTL-17-24
17.1-3	Cryptanalytic Technology	MCTL-17-28
17.1-4	Embeddable Programmable Cryptographic Processor Technology	MCTL-17-32

MCTL DATA SHEET 17.1-1. SYMMETRIC KEY CRYPTOGRAPHIC TECHNOLOGY

Critical Technology Parameter(s)	(1) They must have undergone extensive open peer review, and no attacks been found that allow faster attacks than an exhaustive key search; and (2) have at least a 128-bit key space.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Computers with a composite theoretical performance (CTP) of 45,000 million theoretical operations per second (Mtops) or greater and software specially designed to perform randomness, correlation, weak key, and symmetry under complementation tests to evaluate the strength of new symmetric encryption algorithms during development, test, and evaluation.
Unique Software	Operating systems and application software implementing cryptographic functionality must be specially designed and integrated so that the information systems match and maintain the common criteria ²⁵ evaluation assurance level (EAL) protection profile of the cryptosystem during the operational life cycles of the systems. The system engineering and integration, user system interface, algorithms, and key generators must have zero defects. Cryptographic module security must comply with the provisions of Security of Cryptographic Modules, FIPS Publication (PUB) 140-1, the requirements of the NSA, and it must be consistent with ANSI standards for symmetric key cryptography.
Major Commercial Applications	The U.S. Government cryptographic and cryptanalytic systems and those of a few foreign governments are believed to still be far ahead of most commercial systems, if for no other reason than because significant government resources have been devoted to cryptology, especially since the beginning of World War II. However, although civilian commercial cryptographic applications may not yet equal the strength of government systems, the gap between the strength of government and civilian commercial systems may be closing. In large part, the strength gap may be closing because of the open peer review system and the significant R&D investments that the information systems industry is making in commercial cryptographic systems.
Affordability Issues	Competitive new general-purpose information-system security COTS products that include strong cryptographic functionality, at little or no apparent additional cost, are appearing in the open market; however, the cost of additional staff, processor power, and memory capacity to operate, manage, and maintain the cryptographic functionality for large complex systems is a significant affordability issue.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI, XIII.

BACKGROUND

Cryptology is “the science that deals with hidden, disguised, or encrypted communications. It embraces communications security and communications intelligence.”²⁶ Cryptology is the branch of mathematics encompassing cryptography and cryptanalysis, and its practitioners are cryptologists. Modern cryptologists are usually trained in advanced theoretical mathematics and computer programming.

²⁵ The *Common Criteria* is also ISO 15408.

²⁶ Joint Publication (JP) 1-02 *Department of Defense Dictionary of Military and Associated Terms*, as amended through 9 January 2003: available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

Cryptology is commonly used as a collective term that includes both cryptography and cryptanalysis. However, David Kahn provides a broader definition: “Cryptology is the science that embraces cryptography and cryptanalysis, but the term ‘cryptology’ sometimes loosely designates the entire dual field of both rendering signals secure and extracting information from them.”²⁷

There are two basic classes of cryptographic systems: *secret key* (also called symmetric systems) and *public key* (also called asymmetric systems). *Hybrid* (or mixed) systems that use both types of cryptographic keys, hash functions, and reversible and irreversible algorithms are also widely used forms of cryptography. Most modern cryptographic solutions for business are hybrid systems that are a combination of *symmetric*, or secret key, and *asymmetric*, or public key, technologies because hybrid systems simplify key agreement.

Cryptography is a combination of two basic components: an *algorithm*²⁸ (or cryptographic methodology) and a *key*.²⁹ Algorithms are complex mathematical formulae, and, in the digital age, keys are strings of bits. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption and decryption. Two related algorithms are generally required: one for encryption and the other for decryption. Keys may be any of a large number of binary values. The range of possible values of the key is called the *keyspace*.

The word “*cryptography*” was derived from two ancient Greek words: *kryptos*, meaning hidden, and *graphia*, meaning writing. Cryptography, the art and science of keeping messages secure, is practiced by cryptographers. Cryptography is also the science and study of secret writing. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext (i.e., seeing through the disguise).³⁰

A *cipher* is a secret method of writing, whereby plaintext (or cleartext) is transformed into ciphertext (sometimes called a cryptogram). The word cipher has Hindu and Arabic roots. The Hindu *sifr* was turned into *zephirus*, originally meaning the new Arabic³¹ number zero, by Western scholars. Zero was so important to the new set of numbers that mathematicians started calling all Arabic numerals ciphers. In the 1300s, Italian merchants started using Arabic numerals and even used them to send encrypted messages, which is how *cipher* came to mean “secret code.”³²

The process of changing plaintext into ciphertext is called *encipherment* or encryption.³³ The reverse process of transforming ciphertext into plaintext is called *decipherment* or decryption. Both encipherment and decipherment are controlled by a cryptographic key or keys.³⁴

The financial service industry switched to an interim 128-bit key multiple encryption version of the DES, Triple Data Encryption Standard (Triple-DES), during the selection and promulgation of the AES. The minimum

²⁷ David Kahn, *The Codebreakers: The Story of Secret Writing*, Scribner, New York, 1996, p. xviii.

²⁸ The word algorithm (a variant of *algorism*) is said to have been derived from Abu Ja’far Mohammed ibn Musa al-Khwarizmi’s name. He was an Arabian mathematician of the court of Mamun in Baghdad, c. 825. His semantic legacy also includes the word *algebra*.

²⁹ For example, a DES key consists of 64 binary digits (“0”s or “1”s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. The 8 error-detecting bits are set to make the parity of each 8-bit byte of the key odd (i.e., there is an odd number of “1”s in each 8-bit byte).

³⁰ Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second Edition, John Wiley & Sons, Inc., 1995, p. 1.

³¹ Our numbers evolved from the symbols that Indians used; by rights they should be called Indian numerals rather than Arabic ones. See Charles Seife, *Zero: The Biography of a Dangerous Idea*, Viking, New York, 2000, Figure 14, p. 68.

³² *Ibid.*, pp. 73, 81.

³³ The International Standards Organization (ISO 7498–2) uses the terms “encipher” and “decipher” because the Romance languages have words derived from the Latin root word *crypta* that are associated more with the unpleasant ideas of death and burial than things hidden. The word “encryption” has been coined from the word “cryptography.”

³⁴ Dorothy Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, Reading, Mass., reprinted with corrections, January 1983, p. 1.

AES key size is 128 bits. The European de facto standard, the International Data Encryption Algorithm (IDEA), is a 128-bit algorithm.

Cryptography is sometimes confused with *steganography*, the second basic way a message may be hidden and by far the older way. Whereas cryptography may not necessarily hide the presence of a secret message, steganography is intended to conceal the very existence of the message. Examples of steganography are the old methods of invisible inks and microdots. In the digital age, messages can be concealed in any digital media, such as graphic images, since most graphics standards specify more gradations of color than the human eye can notice. Most image steganography algorithms look for the most complex parts of the image, where neighboring pixels are most different from one another, and add the data to be hidden to the least significant bits of the pixels. Without changing the graphical image noticeably, a 64-kB message can be incorporated in a 1,024 × 1,024 pixel gray-scale picture. Many programs are available in the public domain for embedding messages in graphics.

Asymmetric (secret key) cryptography. The two basic types of cryptography are secret-key systems (also called symmetric or one-key systems) and public-key systems (also called asymmetric or two-key systems.) Both systems have their advantages and disadvantages. Secret-key cryptography is faster than public-key cryptography. Hybrid systems combine the two types of cryptography to exploit the strengths of each.

One of the older and probably the best-known secret-key system is the DES. The newer *Escrowed Encryption Standard (EES)*, published as FIPS Publications (FIPS PUB) 185, also makes use of a secret-key system. The *Data Encryption Standard (DES)*, published as FIPS PUB 46-2, is the standard secret-key system used by the U.S. Government for unclassified, but sensitive, information. Since the late 1970s, DES has also become one of the most widely used systems in international business and financial applications, and it has been a very successful secret-key system. The IDEA is another well-known secret-key algorithm, which is becoming a de facto standard in Europe.³⁵

For secret-key cryptography, only one key is used in the nodes on both ends. The same key is used to encrypt plaintext and decrypt ciphertext. While secret-key cryptography is not as elegant as public-key methods, it should certainly do the required job for most systems—as it has for years. The power of symmetric-keyed cryptography is that for each added bit the key space is twice as large, so a brute force attack takes twice as long.

Data Encryption Standard (DES). FIPS PUB 46-2, *Data Encryption Standard (DES)*, is the best known and most widely used secret-key system. The security provided by DES cryptographic systems depends on the mathematical soundness of the algorithm, length of the keys, key management, mode of operation, and implementation. ANSI adopted DES as the basis for encryption, integrity, access control, and key management. The ANSI name for DES is the Data Encryption Algorithm (DEA). The national and international financial service communities use this name (DEA) widely.³⁶

³⁵ FIPS PUB 185 specifies use of a symmetric-key encryption (and decryption) algorithm (SKIPJACK) and a law-enforcement access field (LEAF) creation method (one part of a key escrow system) which provides for decryption of encrypted telecommunications when interception of the telecommunications is lawfully authorized.

FIPS PUB 46-2 specifies a FIPS-approved cryptographic algorithm as required by FIPS 140-1. This publication provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting the cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.

IDEA is the name of the new, universally applicable block encryption algorithm that permits the effective protection of transmitted and stored data against unauthorized access by third parties.

³⁶ DES, the most popular encryption algorithm, is well defined in a variety of standards, including ANSI X3.92, ANSI X3.106, FIPS 46, and FIPS 81. DES is a block cipher algorithm that can run in a variety of different modes.

MCTL DATA SHEET 17.1-2. ASYMMETRIC KEY TECHNOLOGY

Critical Technology Parameter(s)	(1) Have undergone extensive, open peer review and no attacks discovered that are expected to be practical within 20 years; (2) Have at least 3,072-bit key spaces for Diffie-Hellman and Rivest, Shamir, Adelman (RSA) systems and at least 256-bit key spaces for elliptic curve cryptographic (ECC) systems; and (3) Digital signatures must have a hash value of at least 256 bits.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Software specially designed to support randomness, multiple polynomial quadratic sieve (MPQS), double large prime variation of the MPQS, number field sieve (NFS) factoring and discrete log; e.g., index-calculus algorithms for use in asymmetric system development, testing, quality control, and evaluation. And software specially designed to support Pollard's parallel collision and Koblitz tests for the security of ECC systems.
Major Commercial Applications	The comparatively recent requirements for strong cryptographic applications established by the financial service industries, Internet, electronic commerce, and business network operators have been the principal open source drivers of cryptographic technologies in recent years. While commercial cryptographic applications may not yet equal the strength of government systems, the gap between the strength of government and civilian systems may be closing, in large part because of the open peer review system and the significant R&D investments that the information systems industry is making in commercial systems worldwide.
Affordability Issues	<p>Affordability should not be the principal product acquisition issue for this technology. Competitive, information-system-security COTS products are appearing in the open market with strong asymmetric cryptographic functionality, at little or no apparent additional cost. However, the cost of additional staff to manage and maintain the cryptographic functionality for large complex systems could be a significant affordability issue. Most of this functionality can be automated.</p> <p>But after automation, there is still a potentially expensive requirement to (1) Recruit and retain technically qualified personnel worthy of cryptographic system trust and responsibility and (2) Operate, manage, and support the required end-user training, standardization, and test and evaluation programs required for optimum protocol and system security. Also, the manpower requirements to operate a PKI, especially the Certification Authority (CA) and Registration Authority (RA) personnel requirements, will affect affordability. This, of course, depends on the CA's policy and the Certification Policy Statement (CPS). The Defense Messaging System (DMS) may provide an early indication of affordability from a personnel standpoint.</p>
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI, XIII.

BACKGROUND

Asymmetric (public-key) cryptography is implemented with a two-key cryptographic algorithm. An asymmetric public-key algorithm uses two related keys: a *public key* and a *private key*. The two keys have the property that, given the public key, it is currently considered *computationally infeasible* (italics added) to derive the private key.³⁷ Public-key cryptography uses pairs of keys: a public key that is widely available, and a corresponding

³⁷ ANSI X9.57 definition.

private key known only to the person, application, or service that owns the keys. These key pairs are related in such a way that what is encrypted with the private key can only be decrypted with the public key, and vice versa. Some asymmetric algorithms can also be used for *authentication* (digital signature) and to establish nonrepudiation. For authentication, the message is *signed* with the private key, and the signature is *verified* using the public key. Authentication can also be performed with a hash function, which hashes and compresses a plaintext message of arbitrary length into a fixed-size digest, or *hash value*. It is currently considered computationally infeasible to alter a plaintext message without altering the hash value.

Cryptology is defined by the Joint Chiefs of Staff as “the science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.”³⁸ Cryptology is the branch of mathematics encompassing cryptography and cryptanalysis, and its practitioners are cryptologists. Modern cryptologists are usually trained in advanced theoretical mathematics and computer programming.

Cryptology is commonly used as a collective term that refers to cryptography and cryptanalysis. However, David Kahn provides a broader definition: “Cryptology is the science that embraces cryptography and cryptanalysis, but the term ‘cryptology’ sometimes loosely designates the entire dual field of both rendering signals secure and extracting information from them.”³⁹

The word “*cryptography*” was derived from two ancient Greek words: *kryptos*, meaning hidden, and *graphia*, meaning writing. Cryptography, the art and science of keeping messages secure, is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext (i.e., seeing through the disguise).⁴⁰

A *cipher* is a secret method of writing, whereby plaintext (or cleartext) is transformed into ciphertext (sometimes called a cryptogram). The word cipher has Hindu and Arabic roots. The Hindu *sifr* was turned into *zephyrus*, originally meaning the new Arabic⁴¹ number zero, by Western scholars. Zero was so important to the new set of numbers that mathematicians started calling all Arabic numerals ciphers. In the 1300s, Italian merchants started using Arabic numerals and even used them to send encrypted messages, which is how *cipher* came to mean “secret code.”⁴²

The process of changing plaintext into ciphertext is called *encipherment* or encryption.⁴³ The reverse process of transforming ciphertext into plaintext is called *decipherment* or decryption. Both encipherment and decipherment are controlled by a cryptographic key or keys.⁴⁴

Cryptography is sometimes confused with *steganography*, the second basic way a message may be hidden and by far the older way. Whereas cryptography may not necessarily hide the presence of a secret message, steganography is intended to conceal the very existence of the message. Examples of steganography are the old methods of invisible inks and microdots. In the digital age, messages can be concealed in graphic images since most graphics standards specify more gradations of color than the human eye can notice. The steganography algorithm looks for the most complex parts of the image, where neighboring pixels are most different from one another, and

³⁸ Joint Publication (JP) 1–02, *Department of Defense Dictionary of Military and Associated Terms*, as amended through 9 January 2003: available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, p. 136.

³⁹ David Kahn, *The Codebreakers: The Story of Secret Writing*, Scribner, New York, 1996, p. xviii.

⁴⁰ Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., John Wiley & Sons, Inc., 1995, p. 1.

⁴¹ Number characters evolved from the symbols that Indians used; by rights they should be called Indian numerals rather than Arabic ones. See Figure 14, p. 68, Charles Seife, *Zero: The Biography of a Dangerous Idea*, Viking, New York, 2000.

⁴² *Ibid.*, pp. 73, 81.

⁴³ The International Standards Organization (ISO 7498–2) uses the terms “encipher” and “decipher” because the Romance languages have words derived from the Latin root word *crypta* that are associated more with the unpleasant ideas of death and burial than things hidden. The word “encryption” has been coined from the word “cryptography.”

⁴⁴ Dorothy Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, Reading, Mass., reprinted with corrections, January 1983, p. 1.

adds the data to the least significant bits of the pixels. Without changing the graphical image noticeably, a 64-kilobyte message can be incorporated in a 1,024 × 1,024 pixel gray-scale picture. Programs are available in the public domain for embedding messages in graphics.

Cryptography is a combination of two basic components: an *algorithm*⁴⁵ (or cryptographic methodology) and a *key*⁴⁶ (or key pair, in the case of asymmetric systems). Algorithms are complex mathematical formulae, and, in the digital age, keys are strings of bits. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption and decryption. Two related algorithms are generally required: one for encryption and the other for decryption. Keys may be any of a large number of values. The range of possible values of the key is called the *keyspace*.

There are two basic types of cryptographic systems: *secret key* (also technically called symmetric systems) and *public key* (also technically called asymmetric systems). *Hybrid* (or mixed) systems, which use both types, hash functions, and reversible and irreversible algorithms are also widely used forms of cryptography. Most commercial cryptographic solutions are hybrid systems that are a combination of *symmetric*, or secret-key, and *asymmetric*, or public-key, technologies because hybrid systems simplify key management.

Public-key cryptographic systems use a pair of keys for each party. One of the keys of the key pair is “public,” and the other is “private.” The private key is not revealed. The public key can be known to the world. The public key of a pair of keys used for encryption and decryption requires the private key of the same pair. For a public-key system to be secure, the private key must be kept confidential, known only to its owner. The public key must also be known to belong to the addressee.

A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key, which corresponds to but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user’s public key. Signature generation can be performed by the possessor of the user’s private key.⁴⁷

In determining equivalent asymmetric key lengths that match the 128-bit symmetric key threshold specified for this update cycle, the measure used was *TIME*, a conservative choice. *TIME*, a computer complexity theory concept, is the (estimated) number of computer operations required to solve one instance of the general problem. The equivalence of symmetric keys to asymmetric key sizes was derived by comparing *TIME* to solve the problem using the *known best* methods. The *TIME* to solve a problem is an *estimate* because the solution is impossible and is therefore based on extrapolation of similar solved problems. If the solution cannot be found today, the algorithm is believed to be secure. All this is with *known best* methods of attack. It can be expected that better factoring methods for large composites will be devised and the storage requirements for current methods reduced.

If one believes that the best attacks on a “good” symmetric key algorithm is going to be key exhaustion, Moore’s Law can be used to project the life expectancy of the key. But with asymmetric key algorithms, one has to allow for Moore’s law as well as expect improvements in the algorithms for factoring.

It is relatively easy to equate symmetric key sizes to hashes. The hash size should be double the symmetric key size because there is a birthday paradox collision potential. The work factor for a birthday attack on a hash is the

⁴⁵ The word algorithm (a variant of *algorism*). According to legend, it was derived from Abu Ja’far Mohammed ibn Musa al-Khwarizmi’s name. Khwarizmi was an Arabian mathematician of the court of Mamun in Baghdad, c. 825. His semantic legacy also includes the word *algebra*.

⁴⁶ For example, a DES key consists of 64 binary digits (“0”s or “1”s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd (i.e., there is an odd number of “1”s in each 8-bit byte).

⁴⁷ FIPS PUB 186–2, 27 January 2000, p. 1.

square root of the hash size, so a 256-bit hash corresponds to a 128-bit symmetric key. SHA-2,⁴⁸ has AES-appropriate hash sizes of 256, 384, and 512 bits for 128, 192, and 256-bit AES keys, respectively. These larger key sizes might be appropriate today for high security applications, which produce data that must have a long (70 years or more) life.

One rationale for the existence of larger AES key sizes beyond 128 bits is the possibility of quantum computers becoming a reality. Currently at 5 or so qu-bits, a large quantum computer could threaten the security of existing key sizes with a square-root attack. That is, attacking a 128-bit key would take a 128-bit quantum computer about 2^{64} operations, which is much less than the 2^{128} operations on a von Neumann machine. Hence, the AES has 256-bit keys. Using the TIME metric, AES 256-bit key is about equivalent in security to an ECC key of 512 bits and RSA⁴⁹/digital signature algorithm (DSA) key at 15,360 bits.⁵⁰

⁴⁸ SHA-2 is an informal name, which is consistent with the NIST naming conventions, pending a formal name to be assigned by NIST when the standard is promulgated.

⁴⁹ The combined first letters of the last names of the collaborating creators of the RSA public-key system (R.L. Rivest, A. Shamir, and L.M. Adleman).

⁵⁰ For reputable analyses supporting these conjectures, see <http://www.certicom.com>, RSA Laboratories Bulletin No. 13, April 2000, at <http://www.rsalabs.com/bulletins> and <http://cryptosavvy.com>

MCTL DATA SHEET 17.1-3. CRYPTANALYTIC TECHNOLOGY

Critical Technology Parameter(s)	Technologies and techniques that enable the recovery of plaintext from adversarial ciphertext in time to provide (1) months to days of strategic warning and (2) hours to minutes of tactical warning.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Computers with a CTP of 200,000 Mtops or greater and operating systems and applications designed to test the ability of cryptanalytic systems to perform key searches; statistical, linear, and differential cryptanalyses; and factor 110-decimal digit, or larger, numbers.
Unique Software	Operating systems for computers with a CTP of 200,000 or greater and software applications specially designed to perform randomness, correlation, weak key, and symmetry-under-complementation tests to facilitate analyses of ciphertext protected by symmetric ciphers. Software specially designed to perform randomness, MPQS, double-large-prime variation of the MPQS, NFS factoring for large composites (110-decimal digit or larger), and solving large matrices mod 2^{51} and discrete log (e.g., index-calculus) analyses to facilitate the analyses of ciphertext protected by asymmetric ciphers. And software specially designed to support a square-root attack, based on the Pollard rho algorithm, and Koblitz attacks on ECC systems.
Major Commercial Applications	The primary commercial applications of cryptanalytic technologies and techniques are for (1) continuing peer review of existing cryptographic systems; (2) testing to evaluate the strength of new encryption algorithms during their development, testing, and evaluation phases; and (3) cryptanalyses.
Affordability Issues	Cryptanalytic technologies may be the least affordable of the technologies in the cryptology component. Cryptanalytic computers and software both tend to be very expensive. Perhaps more important, the cryptographers capable of performing cryptanalyses can be even more expensive, and there is a shortage of them. Expert cryptanalysts are rare and attract significant compensation for their services, and there is fierce competition among industry and with governments for reputable cryptanalysts in the labor market.
Export Control References	Cryptanalytic technologies and products are treated as cryptography for national and international export-control purposes and are covered by the cryptography regulations: WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI, XIII.

BACKGROUND

It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.
— Edgar Allan Poe

Cryptanalysis is defined by the Joint Chiefs of Staff as: “The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption.”⁵² In essence, *cryptanalysis* is the science and art of recovering the plaintext of an encrypted message without access to the key. In the digital age, the art of encryption is simply about devising ways to hide text behind walls of random binary

⁵¹ Mod is the abbreviation for *modulus*, which is the number of different numbers used in a system of modular arithmetic. The 2 indicates *binary*: relating to, being, or belonging to a system of numbers having 2 as its base [the digits 0 and 1]. *Mod 2* is the abbreviation for *Modulo 2 arithmetic*.

⁵² Joint Publication (JP) 1–02 *Department of Defense Dictionary of Military and Associated Terms*, as amended through 9 January 2003: available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, p. 135.

numbers. The so-called “black art of code-breaking” is all about using mathematics to find patterns in that binary number randomness—to discover order in a universe that is intended to present none.

Cryptanalysis could not be invented until a civilization had reached a sufficiently sophisticated level of scholarship in several disciplines, including mathematics, statistics, and linguistics. Between A.D. 800 and 1200, Arab scholars enjoyed a vigorous period of intellectual achievement. It was the Arab scholars who invented cryptanalysis. They succeeded in finding a method for breaking the monoalphabetic substitution cipher, a cipher that had remained invulnerable for several centuries.⁵³

No documentary evidence has been found that identifies the person who first realized that the variation in the frequencies of letters could be exploited to break ciphers. Frequency analysis was the first tool of cryptanalysis and is still a primary cryptanalytic technique. The earliest known description of the technique is by a 9th-century scientist, al-Kindi.⁵⁴ His greatest treatise, which was rediscovered only in 1987, is in the Sulaimaniyyah Ottoman Archive in Istanbul, and is entitled *A Manuscript on Deciphering Cryptographic Messages*. In this treatise he explains the *frequency analysis* method of cryptanalysis in two short paragraphs:

One way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. We call the most frequently occurring letter the “first,” the next most occurring letter the “second,” the following most occurring letter the “third,” and so on, until we account for all the different letters in the plaintext sample.

Then we look at the ciphertext we want to solve and we also classify its symbols. We find the most occurring symbol and change it to the form of the “first” letter of the plaintext sample, the next most common symbol is changed to the form of the “second” letter, and the following most common symbol is changed to the form of the “third” letter, and so on, until we account for all symbols on the cryptogram we want to solve.⁵⁵

Of course, it is not possible to apply al-Kindi’s frequency analysis unconditionally because standard frequencies are only an average and will not correspond exactly to the frequency in every text. Also, short texts are likely to deviate significantly from the standard frequencies. Cryptanalysis of a monoalphabetic substitution cipher still demands a good deal of guile, intuition, flexibility, guesswork, and luck, in addition to frequency analysis.

A few centuries later, the center of cryptanalytic interest shifted to Europe. Arguably the first great European cryptanalyst was Giovanni Soro, appointed as Venetian cipher secretary in 1506. Soro’s reputation was known throughout Italy, and friendly states would send intercepted messages to Venice for cryptanalysis. Even the Vatican, probably the second most active center of cryptanalysis in Europe at that time, would send Soro seemingly impenetrable messages that had fallen into its hands.⁵⁶ Francois Viete consolidated the French code-breaking prowess, taking particular pleasure cracking Spanish ciphers.

This was a transition period in Europe when cryptographers were still relying on the monoalphabetic substitution cipher and cryptanalysts were beginning to use frequency analysis to break it. One of the simplest improvements to the security of the monoalphabetic substitution cipher was the introduction of *nulls*, symbols or letters that were not substitutes for actual letters, merely blanks that represented nothing. The nulls would confuse an attack by frequency analysis. An equally simple development was deliberately misspelled words, making it harder for the cryptanalyst to apply frequency analysis.

The history of cryptanalysis and its impact on the affairs of men is so inordinately rich it fills many volumes. Here, however, we include the effect of cryptanalysis on Mary Queen of Scots as the only digression to show how cryptanalysis has affected history. While she was in prison, an encryption scheme was developed to protect her correspondence with her supporters in London. One of Mary’s conspirators, Anthony Babington, used a cipher that

⁵³ The *monoalphabetic substitution cipher* is the general name given to any substitution cipher in which the cipher alphabet consists of either letters or symbols, or a mix of both.

⁵⁴ Abu Yusuf Ya’qub ibn Is-haq ibn as-Sabbah ibn ‘omran ibn Ismail al-Kindi, known as “the philosopher of the Arabs.”

⁵⁵ Simon Singh, *The Code Book*, Doubleday, New York, 1999, p. 17.

⁵⁶ *Ibid.*, p. 28.

was not a simple substitution cipher, but rather a *nomenclator* to protect her correspondence. Babington's nomenclator consisted of 23 symbols that were substituted for the letters of the alphabet (excluding j, v, and w), along with 36 symbols representing words or phrases. Gilbert Gifford, a double agent, who was the courier for Queen Mary's enciphered letter to her supporters in London, delivered them after Thomas Phelippes had made copies.

Phelippes had been appointed to the London cipher school, which was established by Sir Francis Walsingham, Queen Elizabeth's Principal Secretary. Phelippes was a linguist and one of Europe's finest cryptanalysts. As Walsingham's Cipher Secretary, he deciphered Gifford's nomenclator and altered Mary Queen of Scots' encoded message to produce the evidence for her execution. On 8 February 1587, she was executed under the 1584 *Act of Association*, specifically designed to convict anyone involved in a conspiracy against Elizabeth, clearly demonstrating that weak encryption can be worse than no encryption at all.

Sometime in the 1460s, 15th-century Florentine polymath Leon Battista Alberti hit upon the most significant breakthrough in encryption in a thousand years. At the time, all substitution ciphers required a single cipher alphabet for encrypting each message. Alberti proposed using two or more cipher alphabets, switching between them during encipherment to confuse cryptanalysts.

A hundred years later, Blaise de Vigenere became acquainted with the writings of Alberti. Vigenere's interest in cryptography arose during his French diplomatic work while assigned to Rome. Building on the original concept of Alberti, Vigenere developed the cipher that bears his name.

The Vigenere cipher was the first of a class of ciphers known as *polyalphabetic*, so-called because it employs several cipher alphabets per message. The strength of the Vigenere cipher lies in its using not one, but 26 distinct cipher alphabets to encrypt a message. The first step in encipherment is to draw up a so-called Vigenere square composed of plaintext alphabet followed by 26 cipher alphabets, each shifted by one letter with respect to the previous alphabet. A different row in the Vigenere square (a different cipher alphabet) is used to encrypt different letters of the message. The great advantage of the Vigenere cipher is that it is impregnable to frequency analysis and has an enormous number of keys. If Mary's secretary had known about the Vigenere cipher, Mary's messages to Babbington would have baffled Phelippes and her life might have been spared.

The monoalphabetic substitution was quick, easy to use, and secure against those unschooled in cryptanalysis. The polyalphabetic cipher was complex to implement. So, cryptographers searched for an intermediate cipher that was harder to crack than a straightforward monoalphabetic cipher, but simpler to implement than a polyalphabetic cipher. Among the candidates was the remarkably effective homophonic substitution cipher. In the homophonic substitution each letter is replaced with a variety of substitutes, the number of potential substitutes being proportional to the frequency of the letter. Unfortunately, relationships between letters and other language patterns can still be discerned. Although the homophonic cipher is breakable, it is much more secure than a straightforward monoalphabetic cipher.

By the 1700s, European powers each had their own so-called "black chambers" in which teams of government cryptanalysts were working together to crack many of the most complex monoalphabetic ciphers. The black chambers effectively made all forms of monoalphabetic cipher insecure. Faced with professional cryptanalytic opposition, and after the development of the telegraph, cryptographers were forced to adopt the more complex, but more secure, polyalphabetic ciphers.

The Morse code is only an alternative public alphabet, and anyone sending a message had to give it to the telegrapher, who would read it in the process of transmitting it. The solution was to encipher the message before handing it to the telegrapher. The polyalphabetic Vigenere cipher was considered unbreakable and clearly the cipher of choice. For the time being at least, cryptographers had a clear lead over the cryptanalysts.

The greatest breakthrough in cryptanalysis since the Arab scholars of the ninth century broke the monoalphabetic cipher by inventing frequency analysis occurred when the Vigenere cipher was broken, probably in 1854, by Charles Babbage,⁵⁷ whose work was not published. The discovery only came to light in the 20th century when scholars examined Babbage's extensive notes. Babbage's technique was also independently discovered by Friedrich

⁵⁷ The same Babbage who was the inventor of the "Difference Engine" and is generally credited with the invention of the computer.

Wilhelm Kasiski, a retired officer in the Prussian army, who published his cryptanalytic breakthrough in 1863. The technique developed to discover the Vigenere keyword used to decipher the text is known as the Kasiski test. The technique consists of identifying sequences that repeat themselves and the spacing between the repetitions to identify the factors of the spacing, that is, the numbers that will divide into the spacing. From the repetitions and spacing in the ciphertext the possible length of the key (or factors) can be inferred. It is then possible to split the ciphertext into the number of parts corresponding to the length of the keyword, each one enciphered according to a monoalphabetic substitution as defined by each successive letter of the key word.

The whole world of cryptanalysis changed when Claude Elwood Shannon, a 32-year-old researcher at Bell Laboratories, showed how the once-vague notion of information could be defined and quantified with absolute precision. He showed that every mode of communications could be encoded in the universal language of binary digits, or *bits*—a term that his article was first to use in print when he published his theory in 1948—and from which the entire science of information theory grew. Shannon’s discovery, in turn, made possible the use of von Newman’s deterministic computers for both cryptography and cryptanalysis.

Decoding computer-generated messages is becoming increasingly more difficult. In time, multiple encryption techniques (i.e., Triple-DES and the use of public-key encryption for transmitting a new session key for each message) will overwhelm the best special-purpose cryptanalytic computers.

Almost all cryptography is theoretically breakable. Future breakthroughs in mathematics and the ever-increasing processing power of computers may give the cryptanalysts temporary advantages. However, better encryption algorithms may be discovered, keys can be lengthened, and multiple encryption—although time consuming—may be used with different algorithms and key lengths for each successive layer of encryption.⁵⁸ Some writers believe that future cryptanalytic attacks will take so much time and cost so much that cryptanalyses may have little practical utility—even with more powerful processors and better cryptanalytic techniques. “Cheap encryption, coupled with signal-hiding techniques (i.e., spread-spectrum and frequency-hopping) could seal the code-breaker’s fate.”⁵⁹

An attempted cryptanalysis is called an attack. There are four general types of cryptanalytic attacks:

- Ciphertext-only;
- Known plaintext;
- Chosen plaintext; and
- Chosen ciphertext.

A cryptanalytic team chooses the type of attack based on the availability of plaintext and ciphertext, the best guess at the algorithm used for encryption, and other indicators of its origin and nature that may be obvious or available. The skill and ability of the cryptanalysts and the computer resources available for the attack determine the size of cryptanalytic operation and the length of time it takes—sometimes called the “*work factor*.”

⁵⁸ *Superencipherment* has been used at least since World War II when messages that had been enciphered once were again enciphered one or more times to provide increased security.

⁵⁹ Martin C. Libicki, *What is Information Warfare?*, Center for Advanced Concepts and Technology Institute for National Strategic Studies, National Defense University, August 1995, p. 32.

MCTL DATA SHEET 17.1-4. EMBEDDABLE PROGRAMMABLE CRYPTOGRAPHIC PROCESSOR TECHNOLOGY

Critical Technology Parameter(s)	Embeddable, programmable cryptographic CMOS VLSI processors that are militarily critical (1) have a built-in secure operating system; (2) provide multilevel security; (3) are capable of handling 1,024 or more channels simultaneously; (4) can encrypt and/or decrypt 8 or more different algorithms simultaneously; and (5) can be initially loaded with cryptographic algorithms and updated with software.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Software specially designed to perform tests of general-purpose and application-specific versions of cryptographic functionality and assess the results of these tests.
Unique Software	Operating systems and application software implementing cryptographic functionality must be specially designed and integrated so that the information systems match and maintain the assurance-level protection profile of the cryptosystem during the operational life cycles of the systems. The system engineering and integration, user system interface, algorithms, and key generators must have zero defects. The software programs for installing and uninstalling cryptographic algorithms, the secure operating system, and the input/output (I/O) interfaces built into the VLSI chip that maintains the security of the cryptographic modules, are unique. Unique software cryptographic module security-system engineering complies with the provisions of <i>Security of Cryptographic Modules</i> , FIPS Publication (PUB) 140-1 and the requirements of the NSA, and it is consistent with ANSI standards for symmetric-key cryptography.
Major Commercial Applications	This is a dual-use item suitable for use in commercial products such as satellite communications, computing, networking, and automotive products.
Affordability Issues	Affordability is not an issue. This easily customized product has a lower overall cost than a "custom" VLSI chip due to the economies of scale since it can be used in many military and civilian applications. In addition, the life of information system equipment can be extended because algorithm changes do not require equipment changes.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI, XIII.

BACKGROUND

The Embeddable Programmable Cryptographic Processor Technologies and Products item covers programmable cryptographic processor chips that can be embedded in information system hardware.

The Advanced INFOSEC Machine (AIM) is a VLSI programmable cryptographic processor that has successfully communicated simultaneously with two Type 1 U.S. Government link encryptors on independent channels. The flexibility and security that the AIM VLSI offers to the communications, networking, banking, government, and military sectors has not previously been available before in a single part.

Before the development of this product, different devices running different algorithms were needed to address the different levels of data being encrypted. The AIM chip is configured in a standard package so that it can be embedded in the actual information system product itself, rather than being contained in an add-on "black box" with its own power and space needs. The AIM VLSI consists of over 9 million transistors, but has active power management and can use as little as 35 milliwatts in a handheld radio application. A secure operating system is built into the AIM VLSI so even the most highly classified algorithms can be loaded with software alone. The AIM VLSI is capable of handling up to 1,024 channels simultaneously. It also can simultaneously encrypt or decrypt data using eight different algorithms. Both general-purpose and application-specific versions, which are smaller in size but contain the same secure operating system I/O interfaces and programmability as the original chip, are available. The

first derivative of AIM is the AIM-R, a reduced-size, reduced-power, reduced-cost version of AIM for the handheld radio market. Because the AIM VLSI is programmable, the chip itself, unlike other cryptographic products developed for the U.S. Government, is unclassified and can be exported. Foreign users have the option of programming it with their own cryptographic algorithms.

The *Sierra* cryptographic solution combines the advantages of U.S. Government high-grade security with the cost efficiency of a reprogrammable, commercially produced encryption module. Sierra can be used to embed high-grade security into commercial and military encryption products. Available as a module or a chipset, Sierra can be easily embedded in two-way radios, modems, and network cards. Sierra provides a common security solution to users that have multiple encryption requirements. It can be programmed with a variety of encryption algorithms, including Type 1 for U.S. Government classified traffic, DES, and Triple-DES for financial and law-enforcement users, and other commercial algorithms for a wide variety of users. As a software upgradable module, Sierra provides a low-cost migration path for future communications upgrades without the logistics and cost burden associated with hardware changes. Sierra also allows the user to downgrade for applications that are no longer required after security upgrades. It is cost effective in commercial as well as government markets.

SECTION 17.2—DIGITAL STEGANOGRAPHIC TECHNOLOGY

Highlights

- Steganalytic tools can contribute to U.S. military full-spectrum dominance by providing additional information-security tools for the protection of military information.
- The worldwide proliferation of steganography has coincided with the explosive growth of the Internet. Academic and civilian sectors are now advancing the development, production, and use of civilian commercial steganographic products.
- A digital image can usually be coded to hide a significant amount of randomly embedded hidden information before the covert data becomes visible or statistically detectable.
- Information can be hidden in digital media: text, audio, imagery, and video files; transmission control protocol/ Internet protocol (TCP/IP) headers and user datagram protocol (UDP) packet headers; and hidden partitions and slack space on disks.
- Information can be randomly embedded in the quantization noise of image files and other data, without increasing the size of the host file.
- Electronic data steganographic and steganalytic techniques are in the public domain and are reasonably well understood.
- Comparatively inexpensive steganographic and steganalytic applications run on personal computers.

TERMS AND DEFINITIONS

Digitized data: any information that can be represented in a digital format (file). This includes audio, video, imagery, and document files as well as communication protocol packets.

Steganography: the practice of covert communication.

Steganalysis: the processes and techniques used to detect the presence of steganography.

OVERVIEW

Steganographic tools for creating concealed steganographic messages and performing steganalysis are covered in this subsection. Steganography is sometimes cited as one of the earliest documented forms of encryption, and seems to properly belong in the field of cryptology; however, cryptography per se is not covered in this subsection. The cryptography technology items are in the Cryptologic Technology subsection, 17.1.

Steganographic technologies are most closely related to the cryptography and cryptanalysis technology items in this subsection because they are concerned not only with methods of concealing the contents of a message, but also, through hiding the existence of the message rather than encrypting it, with steganography. They are also closely related to the *software* technology items, if only because the current steganographic tools are software applications.

Steganography is the art of hiding information in any one of the more obvious types of communication. Although not widely used, *digital steganography* involves the hiding of data inside a digital data file. *Steganalysis* is the process of detecting steganography by searching for variances between bit patterns and statistically testing files.

There are no national or international standards for steganography. It may be some time before the development of steganography standards begins. Although steganography has many practical uses, it still remains largely a computer artifact with comparatively few practical applications that have been widely adopted and in regular use.

Many first-generation commercial products are already in the world market. A representative list of steganography and steganalytic products is included in the steganography technology item data sheet.

BACKGROUND

“Steganography is the practice of *hiding* a message in such a manner that its *very existence is concealed*” (italics added). The DoD *Dictionary of Military and Associated Terms* does not define steganography per se, but seems to imply that steganography is considered a cryptologic science. The DoD definition of *cryptology* is: “The science which deals with *hidden, disguised* [italics added], or encrypted communications. It includes communications security and communications intelligence.” Differentiating between cryptography and steganography: “Cryptography is the practice of scrambling a message so it cannot be understood. Steganography is the practice of concealing or camouflaging a message so it cannot be detected.” An encrypted message may raise suspicion while a steganographic message may not even be detected. These three related definitions include the ideas of concealing the very existence of a message and hidden and disguised communications. Drawing on these ideas, for the purpose of the steganographic technology items, *digital steganography* is defined as the science and art of hiding or disguising digital information such that the *very existence* of the covert data is *hidden* or *disguised* in any digital vehicle, which in addition may be encrypted.

It will help to understand the contents of this subsection as well as the individual steganography and steganalysis technology items if the following concepts and definitions are kept in mind:

- Cryptography is sometimes confused with *steganography*, another basic way a message may be hidden and by far the older way.
- Whereas cryptography is the practice of scrambling a message so it cannot be understood, *steganography* is the practice of hiding, concealing, or camouflaging information within a more obvious kind of communication so it cannot be detected.
- “**Steganography** is the practice of hiding a message in such a manner that its very existence is concealed.”
- *Steganalysis* is the steps and operations performed in discovering hidden or disguised information in digital media by looking at any files and variances between bit patterns and converting the information into the original form without prior knowledge of its existence, the method used, or key employed in embedding the information.
- Successful *steganalysis* will discover hidden or disguised covert information, which may have been encrypted before embedding, in various types of digitized data.

The steganography community is continually researching and implementing new algorithms. There seem to have been no recent discoveries or breakthroughs. There are, of course, the continual development and improvements in commercial applications, with frequent revisions offered to the public by the steganography software publishers. There have been no expensive advertising campaigns in the trade journals and magazines typical of large, successful information-technology software products.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.2. DIGITAL STEGANOGRAPHIC TECHNOLOGY

17.2-1	Digital Steganographic Technology.....	MCTL-17-39
17.2-2	Digital Steganalytic Technology.....	MCTL-17-41

MCTL DATA SHEET 17.2-1. DIGITAL STEGANOGRAPHIC TECHNOLOGY

Critical Technology Parameter(s)	The militarily critical parameters for steganography are the specifications at which the covert data is below the detectable threshold for each type of digital data. These statistical and human-eye threshold specifications are different for each technique and form of digital media: text, audio, image, and video files; TCP/IP and UDP packet headers; hidden disk partitions; and, slack space on disks.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Computers of 45,000 CTP or greater and software specially designed to perform statistical tests to determine the detectability of disguised or hidden data during development, test, and evaluation of steganographic systems.
Unique Software	The operating systems and application software that feature steganographic functionality for military information systems must be specially designed and integrated so that the design assurance levels of the steganographic system implementations match and maintain the required common criteria EALs for the systems during their life cycles. The steganographic software security system engineering and integration, user system interface, algorithms, and embedding generators must have zero defects and comply with the applicable provisions of Security Requirements for Cryptographic Modules standard.
Major Commercial Applications	Personal and commercial steganographic applications are widely available for watermarking and embedding covert data in digitized data for authentication and for copyright and patent protection. Research prototypes and proof-of-concept applications are the drivers for this technology.
Affordability Issues	Affordability should not be the principal acquisition issue for steganographic products. Competitive new COTS steganography products that meet the militarily critical criteria are continuing to appear in the open market. If COTS products can meet a military requirement, the adoption of COTS products is less expensive and could eliminate some of the need for inventory, depot storage, and related life-cycle costs. However, the cost of additional staff to manage and maintain the steganographic functionality for large, complex systems could be a significant affordability issue. Most of the functionality can be automated; however, there are still potentially expensive requirements to recruit and retain technically qualified personnel worthy of the trust and responsibility to operate, manage, and support the end-user training, standardization, test, and evaluation programs required for optimum system security.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

BACKGROUND

“Steganography is the practice of *hiding* a message in such a manner that its *very existence is concealed* [italics added].” The DoD *Dictionary of Military and Associated Terms* does not define steganography per se, but seems to imply that steganography is considered a cryptologic science. The DoD definition of *cryptology* is “The science which deals with *hidden, disguised* [italics added], or encrypted communications. It includes communications security and communications intelligence.” Differentiating between cryptography and steganography: “Cryptography is the practice of scrambling a message so it cannot be understood. Steganography is the practice of concealing or camouflaging a message so it cannot be detected.” An encrypted message may raise suspicion while a steganographic message may not even be detected. These three related definitions include the ideas of concealing the very existence of a message and hidden and disguised communications. Drawing on these ideas, for the purpose of this technology item, *digital steganography* is defined as the science and art of hiding or disguising digital information such that the *very existence* of the covert data is *hidden* or *disguised* in any digital vehicle, which in addition may be encrypted. Steganography could be used to hide or disguise sensitive information transmitted over

open unprotected communications lines. For additional security, the information can be encrypted before embedding in the digitized data.

Steganography is that branch of information privacy that attempts to obscure the existence of data through such devices as invisible inks, secret compartments and use of subliminal channels. Steganography, the science and art of concealing “the fact of” a message, is one of the oldest methods used for message security. It was the threat of enemy interception that originally motivated the development of techniques for disguising a message so that only the intended recipient could read it. As early as the 5th century B.C., the Spartans used a *skytale*, the first military cryptographic device (really a form of steganography) for disguising military messages. A somewhat similar device was also in use in China more than 5,000 years ago. Chinese generals sent messages from the battlefield by wrapping a band of silk around a thin pole and then writing on the material. Only someone who had a pole with the same diameter could read the message. To others, the message would look like a band of silk with a random pattern of markings. This is one of the earliest documented forms of encryption. In the days of the Roman Empire, secret information was tattooed on a messenger’s shaved head. When the hair grew back, the messenger was sent out with the secret message on his scalp, often with an obvious decoy message in hand in case he was caught. Later examples of steganography are the use of invisible inks and microdots to conceal messages. Steganography has its place in security systems. It is not intended to replace cryptography but to supplement it. Hiding a message with steganographic methods reduces the chance of the message being detected; however, if that covert message is also encrypted, it requires cryptanalysis to recover the plaintext.

MCTL DATA SHEET 17.2-2. DIGITAL STEGANALYTIC TECHNOLOGY

Critical Technology Parameter(s)	(1) The statistical threshold specifications; and (2) the human sensor detection threshold specifications, at which hidden or disguised covert information is reliably discovered. These parameters are currently indeterminate, but believed to be different for each technique and form of media.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Computers of 45,000 CTP, or greater, and software specially designed to perform nominal statistical tests to determine the capability of steganalysis software to detect disguised or hidden data during the development, test, and evaluation of steganalytic systems. Processor requirements vary depending on the media being analyzed and response times that are acceptable.
Unique Software	The operating systems and application software that feature steganalytic functionality for military information systems must be specially designed and integrated so that the steganalytic system implementations are capable of detecting hidden or disguised information that is below the normally detectable threshold for each type of digital data and converting it into its original form.
Major Commercial Applications	Emerging first-generation personal and commercial stenographic applications are widely available for watermarking and embedding covert data in images, video, audio, or text files for authentication, and copyright and patent protection.
Affordability Issues	Affordability should not be the principal acquisition issue for steganographic products. Competitive new COTS steganalytic products for the detection and distortion of embedded messages are continuing to appear in the open market. If COTS products can meet military requirements, which is yet to be determined, the adoption of COTS products would be less expensive and could eliminate some of the need for inventory, depots, storage, and related life-cycle costs. However, the cost of analysts and additional staff to manage and maintain the steganographic functionality for large complex systems could be a significant affordability issue. Most of the functionality can be automated; however, there are still potentially expensive requirements to recruit and retain technically qualified analysts and other personnel, all of whom must be worthy of the trust and responsibility, to operate, manage, and support the required end-user training, standardization, test, and evaluation programs required for optimum system security.
Export Control References	Steganalysis is not specifically covered by current national or international export controls, if the application has no cryptography or cryptanalysis features. However, for export-control purposes, steganalysis is treated like cryptography by export-control officials and the following controls may apply pending a (case-by-case) commodity jurisdiction ruling: WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

BACKGROUND

For the purpose of this technology item, the science and art of *steganalysis* is defined as “the steps and operations performed in discovering hidden or disguised information in digital media and converting it into the original form without prior knowledge of its existence, the method used, or key employed in embedding the information.”

Steganography is that branch of information privacy technology that attempts to obscure the existence of data through such devices as invisible inks, secret compartments, and use of subliminal channels. Steganography, the science and art of concealing “the fact of” a message, is one of the oldest methods used for message security. It was the threat of enemy interception that originally motivated the development of techniques for disguising a message so

that only the intended recipient could read it. As early as the 5th century B.C., the Spartans used a *skytale*, the first military cryptographic device (really a form of steganography) for disguising military messages. A somewhat similar device was also in use in China more than 5,000 years ago. Chinese generals sent messages from the battlefield by wrapping a band of silk around a thin pole and then writing on the material. Only someone who had a pole with the same diameter could read the message. To others, the message would look like a band of silk with a random pattern of markings. This is one of the earliest documented forms of encryption. Later examples of forms of steganography used in the past are the use of invisible inks and microdots to conceal messages. Steganography could have an important place in security systems. Steganography and steganalysis would not replace cryptography and cryptanalysis, but they could supplement it. Hiding a message covertly with steganographic methods reduces the chance of the message being detected. However, if a covert message were found to be encrypted, cryptanalysis would be required to recover the plaintext. This might be computationally infeasible or in any case require an inordinate amount of time and effort.

To date, general detection techniques that apply to digital image steganography have not been devised, and methods beyond visual analysis are being explored. Too many images exist to be scanned manually for hidden messages. Some weaknesses of steganographic software that can point to the possible existence of hidden messages have been identified. Detection of these “signatures” can be automated into steganalytic tools for detecting the existence of steganographic messages. Tools for detecting hidden information are promising future work in steganalysis for watermark verification and computer forensics. Steganalysis remains a rapidly evolving field; recent breakthroughs have shown that it is far from being mature and well understood.

SECTION 17.3—IDENTITY-MANAGEMENT TECHNOLOGY

Highlights

- The almost daily need to gain access to sensitive facilities, information-processing equipment, and data requires the establishment of identity.
- The reason for using identity-management security technology is to provide enhanced security in accessing sensitive facilities, equipment, information, and data and to reduce fraud.
- Proper use of emerging secure biometric identity-management automatic (computer-assisted) identification-system technology with accurate enrollment can significantly improve identity management and reduce the national security and business risks associated with identity fraud.
- Smart card applications are increasingly used to replace passwords in logical access and circulation control systems and for digital signatures.
- On-board biometric identity-management smart-card processor and storage size limit the functions that can be performed by a secure biometric identity-management system and is a limiting factor in system performance.
- There are no suitable scales for the objective numeric measurement of biometrics and making objective comparisons.
- Biometric technology does not provide 100-percent accuracy, and in many cases it can be defeated or circumvented.
- Biometric identity system errors can and do occur. Probable false rejection rates (FRRs) and probable false-alarm rates (FARs) in biometric systems are never zero.
- Error rates and ease of use are usually the driving factors in the choice of a biometric system.
- The biggest security risk to secure biometric identity-management systems is in the enrollment process.

OVERVIEW

The heart of a secure biometric identity-management system is the biometric data, which are derived from a human being and must be processed by a secure biometric identity-management system to verify claimed identity (authentication) or discover the individual's true identity.⁶⁰ A biometric is a scale of suitable length and granularity for measuring and objectively specifying the parameters of a human physiological characteristic or personal behavioral trait that can be used to securely identify, or verify the claimed identity of, an enrollee⁶¹ accredited in a secure biometric identity-management system.

This section concentrates on selected militarily critical technologies required for the development, production, and use of secure identity-management systems: biometrics, smart cards, and system engineering and integration considerations. This subsection does not contain an exhaustive treatment of these technologies. A complete treatment of any of these technologies would fill many volumes.

⁶⁰ *Frequently Asked Questions, Definitions*, International Biometric Group, see http://bioprivacy.org/faq_main.htm and Michelle C. Frye, *The Body as a Password: Considerations, Uses and Concerns of Biometric Technologies*, A Thesis Submitted to the Faculty of the Graduate School of Arts and Sciences in Georgetown University, Washington, D.C. 27 April 2001.

⁶¹ *1999 Glossary of Biometric Terms*, Association for Biometrics (AfB) and International Computer Security Association (ICSA), see <http://www.afb.org.uk/>

The identity-management technologies are relevant to essentially all the technology items in the Information Security section in that the more sensitive aspects of these items require at least some protection during their development and in the production and use of information-security articles of intrinsic utility. The identity-management technologies are also relevant to all of the information-systems technology items that incorporate mandatory access controls. Finally, in a sense, identity-management technologies are related to all of the militarily critical technologies because there has always been a military information-security requirement for identity management since man first started using military force. The development, production, and use of military arms starts with an acquisition phase, the details of which should never be revealed to adversaries prematurely. In the operational phase, the often decisive element of surprise is lost if the adversary has had time to prepare for all the weapons in an arsenal and is not surprised. The positive identification of friendly forces with a right and need to know the secrets of militarily critical technologies is crucial.

Foreign cooperation, and even collaboration, is becoming increasingly important in the timely development of quality national and international standards. The open scientific method of peer review in the development of standards brings any technology to maturity more quickly, and the United States benefits from international comments and criticisms in the standards-development process. Perhaps the best opportunity for the United States to benefit from international cooperation is through participation in the development of biometric standards, many of which are still in the earliest stages.

BACKGROUND

Over the years, many parts of the anatomy, personal characteristics, and imaging methods have been suggested for biometrics. Some personal characteristics have been used successfully with various techniques and have legacies of many years. Some, such as facial recognition and fingerprints, are ancient. Facial recognition is as old as the human race. Personal recognition based primarily on the face was the basis for tribal security before written history. Records that have survived show that the ancient Egyptians made use of unique physical and sometimes behavioral characteristics for individual workers building the great pyramid of Khufu to verify their true identity and legitimate right to claim on a specific day their monthly allowance of 1.5 khars made up of mostly wheat with a proportion of barley.⁶² Babylonian kings used an imprint of the hand to prove the authenticity of certain engravings and works. There are indications that the Chinese used fingerprints centuries ago for chops. Personal characteristics such as gait and voice have also been used for centuries. The first scientific studies on fingerprints were initiated in the late 16th century. Fingerprints, which have been used extensively for about the last 100 years, are the oldest biometric used to establish identity.

Secure biometric identity-management system technologies are moving very rapidly, driven primarily by (1) the requirements of the electronic banking and commerce Internet interests for the reduction of financial fraud and (2) nation states' interest in the reduction of identity fraud. A third, and perhaps less demanding driver because of the usual funding difficulties, is the government and military sectors' requirements for a capability to control access to sensitive facilities, equipment, information, and data, but this may be changing since 9/11. In any case, the rate of change in identity-management technologies is far outpacing the development of the national and international standards required for interoperability.

A certain amount of trade jargon has grown up with the biometric field. The following provides a basic vocabulary, which should help in reading and understanding the identity-management technology item data sheets.

- *Identification* is associating an individual with his or her true identity among many others in a trusted database for validation of a claimed identity.⁶³ (Through a 1:n comparison process with n templates in the database.)
- *Three ways a person can be positively identified* are by (1) something you have (a credit card or driver's license), (2) *something you know* (a password or PIN), and (3) *something you are* (objectively established by a measured biometric sample).

⁶² Julian Ashbourn, *Biometrics: Advanced Identity Verification*, Springer, New York, 2nd printing, 2002, pp. 12–13.

⁶³ X9.84 and the BioAPI draw the distinction between two types of authentication: *verification* (1:1) is the validation of a claimed identity, whereas *identification* (1:n) is the discovery of n identity.

- *Enrollment*, which establishes the valid and authentic link between the biometric template specification and the individual, forms the logical basis for positive identification and authentication.
- *Authentication* (or *verification*) process is less complex than identification, since the biometric system is only asked to verify the authenticity of her/his (i.e., a single) claimed identity (through a 1:1 comparison of a biometric sample with an authentic template).
- *One-to-one authentication* (1:1) is accomplished by a comparison of the submitted sample biometric template with the valid and authentic enrolled template of the individual, which can be carried in encrypted form in a smart card by the owner.
- *Smart cards* are credit-card-sized cards that contain both a processor and memory.
- *Two-factor authentication systems* are based on (1) (something the user is) her/his measured biometric sample and (2) (something the user has) because the user must also have the smart card containing her/his enrolled template.
- *One-to-many identification* (1: n) is accomplished by the comparison with n other templates in a trusted database to positively identify the individual who submits a biometric sample.
- *Secure biometric identity-management systems* include all of the hardware, associated software, and interconnecting infrastructure required for end-to-end biometric processing. If the biometric process is an integral part of a larger system, then this definition extends to any part of the larger system that holds relevant user data, such as directories, transaction logs, and digital time-stamping where proof of timeliness may be required.
- *The end-to-end system engineering* of an integrated biometric process extends to the point that the authentication or identification function is completed and after which the biometric process is no longer required for the larger system to function.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.3. IDENTITY-MANAGEMENT TECHNOLOGY

17.3-1	Biometric Technology	MCTL-17-49
17.3-2	Smart-Card Technology	MCTL-17-54
17.3-3	Secure Identity-Management System Technology.....	MCTL-17-57

MCTL DATA SHEET 17.3-1. BIOMETRIC TECHNOLOGY

Critical Technology Parameter(s)	(1) Any two fingerprint scans in compliance with the FBI standard WSQ; ⁶⁴ (2) fingerprint readers that can provide “proof-of-life”; (3) iris pattern digital camera subsystems; (4) transmission (or signal processing) system segment in compliance with the BioAPI ⁶⁵ open-systems standard, the CBEFF, ⁶⁶ XCBF, ⁶⁷ and ANSI X9.84, ⁶⁸ including Normative References; ⁶⁹ (5) a biometric system and subsystem Common Criteria ⁷⁰ protection profile appropriate for the classification level of the facility, equipment, data, and information for which the secure biometric system controls access in accordance with <i>Department of Defense & Federal Biometric System Protection Profile for Medium Robustness Environments</i> ; ⁷¹ and (6) for those systems that incorporate databases, the protection profile shall be appropriate for information classified CONFIDENTIAL and will in no case be less than a certified ⁷² common criteria level of EAL 5 ⁷³ to provide prudent protection for the privacy of the enrollees.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Application software for COTS secure biometric identity-management systems is essentially unique, since it is proprietary at this time.
Unique Software	None identified.
Major Commercial Applications	Although there are limited U.S. Government and commercial markets so far, widespread commercial use, especially in Europe, of secure biometric identity-management system technologies and products by various financial service industries has been the driver. The current commercial base for secure identity-management systems is in regulated commercial industries such as transportation; banking and financial service; manufacturing and distribution; education; and health care. The major commercial market for biometric technology is for access to physical and virtual places, from secure doors to office computers, and for systems that must verify that people are who they claim to be. One prominent application for this technology may be a preferred traveler’s card, the so-called “happy traveler’s” card, which definitively establishes the qualified bearer’s identity for speeding enrolled travelers through airports.
Affordability Issues	Affordability of secure biometric identity-management system technologies and products should be an increasingly smaller issue over time because rapid adoption in the civilian market place has created a competitive environment with constantly improving products, which are becoming widely available at lower and lower prices. However, the personnel required to administer, operate, and maintain the key-management, enrollment, transmission, storage, verification, identification, and termination system segments could be a significant system cost factor.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

⁶⁴ Wavelet Scalar Quantization (WSQ).

⁶⁵ American National Standards Institute (ANSI), International Committee for Information Technology Standards (INCITS), ANSI INCITS 358-2002, *The BioAPI Specification*, Version 1.1, 22 March 2002.

⁶⁶ Common Biometric Exchange File Format, NISTIR 6529.

⁶⁷ XCBF is the XML Common Biometric Format. XML is a metalanguage, written in SGML, used for the interchange of documents on the WorldWide Web. SGML is a standardized markup language for describing the logical structure of a computer document.

⁶⁸ ANSI X9.84 *Biometric Information Management and Security*, 27 March 2001.

⁶⁹ *Ibid.*, p. 2.

⁷⁰ The *Common Criteria* is also ISO 15408.

⁷¹ Version 0.02, 3 March 2002.

⁷² Certified by a member of the National Voluntary Laboratory Accreditation Program (NVLAP), organized by NIST, which provides accredited laboratories that perform FIPS 140–1 compliance testing.

⁷³ Based on Version 2.1 of the “Common Criteria,” International Standard 15408. The Common Criteria can be found at <http://csrc.nist.gov/cc>. (EAL 5 compares to the TCSEC B2: Structured Protection.)

BACKGROUND

A biometric is a human physiological characteristic or personal behavioral trait that can be measured with a scale of suitable length and granularity to objectively specify the parameters required to identify, or verify, the claimed identity of an enrollee⁷⁴ accredited in a biometric identity-management system.

The six leading biometrics judged best suited to military applications were selected for coverage in this technology item. The six are shown in the columns of the Comparative Biometric Systems table (Table 17.3-1): (1) *Fingerprint Analysis*, (2) *Facial Features*, (3) *Hand Geometry*, (4) *Iris Recognition*, (5) *Speaker Recognition*, and (6) *Signature Recognition*. The technologies on which these six biometric systems are based are rapidly maturing and in wide commercial use, and they have a significant international market share. Biometric technologies are enablers for secure biometric identity systems, not the end products.

Many parts of the anatomy, personal characteristics, and imaging methods have been suggested. Some have been used successfully with techniques and technologies that have legacies of many years. An exhaustive biometric candidate list should include, among others: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits, odors, and head resonance. However, the selection of candidates suitable for military application becomes easier when evaluated in terms of the criteria developed by the National Biometric Test Center.⁷⁵ The National Biometric Test Center uses five criteria in the selection of biometrics suitable for identity management: (1) *Robustness*, (2) *distinctiveness*, (3) *accessibility*, (4) *acceptability*, and (5) *availability*. *Robust* means repeatable and not subject to large changes. A biometric is *distinctive* if wide differences exist in the pattern(s) among the population. *Accessible* means easily presented to an imaging sensor. *Acceptable* refers to the acceptability of the measurement technique to the users; usually those sensors perceived as nonintrusive are the most acceptable. *Availability* refers to the number of independent measures that can be presented by each user (i.e., 2 iris patterns or 10 fingerprints).

Seven biometric systems were excluded from consideration in this technology item since they are either still under scientific investigation or not in wide commercial use because of various factors that affect the identification accuracy, which are difficult to control. The excluded potential candidates are (1) keystroke dynamics, (2) vein pattern, (3) retinal pattern, (4) facial thermograms, (5) deoxyribonucleic acid (DNA), (6) gait, and (7) ear biometric techniques. These seven seem to be poorly suited to general use in military systems. Body odor, ear shape, and full-body thermal image biometric techniques were also considered, but cannot be recommended for military use because in most cases the technologies are still experimental; considered too intrusive; have large inherent error rates; or, like the biometrics used for a polygraph, are too complex and require elaborate data capture facilities and equipment and highly skilled, specially trained operators. Also, most of these excluded systems lack the required affordability or are not yet widely available in commercially viable products at this time.

Six biometrics—(1) fingerprint, (2) facial features, (3) hand geometry, (4) iris recognition, (5) speaker recognition, and (6) signature recognition—were selected because they have been in use for many years and enjoy the top six positions in biometric system commercial market share. An outline of the characteristics of these six selected biometrics and their international market share are shown in the first column of Table 17.3-1.

There are no suitable scales for the objective numeric measurement of biometric characteristics with which objective comparisons of biometrics can be made. Subjective evaluation ratings for each of the included biometric systems, on which there seems to be a consensus in the trade journals and technical literature, and their current use appear in Table 17.3-1. Note that only fingerprint systems and iris-recognition systems are considered *very strong*. *Very strong* means comparatively *low* error rates and *limited* consequences from probable damage or compromise of data. Most biometric systems can be used for facility- and equipment-access control. Speaker recognition and signature recognition are not generally considered suitable for one-to-many identification systems with large populations.

⁷⁴ 1998 *Glossary of Biometric Terms*, Association for Biometrics (AfB) and International Computer Security Association (ICSA), see <http://www.afb.org.uk/downloads/glossuk1.html>.

⁷⁵ *National Biometric Test Center Collected Works: 1997–2000*, edited by James L. Wayman, Director, National Biometric Test Center, San Jose State University, Version 1.3, August 2000, is highly recommend to all biometric system designers.

Table 17.3-1. Biometric System Comparative Description

BIOMETRIC SYSTEM				
Characteristics	Description	Strengths	Applications	2001 Market Share⁷⁶
Finger-print Systems	Fingerprint analysis is the comparison of an enrolled template of the fingerprint pattern on an individual's fingertips, which have been entered by an enrolled individual for authentication and identification functions. May have up to 40 variables. Highly distinctive but not very robust since the fingerprints can be easily damaged.	Very strong identification capabilities. Uniqueness of every fingerprint. No two alike have ever been found.	Facility and equipment access control in sensitive facilities and law-enforcement applications.	48.8%
Facial Features	Translates the characteristics of a face into a unique set of numbers for each individual. An eigenface algorithm maps the characteristics of a person's face into a multi-dimensional face space. This is the only biometric system that can be used passively. 3-D facial recognition differs in acuity, accuracy, speed, cost, and versatility from 2-D facial recognition.	Strong identification capabilities. Non-invasive. Can be used surreptitiously.	Facility and equipment access control, circulation control in sensitive facilities, passenger and terrorist recognition at airports, terrorist recognition at large sports events, casino surveillance.	16.4%
Hand Geometry	Hand geometry systems take a physical hand biometric input by measuring various shape features of the hand and analyzing them. Less distinctive than fingerprints but more robust.	Not as strong as fingerprint analysis systems. People's hands are more similar to others than their fingerprints.	Facility access and circulation control in sensitive facilities.	10.4%
Iris Recognition	Iris authentication and identification systems analyze the iris features that surround the pupil. Requires no contact, only user cooperation. May have up to 250 variables. Robust and quite distinctive.	Very strong identification capabilities. Can be more accurate than fingerprints. Uniqueness of every iris, which does not change with age.	Facility and equipment access control in sensitive facilities, customer verification at ATMs, and fraud reduction in the financial service industry.	6.2%
Speaker Recognition	The two components are an acoustic channel and a speaker recognizer. The speaker recognizer consists of the acoustic processor and a speaker decoder. Not intrusive, but not very robust.	Not suitable for identification usage.	Facility and equipment access control in sensitive facilities: still not secure enough to rely upon as a stand-alone biometric.	4.3%
Signature Recognition	Signature verification systems analyze a written signature or other signed symbols for comparison with the authentic signature G10 template of an enrolled individual. Not very distinctive or robust.	Not suitable for identification usage.	Authenticating financial service transactions and fraud reduction in the financial service industry and legal transactions.	2.7%

Fingerprint Systems. Fingerprint images are acquired from live-scan fingerprint readers. Live-scan readers scan the fingerprint directly from the subject's fingers. The scanned images are then processed to extract specific types of features from the images. Features from the scanned fingerprint image can be compared against a master

⁷⁶ *Biometric Market Report 2000-2005*, Biometric Group, September 2001, p. 3. See http://www.giometricgroup.com/e/biometric_market_report.htm

file containing features extracted from previous images. In AFIS, when the scanned fingerprint matches a master file image, a positive identification is reported. The FBI and NIST have established standards for fingerprint scanner image quality.⁷⁷ There may not be a perfect match, in which case an adjustable logic declares a match if the scanned fingerprint matches within the preset acceptable tolerance. The fingerprints of every individual are unique. No two have ever been found that were identical. Even identical twins have distinct fingerprints. Fingerprint systems are typically used for verification in military systems and are currently the most reliable and cost-effective biometric. Fingerprint systems are the oldest biometric and considered the most effective identification biometric by most writers; however, the emerging iris technology seems to be more accurate. The privacy risks associated with this biometric are rated “high” by the International Biometric Group. For certain types of deployments, proper protections must be in place to ensure that the technology is not misused.

Iris Recognition. Iris recognition is currently reported as the most accurate biometric identifier. Britain’s National Physical Laboratory published a study last year showing that iris-recognition technology decisively outperformed five other biometrics systems (facial recognition, fingerprint, hand geometry, vein, and voice recognition) on accuracy and throughput (or processing) speed of the matching algorithms. The evaluation measured each biometric technology’s ability to positively identify users. Iris recognition is now generally considered the most accurate, scalable, and cost-effective authentication solution. It is also a robust biometric. The privacy risks associated with this biometric are rated “high” by the International Biometric Group. For certain types of deployments, proper protections must be in place to ensure that the technology is not misused.

Facial Recognition. Sources used for the electronic capture of a subject’s facial image (“mugshot”) include still and video cameras and other types of video recorders that capture images and produce digital image files directly from the subject’s head and body. Scanners are used to digitize images from photographs, pictures, or sketches. The digital representations of these images consist of grayscale or color pixels, depending on the application and equipment. These digital images may be stored, in a compressed or uncompressed form, in an image storage and retrieval system. Textual descriptive data and other information is stored with each image. When required, specific images stored on a master file can be retrieved from the image storage and retrieval system and be incorporated as part of an electronic facial mugshot book or an electronic lineup. Facial recognition R&D made up more than 90 percent of federal surveillance budgets since 1997.⁷⁸ The privacy risks associated with this biometric are rated “High” by the International Biometric Group. For certain types of deployments, proper protections must be in place to ensure that the technology is not misused.

Hand Geometry. In commercial hand-geometry-based authentication systems, 3-D profiles of the hand are sensed. Finger lengths are relatively invariant and peculiar, although not unique, to each individual. The image-acquisition system, which requires cooperation of the subject, captures frontal and side-view images of the palm flatly placed on a panel with outstretched fingers. The representational requirements of the hand are comparatively small (9 B), which is an attractive feature for bandwidth- and memory-limited systems. Because the hand geometry is not unique, these systems cannot be scaled up to provide identification of an individual in a large population of identities. In spite of this limitation, hand geometry has become a very popular access-control biometric system for small domains, and it has captured almost half of the physical access-control market.

Finger Geometry. Finger geometry, a variant of hand geometry, is a relatively new technology that relies on the geometrical invariants of the index and middle fingers. It is claimed to be more accurate than hand geometry technology, although it is not as mature. The privacy risk associated with both the hand and the finger biometric have been rated “low” by the International Biometric Group. The basic functionality of these technologies ensures that there are few, if any, privacy issues.

Speaker Recognition. Voice capture is unobtrusive, and voiceprint is an acceptable biometric in almost all societies. Some applications entail authentication of identity over the telephone. The privacy risks associated with this biometric are rated “medium” by the International Biometric Group. The basic functionality of the technology ensures that there are few, if any, privacy issues.

⁷⁷ *Minimum Image Quality Requirements for Live Scan, Electronically Produced Fingerprint Cards*, FBI/NIST Appendix F/G, IAFIS-IC-0010(V2), April 1993.

⁷⁸ Brian DeBose, “Millions Spent to Develop Cameras,” *The Washington Times*, 17 April 2002.

Signature Recognition. Dynamic signature verification can be the least expensive of the six biometrics considered in this item, but keystroke and speaker verification can be even less expensive, depending on the implementation. The accuracy of this biometric is generally considered to be inferior to that of fingerprint scan and iris scan biometrics. The International Biometric Group rates privacy risks associated with signature biometrics “low.”

MCTL DATA SHEET 17.3-2. SMART CARD TECHNOLOGY

Critical Technology Parameter(s)	(1) A secure biometric multifunction smart card; ⁷⁹ (2) with an embedded 16-bit on-board processor; (3) embedded 128-kB on-card data storage; (4) on-board template and scan match processing algorithms; (5) an on-board crypto module ⁸⁰ supporting 128-bit AES symmetric key, ⁸¹ two 1,024-bit RSA ⁸² or DSA/DH asymmetric keys, ⁸³ or two 161-bit elliptic curve ECDSA/ECDH keys, and an ANSI-approved hash function or SHA-1 hash; ⁸⁴ and (6) tamper-proof smart cards that are ISO 7810- and 7816- or 14443-compliant and secure-card fabrication equipment.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Application software for COTS secure biometric identity-management systems is proprietary at this time. However, the operating systems are either commercial, widely used operating systems, such as IBM's S390/MVS, Mondex's Multos, Sun Microsystem's Java Card, and the Macintosh operating system, or open systems such as Compaq Open VMS and Linux, which are used to provide cross-platform multi-vendor database synchronization for most secure biometric identity-management systems.
Major Commercial Applications	The major commercial market for biometric technology is for access to physical and virtual places, from secure doors to office computers, and for systems that must verify that people are who they claim to be. Although there are limited U.S. Government and commercial smart card markets so far, widespread commercial use, especially in Europe, by various financial service industries has been the driver. The current commercial base for smart cards is in regulated commercial industries such as transportation, banking and financial service, manufacturing and distribution, education, and health care.
Affordability Issues	Smart cards are comparatively inexpensive components ⁸⁵ of information-security systems. The affordability issues result from the other system components.
Export Control References	There are no export controls on smart cards. If smart cards are loaded with cryptography, then they will fall under the normal cryptographic export controls: WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

⁷⁹ Identification Cards-Integrated Circuit (s) Cards with Contacts: Additional Interindustry Commands and Security Attributes, BS ISO/IEC 7816-4 thru -9 or 14443 compliant.

⁸⁰ FIPS PUB 140-1 *Security Requirements for Cryptographic Modules* and 140-2 (X9.66) *Cryptographic Module Validation Program* compliant.

⁸¹ ANSI X9.91, *Advanced Encryption Standard (AES)*.

⁸² ANSI X9.44, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Management of Symmetric Keys Using RSA and Advanced Encryption Standard (AES)*, FIPS PUB 197, 26 November 2001 compliant.

⁸³ ANSI X9.30-1997, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1, The Digital Signature Algorithm (DSA)*, American National Standards Institute, American Bankers Association; and ANSI X9.30-1997, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 2, The Secure Hash Algorithm (SHA)*, American National Standards Institute, American Bankers Association; X9.42-2000, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography* and ANSI X9.62-1999, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (EDCSA)* compliant.

⁸⁴ ANSI X9.31-1998, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, The RSA Signature Algorithm (RSA)*, American National Standards Institute, American Bankers Association and FIPS PUB 180-1 *Secure Hash Standard* and 186-2, *Digital Signature Standard*, 27 January 2000 compliant. Two asymmetric keys are required: one to provide signatures and the other for (symmetric) key establishment. SHA-1, a hash function, is not keyed.

⁸⁵ See Section 4.4.1, Part 1: Introduction and general model, of the *Common Criteria for Information Technology Security Evaluation* (Common Criteria Version 2.1), which is identical to *International Standard ISO/IEC 15408:1999*, p. 25. Throughout the Information Security section, the organization and construction of the common criteria were used. *Class* is used for the most general grouping, which is the Information Systems section group. *Family* is a grouping of sets within a class, in this case, the Information Security family. *Component* describes a specific set and is the smallest selectable set of *technology items*.

BACKGROUND

In most technical references, the term “chip card” covers (1) Smart cards, featuring embedded CMOS micro-controllers and memory chips; (2) memory or dumb cards, featuring embedded EEPROM (considered software) chips; and (3) both contact and contactless (or proximity cards.) Contact smart cards must conform to ISO 7816 and are easily identified by their standard metallic contact pads. Contactless smart cards, which must be in conformance with ISO 14443 (Type A, B, or C), do not have power cells but have embedded loop antennas, usually on the back. Contactless cards communicate with this embedded loop antenna by RF modulation and are energized by movement within the electromagnetic field produced by the card-reader antennas.

The use of chip-card technology is ideal for military applications because the wallet size of the chip-card is convenient and can serve many military functions. Chip cards are the most widely used and abundant of all the identity-management tools, and users can almost effortlessly carry them. In addition to being a fairly mature technology that has undergone a long period of extensive tests in actual use, these cards are also the least expensive and therefore most affordable solution for most military system applications. Any of many existing bar codes, magnetic-stripe, and proximity-card access features that may be required can be integrated within the same multifunction smart card. The card format is preferred for military service over tags and other tokens because it provides a convenient and versatile platform that can house an RF antenna and because chip cards are the highest volume semiconductor product manufactured worldwide.

American Express has recently started offering a type of dumb card called Blue. The Visa Web site carries a specification for their smart card. Discover and MasterCard also have smart-card programs, but all of these programs have very few terminals in position. The merchant must bear about two-thirds of the reader terminal costs, and few merchants can make a business case for their installation. A variety of dumb cards are in wide use in Europe, and they are increasingly used in the United States for pay phones or vending machines and in public transportation systems. In the pay phone cards, the memory stores a dollar value that is debited on use. The value can be restored in some systems.

The second type of card is often called the “true smart card.” In this card, a microprocessor (typically 8, 16, or 32Kbits) is embedded, as well as a magnetic memory of up to 128 kB. There are also optical memory cards that can store up to 4 MB of data. These are the types used in most secure biometric identity-management systems. True smart cards have the ability to make decisions about the data stored on the card and are not dependent on the unit to which they are submitted to make the applications work. The true smart card can also be a multifunction card.

There are two versions of the microprocessor-equipped true smart card—the contact version and a contactless version. As the name suggests, the contactless card system passes the data between the card and the reader without any physical contact. The advantage of the contactless system is that there are no contacts to wear out, but the card and reader are more sophisticated and therefore more expensive.

The contacts on contact cards will last through the limited lifetime of the credential in most systems. For optimum operational security and accuracy, a biometric card must be updated every 3 to 5 years anyway because the templates must be updated to maintain template fidelity; otherwise, the normal human physiological changes will reduce the accuracy and efficiency of the system.

GlobalPlatform provides an open-system architecture for fast and easy development of globally interoperable smart (microprocessor) card systems. The system architecture comprises three system segments—card, terminal, and systems—each of which may include specifications, software, or chip-card technology. The *GlobalPlatform* Web site⁸⁶ carries the following technical data and specifications for download:

- Card-Related Chip Technology, which includes the *GlobalPlatform Card Specification* v2.1, published June 2001;
- *Java Card Export file for GlobalPlatform Card Specification 2.1 API*, published March 2002;
- *Errata and Precisions List v 0.4*, published October 2002; and
- *Frequently Asked Questions Related to the 2.1 Card Specification*, published October 2002.

⁸⁶ <http://www.globalplatform.org/specifications2.asp>

The introduction of Java Card (a registered trademark of Sun Microsystems, Inc.) significantly reduces the time required to develop and deploy application software resident in microprocessor cards. Card-acceptance devices should be programmed and tested with the cards and other components of the application support infrastructure. Microprocessor card-based applications are most effectively implemented when the card and terminal application programs are developed in parallel from the same application specification. A reduction in the development and testing effort, similar to that offered by Java Card, is needed to create the associated software for card-acceptance devices.⁸⁷

Even though prices have fallen over the past few years, memory and microprocessor smart-card systems are still more expensive to create than the magnetic-stripe card and bar-code systems. Smart cards have the advantage over the magnetic stripe in the amount of data that can be stored and the processing features in true smart cards, although some bar-code fields can hold a surprising amount of data. The security, ease of use, and operational flexibility of a multifunction, secure biometric microprocessor card makes it the best system segment option for secure biometric identity-management in military systems. And of course, pictures and magnetic and bar-code stripes can all be located on the outside of a microprocessor card, making it a highly flexible multifunction card.

Optical-memory card technology is a technology similar to that used for music CDs and CD ROMs. A panel of the “gold colored” laser-sensitive material laminated in the card is used to store information. A laser burns a 2.25- μ m diameter hole in the material that can then be sensed by a low-power laser during the read cycle. The presence or absence of a hole represents a binary symbol, either a “1” or a “0.” Because the media is actually burned during the write cycle, this is a write-once, read-many (WORM) times media. The data are nonvolatile (not lost when power is removed), and these cards currently can store 4 to 6.6 MB of data. The State Department’s border-crossing ID card used by frequent travelers at entry points along the U.S. border with Mexico is a type of this card.

Another noncontact method for storing information is RFID. RFID has been available for several years, but is still only available in nonstandard proprietary forms from a variety of vendors. The biggest obstacle to standardization is the globally available frequencies. RFID systems provide information from an RF tag from a distance of a few millimeters to several meters. The tags vary in form and fit, from the tiny injectable glass transponders for tracing animals to brick-size containers attached to the side of trains. The frequencies vary from 125 kHz to 5.8 GHz.

The first smart cards were used in France in 1982. The first patent was filed in France in 1947. Smart-card technology and products were rapidly accepted in Europe because the high cost of telecommunications there made on-line verification of transactions very expensive. The smart card provided the mechanism to move that on-line verification off line, reducing transaction costs without sacrificing any of the security.

⁸⁷ Open Platform Terminal Specification v1.5, Management Summary, 30 October 1999, p. 1.

MCTL DATA SHEET 17.3-3. SECURE IDENTITY-MANAGEMENT SYSTEM TECHNOLOGY

Critical Technology Parameter(s)	<p>(1) A secure biometric multifunction microprocessor smart card with the capability to support fingerprint scans for WSQ coding of any two fingerprints, plus an iris scan for the Daugman algorithm to provide at least a 0.99 effectiveness in 1:1 identity verification: (a) an embedded 16-bit on-board processor; (b) embedded 128 kB on-card data storage; (c) on-board template and scan match processing algorithms; (d) an on-board crypto module supporting 128-bit AES symmetric key, two 1,024-bit RSA or DSA/DH asymmetric keys, or two 161-bit elliptic curve ECDSA/ECDH keys, and an ANSI-approved hash function or SHA-1 hash;</p> <p>(2) Fingerprint optical or chip reader subsystem that can provide “proof-of-life” and uses the FBI standard WSQ algorithm;</p> <p>(3) Iris pattern digital camera subsystems;</p> <p>(4) An enrollment application subsystem;</p> <p>(5) Tamper-proof smart cards that are ISO 7816 or 14443 compliant and secure-card fabrication equipment;</p> <p>(6) A fully implemented PKI that is X9.79 compliant; and</p> <p>(7) system compliance (with the BioAPI open-systems standard, the CBEFF, XCBF, and ANSI X9.84, including Normative References; and a system and subsystem Common Criteria Protection Profile appropriate for the classification level of the facility, equipment, data, and information for which the secure biometric system controls access, except for systems that include databases, in accordance with Department of Defense & Federal Biometric System Protection Profile for Medium Robustness Environments. For those systems that incorporate databases, the Protection Profile shall be appropriate for information classified CONFIDENTIAL and will in no case be less than a common-criteria-level of EAL 5 to provide prudent protection for the privacy of the enrollees.</p>
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Application software for COTS secure biometric identity-management systems is proprietary. However, the operating systems are either commercial, widely used operating systems, or open systems.
Major Commercial Applications	The major commercial market for secure identity-management system technology is for access to physical and virtual places, from secure doors to office computers, and for systems that must verify that people are who they claim to be. One prominent application for this technology may be the so-called “happy traveler’s” card, which definitively establishes the qualified bearer’s identity for speeding enrolled travelers through airports.
Affordability Issues	Secure biometric identity-management systems offer the potential for (1) increasing the operational security, privacy, efficiency, and convenience of identity-management systems while (2) decreasing operational losses and identity fraud. Affordability of secure biometric identity-management system technologies and products should be an increasingly smaller issue over time. However, the personnel required to administer, operate, and maintain the key-management, enrollment, transmission, storage, verification, identification, and termination system segments could be a significant system cost factor.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII. These controls are due to the biometric system segments as well as the cryptographic modules.

BACKGROUND

Secure Biometric Identity-Management System Description. Biometric data is derived from a human being and must be processed by a secure biometric identity-management system to verify claimed identity (*authentication*) or discover the individual's true *identity*.⁸⁸ A *biometric* is a scale of suitable length and granularity for measuring and objectively specifying the parameters of a human physiological characteristic or personal behavioral trait that can be used to securely *identify*, or *verify* the claimed identity of, an enrollee⁸⁹ accredited in a secure biometric identity-management system. The American Institute of Certified Public Accountant and the Canadian Institute of Chartered Accountants jointly developed the *SysTrust Principles and Criteria for Systems Reliability* standard that describes a system as being composed of infrastructure, software, people, procedures, and data, and it addresses the availability, security [system] integrity, and maintainability as the four principles.

Identity Terminology. The information-security community generally accepts three ways through which a person can be *positively identified*, that is, prove you are who you say you are, prove you are not who you say you are not, or prove you are not among a group of people already known to the system. The three ways a person can be positively identified are by (1) *something you have* (a credit card or driver's license); (2) *something you know* (a password or PIN); and (3) *something you are* (authenticated by biometric). Using relatively forge-proof unique identifiers of a human body, which can be objectively measured with biometrics, is a way of specifying *something you are* for *authentication* and *identification* purposes, and it has particular value for use as a countermeasure against information-system identity-fraud security exposures. *Something you are* can be determined by objectively measuring a human anatomical or physiological trait that is unique to an individual, such as fingerprints or iris patterns.⁹⁰ Of course, for very small, highly sensitive operations, personal recognition, with trusted third-party introductions, is still the best and most secure system for identification, access control, and circulation security.

The American National Standard X9.49-1999 *Secure Remote Access to Financial Services* classifies these authentication factors as something you have (possession factor), something you know (knowledge factor), and something you are (biometrics). The standard provides a risk-assessment methodology to determine an application's security requirements (confidentiality, integrity, authentication, and nonrepudiation) for online financial services (e.g., home banking) where remote access is required.

Requirement. The reason for using any kind of security technology is to provide enhanced security with respect to accessing sensitive facilities, equipment, information, and data and to reduce fraud. Merchants are looking for a better way to manage transactions, and consumers are looking for a faster, more secure way of shopping. Biopay has equipped 100 stores in 14 states with biometric smart-card systems, which have saved some large retailers as much as \$10,000 a month that was formerly lost through identity fraud. Industry marketing representatives claim that a properly designed and managed biometric deployment will provide a positive return on investment within a year. Biometric identity management provides a more robust audit trail. Once an individual is *positively identified* at the time of enrollment, that identity information can be relied on in future interactions. *Identification* is associating an individual with an identity. Biometric systems require sensors to convert the physical characteristic or behavior of a person into a signal that can be stored to provide a template for future comparisons. Only biometrics, automatically recognizing a person using distinguishing traits, can recognize you as you to establish identity. The six biometrics selected for coverage in this technology item are a family of fairly mature technologies that are being widely used for applications such as access-control systems in major airports and in other areas requiring restricted access.

Applications. Smart-card applications are increasingly used to replace passwords in logical access and circulation control systems and for digital signatures. Smart cards are now used in most wireless system applications

⁸⁸ *Frequently Asked Questions, Definitions*, International Biometric Group, see http://bioprivacy.org/faq_main.htm and Michelle C. Frye, *The Body as a Password: Considerations, Uses and Concerns of Biometric Technologies*, A Thesis Submitted to the Faculty of the Graduate School of Arts and Sciences in Georgetown University, Washington, D.C. 27 April 2001.

⁸⁹ *1999 Glossary of Biometric Terms*, Association for Biometrics (AfB) and International Computer Security Association (ICSA), see <http://www.afb.org.uk/>

⁹⁰ Valene Skerpac, "Got Biometrics?" *Information Security Bulletin 41*, April 2000, p. 41.

to protect billing codes and provide nominal privacy for the RF links. National identity programs are receiving increasingly favorable worldwide attention. Argentina, Finland, Spain, Malaysia, Mexico, Norway, and the UK have a national ID card, and others are considering some form of national or regional identity or drivers' credentials, including India and China. Austria uses secure biometric smart cards⁹¹ in its universal health-care program for the secure identity management of all Austrian citizens. Health care and banking industries are adopting smart cards. The key to biometrics is making them easy to use and inexpensive and integrating them into real-world applications. In the long run, biometric technologies are going to get cheaper and easier to install. Many believe that inevitably they will become more popular. Millions of organizations are already using some type of biometrics. Biometric identification systems are preferred over passwords when convenience or productivity issues are critical or when the cost of managing user IDs and passwords is prohibitive. Biometric technology is based on digital matching between a stored template and a submitted biometric sample.

Functions. *Enrollment* (or data collection) is the most critical single biometric system function. Enrollment establishes the valid and authentic link between the biometric specification and the individual, which forms the logical basis for positive *identification* and *verification*. Establishing a "true" identity at the time of enrollment must be done with documentation external to any biometric system. The purpose of a positive identification system is to prevent the use of a single identity by multiple people. For *verification*, the system captures a presented biometric to create a sample biometric template during enrollment and verifies that a user is who he or she *claims* to be by a "one-to-one" matching of the presented sample biometric with the trusted enrollment biometric template data either on a card or in a trusted database. *Identification* captures a user's presented biometric characteristic to create a sample template and *determines if the user is someone known* to the system by some form of comparison of "one-to-many" templates for matching with a trusted enrollment biometric template in the system's trusted database. If a positive identification attempt fails to find a match between an enrollment template and the submitted sample, a "rejection" results; a match between sample and template results in an "acceptance."

Security Risks. The 9/11 terrorist attacks were carried out with the deadly low-tech combination of suicidal fanaticism and box cutters. While technology can never replace vigilance and common sense, at least some of the operational flexibility enjoyed by the terrorists was based on fraudulently obtained drivers' licenses. At least seven hijackers obtained fake IDs from Virginia by lying about their residency status. The loopholes exploited by the hijackers are being closed, and Virginia drivers' licenses are being upgraded. Commenting on the proposed "smart" drivers' licenses to be proposed, a Northern Virginia congressman, Democrat James P. Moran, said, "You could make a strong case that the hijackings on September 11 would not have happened if we had had this system in place."⁹² Proper use of emerging secure biometric identity-management, computer-assisted identification system technologies with proper enrollment procedures can significantly improve identity management and reduce the national security and business risks associated with identity fraud. People managing and operating secure identity-management systems, so called "insiders," are always the weakest link in any security system. The security of secure identity-management systems depends on the absolute integrity of the enrollment process and cryptographic key management, and the conscientious, disciplined participation of the end-users in protecting the security of the system.

The biggest security risk to secure biometric identity-management systems is in the enrollment process. If an individual who has established a fraudulent identity is successful in posing as another individual or misrepresenting facts regarding his identity during a biometric enrollment process, it is unlikely that the enrollment process will discover the identity fraud. An individual with a fake passport, for example, may be able to use this passport as the basis for enrollment in a biometric system. The system can only verify that the individual is who he or she claimed to be, and was proved to be, to the satisfaction of the registration authority during enrollment. Only if the biometric system has a perfect universal domain (which exists only in the imagination), with an infinitely large trusted central database against which the template of a new enrollee can be compared to each user already enrolled for a match, can an individual be discovered attempting to enroll more than once. Otherwise, biometric systems alone cannot prevent an individual from assuming a false identity during enrollment. Background investigations and even polygraphs or DNA testing may be needed to discover true identities and reduce identity theft, but going to these lengths to establish identity is impractical for most large government and commercial applications. There are many

⁹¹ XBS21 Security Business Systems, AG provides the Austrian health care secure biometric identity-management systems.

⁹² "'Smart' Driver's Licenses to be Proposed," *The Washington Post*, 3 May 2002, p. B3.

security risks associated with biometric identity-management systems. Biometric systems cannot replace a requirement to enforce the classic rules for security and access control.

Secure Biometric Identity Management System Architecture. The system architecture for a militarily critical *Secure Biometric Identity Management System* will usually contain the following seven top-level functional system segments: (1) enrollment (or data collection); (2) transmission (or signal processing); (3) decision; (4) storage; (5) verification; (6) identification; and (7) termination. These are the building blocks for developing a secure integrated information system for processing *biometric data* and maintaining its integrity and security throughout the life cycle of the data. Matching is typically included as a separate system segment from the decision function by many authorities. These seven system segments are at the top-level block diagram order of detail. Of course, at the computer program configuration item level of granularity the matching syllogistic program would be specified in a separate item for a biometric system.

Six leading biometrics judged best suited to military applications were selected for coverage in this technology item. The six are shown in the columns of Table 17.3-1: (1) *Fingerprint Analysis*; (2) *Facial Features*; (3) *Hand Geometry*; (4) *Iris Recognition*; (5) *Speaker Recognition*; and (6) *Signature Recognition*. The technologies on which these six biometric systems are based are maturing rapidly, are already in wide commercial use, and have a significant international market share. Biometric technologies are enablers for secure biometric identity systems, not the end products.

A secure biometric identity-management system includes all of the hardware, associated software, and interconnecting infrastructure required for end-to-end biometric processing. If the biometric process is an integral part of a larger system, then this definition extends to any part of the larger system that holds relevant user data, such as directories, transaction logs, and digital time-stamping, where proof of timeliness may be required. In addition, in a system that is well engineered end-to-end, the integrated process extends to the point after which authentication or identification is complete and no longer required for the larger system to function.

System Strength. The inherent strength of a biometric identity-management system and its suitability for various military applications should be among the criteria used for selection. Assessing the strength or risk of error for a specific biometric process is very different undertaking compared with the relatively straightforward methods of assessing the risk of error in other specific technological processes. The potential vulnerabilities or points of attack within a biometric process, which can lead to a compromise of data integrity or the intended functionality of the chain of processes, introduce many undefinable variables. The exact quantification of such risks is so exceedingly difficult as to be virtually impossible. Efforts to establish robust independent testing methodologies are currently underway at the Biometric Working Group and the Center for Mathematics and Scientific Computing, National Physical Laboratory, in the UK.⁹³ Risk of occurrence levels and resulting error rates are classified here as *low*, *medium* or *high*, with related probable damage or compromise of data or functions as *limited*, *moderate*, or *disastrous* in consequences, respectively. Like any security system, neither the level of risk nor the potential consequences for secure biometric identity-management systems is ever zero.⁹⁴ “*No biometric identification system, however, works perfectly.*”⁹⁵

Response Time. Some system processing times are longer than others, but the present state-of-the-art system response times are comfortably under 30 seconds for most systems. System requirements can vary widely, depending on the nature of the application. Fingerprint systems used for identification by federal, state, and local law-enforcement agencies tend to require large databases. Binning techniques can be used to reduce processing time in large fingerprint (and facial recognition) systems. See Table 17.3-2.

⁹³ “Metrics—Technology Assessment Guide,” *Biometrics Market Intelligence*, February 2002, p. 8. An interesting table on this same page provides a starting point for a high-level evaluation in a first-pass assessment of various biometric technologies.

⁹⁴ Fitch, Canaris, Kapur, and Tvrđik, *Security and Data Integrity in Identity Management Systems*, SyntheSys Secure Technologies, Inc., Boca Raton, Fla., January 2002.

⁹⁵ James L. Wyman, Director, U.S. National Biometric Test Center, “Biometric Identification Technologies in Election Processes—Summary Report,” *National Biometric Test Center Collected Works, 1997–2000*, Version 1.3, San Jose State University, August 2000.

One-to-One Authentication. The two principal functions of biometric systems are *authentication* (or verification) and *identification*. Authentication is less complex than identification, since the biometric system is only asked to determine the authenticity of a single claimed identity. Authentication is accomplished by a one-to-one comparison of the submitted sample biometric template with the valid and authentic enrolled template of the individual, which can be carried in encrypted form in a smart card by the owner. In the better authentication system designs the biometric template is encrypted and never leaves the smart card, which is always in the possession of the owner. The comparison with the submitted sample takes place on the card. This further guarantees the privacy of the card owner. In addition, if the card is lost no one else can use it because others cannot present a sample that will match the on-board encrypted template of the owner and, given an unimpeachable enrollment process, the enrolled template on the card cannot be changed. When the biometric templates are stored on a card, the matching algorithm only has to perform a comparison of the user's biometric sample with the enrolled template held in the user's card, not an entire trusted database of n templates. This results in what is called *two-factor* authentication system based on (1) (*something the user is*) his or her measured biometric sample and (2) (*something the user has*) because the user must also have the card containing her/his enrolled template. Two-factor biometric systems using a smart card are, by definition, authentication systems because the card explicitly claims identity. Storing the biometric template in a card also reduces privacy concerns and the execution of the biometric-comparison algorithm on the same smart card further improves security because the template can be encrypted and need never leave the card or the possession of the owner.

One-to-Many Identification. In the one-to-many identification systems, the comparison necessary to positively identify the individual who submits a biometric sample must be with n other templates in a trusted database. Identification is a much more complex and usually more time consuming operation. Large databases tend to increase the time required to find the matching biometric and can also be a potential for security compromises made for operational convenience and usability. Hand geometry, speaker recognition, and signature recognition techniques are generally not recommended for one-to-many identification systems. See Table 17.3-2.

Error Rates. The driving factors in the choice of a biometric system are usually the error rates and ease of use. Errors can and do occur. However, the determination of theoretical derivation of system error rates and the trade-off between probable FRRs and probable FARs is a complex analytic problem.⁹⁶ Biometric thresholds must be set to provide a "secure enough" FAR with a "usable" FRR. FRRs vary widely among different types of biometric technologies and systems; however, within any single, given biometric system the FRR will be approximately the same whether the process is used for verification or identification because there is only one authentic template on file against which the live subject can make a match. Another potential error-rate measurement to consider is the "failure-to-enroll" rate. These error rates are difficult to identify and explain because so many variables are involved. Product and marketing managers are reluctant to go on record with any guarantee of unequivocal rates. In the final analysis, the error rates can only be established by operational use of a system; however, an attempt to assign representative subjective estimates of the six systems selected for this item as well as the system's ease of use appear in Table 17.3-2.

Comparative Costs. Costs for secure biometric identity-management systems are hard to derive. Pricing structures for systems offered by full systems houses are proprietary, and the resources for costing efforts in this period of growth and change are reserved for responses to requests from prospective customers. Similarly, component⁹⁷ suppliers' true costs are closely held and revealed only in bargaining with systems houses on a case-by-case basis, depending on the specifications that must be met, size of the order, and required delivery dates.

⁹⁶ For an understanding of this complex subject, see James L. Wayman, Director, *Error Rate Equations for the General Biometric System*, U.S. National Biometric Test Center, San Jose State University (originally published in *IEEE Robotics and Automation Magazine*, March 2000).

⁹⁷ See Section 4.4.1, Part 1: Introduction and general model, of the *Common Criteria for Information Technology Security Evaluation* (Common Criteria Version 2.1), which is identical to *International Standard ISO/IEC 15408:1999*, p. 25. Throughout the Information Security section, the organization and construction of the common criteria were used. *Class* is used for the most general grouping, which is the Information Systems section group. *Family* is a grouping of sets within a class, in this case, the Information Security family. *Component* describes a specific set and is the smallest selectable set of *technology items*.

Finally, a complete system architecture for an “ideal” secure biometric identity-management system comparison scale would have to be developed for a range of arbitrary domain sizes, which would provide a set of constant baseline costs for each system size to which the biometrics incremental costs could be added for valid

Table 17.3-2. Biometric System Comparative Description

Characteristics	Median System Processing Time for a Single Transaction	Systems Requirements	One-to-One Authentication Systems	One-to-Many Identification Systems	FAR and FRR Error Rates	Ease of Use	Relative Cost ⁹⁸
Fingerprint Systems	8 seconds for systems with optical sensor readers 15 seconds for chip-based sensor reader systems.	Fingerprint imaging techniques encode fingerprint information as a series of “minutiae” for templates ranging from 220 to 2,000 bytes; a system should require at least two finger-prints.	Compares a sample to a person’s enrolled authentic template on a card or in a trusted database to authenticate a claimed identity.	Capable of identification by comparing a sample measurement to a collection of many templates in a trusted database.	Recent study of single-finger comparison— FARs on the order of 10^{-5} ; FRRs on the order of $10^{-3,4}$, without binning or filtering.	May require significant cooperation from claimant.	\$\$\$
Facial Features	14 seconds.	Requires large, direct-access storage for large propulsions. Templates require 3500 bytes.	Compares a sample to a person’s enrolled authentic template on a card or in a trusted database to authenticate a claimed identity.	Capable of identification by comparing a sample measurement to a collection of many templates in a trusted database.	May be one of the higher error rate metrics.	Deserves a 10 on a scale of 1 to 10. Can be used surreptitiously.	\$\$\$\$
Hand Geometry	2 seconds for authentication; ~8 seconds, depending on size of database.	Requires the least amount of storage. Storage requirements for hand and finger templates are 800 to 9000 bytes.	Compares a sample to a person’s enrolled authentic template on a card or in a trusted database to authenticate a claimed identity.	Not recommended for identification. Users must claim an identity with a biometric template of the person they claim to be.	Not as accurate as fingerprints. Hands are not as unique as fingerprints.	Easiest to use.	\$\$\$\$\$

(Continued)

⁹⁸ Relative costs taken from the *Zephyr Analysis*, see http://www.biometricgroup.com/e/zephyr_charts.htm

Table 17.3-2. Biometric System Comparative Description (Cont'd)

Characteristics	Median System Processing Time for a Single Transaction	Systems Requirements	One-to-One Authentication Systems	One-to-Many Identification Systems	FAR and FRR Error Rates	Ease of Use	Relative Cost ⁹⁹
Iris Recognition	10 seconds.	Iris recognition systems require 512KB for each template, and only one template is required per person.	Compares a sample to a person's enrolled authentic template on a card or in a trusted database to authenticate a claimed identity.	Capable of identification by comparing a sample measurement to a collection of many templates in a trusted database.	Performs verification and identification with a FAR of 0.0. These systems operate at extremely false-accept and false-reject rates for individual comparisons.	Rated 9 on a scale of 1 to 10 in tests.	\$\$\$\$\$\$
Speaker Recognition	11 seconds.	Speaker recognition systems require 3KB to 1MB of voice data per 6seconds.	Compares the voice of a speaker to a sample of an enrolled person's authentic voice pattern template on a card or in a trusted database to authenticate a claimed identity.	Not recommended for identification. Users must claim an identity with a biometric template of the person they claim to be.	After 30+ years of research, this biometric is still not secure enough to rely upon as a stand-alone biometric.	Generally easy to use.	\$
Signature Recognition	~15 seconds plus the highly variable time required for completion of the sample signature or other signed symbols.	Requires large direct access storage for large populations. Templates require as little as 1KB.	Compares a sample to a person's enrolled authentic template on a card or in a trusted database to authenticate a claimed identity.	Not recommended for identification. Users must claim an identity with a biometric template of the person they claim to be.	May have high error rates due to normal variations in signature metrics and the physical condition of the claimant.	Most natural and some consider it easy.	\$\$

comparisons. The last column in Table 17.3-2 presents cost comparisons derived by interpolation of the positions of the cost symbols appearing in a *Zephyr Analysis* chart. Costs for adding biometrics to individual PCs can be more readily estimated. Various vendors incorporate fingerprint and iris devices into PC peripherals to supplement passwords for individual PCs and small LANs at prices ranging from \$100 to under \$300. Only those biometric hardware and software implementations, which have successfully passed NIST or an NVLAP-accredited laboratory testing for compliance with FIPS 140-1, should be considered for militarily critical information-security systems. Independent consultants advise that

- Biometric vendor claims are often unsubstantiated and product quality is usually poor or unacceptable;

⁹⁹ Relative costs taken from the *Zephyr Analysis*, see http://www.biometricgroup.com/e/zephyr_charts.htm

- The oldest “positive-identification” biometric, fingerprints, have been judged to be unscientific and must be accepted only as a probabilistic identification technology in U.S. courts;
- Identity theft, which is becoming a plague in the private sector, is both more likely and easier with COTS vendor systems that are either theoretical and never “buildable” or thrown-together gadgets that offer little real security; and
- DNA may be the best biometric ever developed, and with “chemlabs-on-a-chip” being produced by numerous government and civilian labs, DNA testing in near real time is highly probable in the near future.

SECTION 17.4—NETWORK FIREWALL TECHNOLOGY

Highlights

- A packet filter firewall is best suited to environments that do not require high security, complex filtering, or that do not have a large number of hosts to protect.
- Firewall functionality combinations now appearing in hybrid firewalls offer a variety of features, and most can be tailored to meet unique business and military information-system security requirements.
- A firewall now must be a part of any militarily critical or national infrastructure network-security architecture.
- Home users on commercial dial-in or with cable or digital subscriber line (DSL) connections should routinely employ personal firewalls and firewall appliances.
- Until very recently, relatively few vendors offered firewall systems.
- A firewall cannot defend against a data-driven attack in which something is mailed or copied to an internal host where it is then executed.
- A firewall cannot replace security discipline.

OVERVIEW

This section covers the major types of firewalls used to protect sites from exploitation of the inherent vulnerabilities of the TCP/IP protocol suite and legacy single-channel signaling, which is still in wide use and carries the bulk of Internet and other network traffic. Firewalls are also necessary at nodes serviced by fiber-optic links using signaling system number 7¹⁰⁰ and synchronous optical network switches. A firewall system can be a router, a personal computer, a host, or a collection of hosts, each set up specifically to shield a site or subnet from protocols and services that can be abused from entities outside the subnet. A firewall system is usually located at a higher level gateway, such as a site's connection to the Internet; however, firewall systems can be located at lower level gateways to provide protection for some smaller collection of hosts or subnets.

The network firewall technology items in this subsection are closely related to some of the technology items in the Information Technologies section because firewalls are software, or hardware and software combination, systems interposed between assets to be protected, such as mainframes, servers, workstations, local-area or enterprise and larger networks, and external, potentially hostile or uncontrolled networks and systems such as the Internet.

Computer operating systems and most applications have vulnerabilities that must be protected, thus making the Information Processing subsection technologies closely related to the network firewall items in this subsection, as are some telecommunications technologies in the Information Communications subsection. The networks and switching technology items in the links and nodes of information communications systems are also closely related to the network firewall items.

BACKGROUND

As the name implies, a firewall is a protection device that shields vulnerable areas from some form of danger. Since its discovery, fire was a principal form of comfort as well as danger. When men began to build clusters of houses with common walls, the need for firewalls to limit fire damage from an adjoining neighbor's house if it

¹⁰⁰ International common-channel signaling system recommendations established by the International Consultative Committee for Telephone and Telegraph (CCITT), a consultative committee of the International Telecommunications Union (ITU).

caught fire became obvious. Heavy masonry walls that extended a practical height above the rooflines were built between most houses with common walls to reduce the danger from a neighboring fire. These are common in the United States between what we now call “zero-lot-line” town houses or cluster homes. In the context of the Internet, a firewall manifests itself as a router, a personal computer, or a host or a collection of hosts set up specifically to shield a site or subnet from protocols and services that can be abused by entities outside the firewall through the use of open networks like the Internet. There is no firm definition of what constitutes a firewall. And until very recently, relatively few vendors offered firewall systems. Site administrators originally built their own firewalls, and no two were alike. The administrator’s time and effort often outweighed the cost of current vendor-tailored solutions. The term firewall can mean many things to many people. No definitions were identified that are approved by recognized standards organizations; however, the NIST Web site carries a helpful provisional definition:¹⁰¹

A firewall is any one of several ways of protecting one network from another untrusted network. The actual mechanism whereby this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that exists to block traffic, and the other, which exists to permit traffic. Some firewalls place greater emphasis on blocking traffic, while others emphasize permitting traffic.

Information-system network firewall history is very short, beginning in the early 1990s, about the same time that the phenomenal growth of open networks was apparent, principally due to the worldwide popularity of the Internet. For all the manifold marvelous benefits of the Internet, its enormous worldwide user base includes some comparatively small but significant elements that present a very real, tangible security threat. Criminals, vandals, and terrorists, to name a few of the easily recognized and more dangerous threat elements, can create information-system problems that have proved to be very expensive in terms of time as well as money. Although teleprocessing and dedicated closed networks existed before the advent of open networks and the Internet, these were largely exclusive intranets and extranets linking the business nodes in larger companies and those of their suppliers and teammates, usually over private leased lines with very little threat exposure. The internal threat was the largest threat for these closed networks and, of course, “insiders” are still responsible for the largest single category of security breaches. With the advent of the Internet, the world suddenly had access to all unprotected information-processing nodes that were “wired.” As the Internet developed into a complex, worldwide, modern, open network, security for everyone using the Internet became more problematic. Break-ins, viruses, and attacks now occur so frequently that they have become a regular, if unpleasant, part of access to the Internet. Now a firewall has to be a part of any network-security architecture, and home users on commercial dial-in or with cable or DSL connections routinely employ personal firewalls and firewall appliances.

Firewalls operate at Layers 7, 4, 3, and 2 (highest to lowest) of the open systems interconnect (OSI) model.¹⁰²

- Layer 7 is the *application layer*,¹⁰³ the top layer of the OSI seven-layer model. This layer handles issues like network transparency, resource allocation, and problem partitioning. The application layer is concerned with the user’s view of the network (e.g., formatting electronic mail messages). The presentation layer provides the application layer with a familiar local representation of data that is independent of the format used on the network.
- Layer 4 is the *transport layer*, the middle layer of the OSI seven-layer model. The transport layer determines how to use the network layer to provide a virtual error-free, point-to-point connection so that host A can send messages to host B and they will arrive uncorrupted and in the correct order. It establishes and dissolves connections between hosts. Level 4 is used by the session layer.

¹⁰¹ <http://csrc.nist.gov/publications/nistpubs/800-10/node81.html>.

¹⁰² The OSI model (ISO 7498, Open Systems Interconnect Reference Model) is an abstraction of network communications between computer systems and network devices. OSI is a model of network architecture and a suite of protocols (a protocol stack) to implement it, developed by ISO in 1978 as a framework for international standards in heterogeneous computer network architecture.

¹⁰³ For a complete explanation of all the levels and more detail, see Special Publication 800–41, *Guidelines on Firewalls and Firewall Policy*, NIST, Technology Administration, U.S. Department of Commerce, January 2002, p. 3.

- Layer 3 is the *network layer* (communications subnet layer). The network layer determines routing of packets of data from sender to receiver via the data-link layer, and it is used by the transport layer. The most common network layer protocol is IP.
- Layer 2 is the *data-link layer*. The data-link layer splits data into frames for sending on the physical layer and receives acknowledgment frames. It performs error checking and retransmits frames not received correctly. It provides an error-free virtual channel to the network layer. The data-link layer is split into an upper sublayer (logical link control) and a lower sublayer (media access control). Examples of protocols at this layer are ABP, Go Back N, SRP.
- Layer 1 is the *physical layer*. The lowest layer of the OSI seven-layer model, the physical layer has the electrical and mechanical connections to the network. The physical layer is used by the data-link layer. Examples of physical layer protocols are CSMA/CD, token ring, and bus.

Basic firewalls operate on a smaller number of layers. The more advanced firewalls will cover a larger number of layers. Generally, firewalls capable of examining a larger number of layers are more thorough and effective. A firewall that functions in layers 2 and 3 usually does not deal with specific users, but a higher end application proxy gateway firewall can enforce user authentication, as well as logging events for specific users. The greater the numbers of layers a firewall can examine tends to increase the configuration granularity present in the firewall. The added layer awareness created by utilizing all four applicable layers allows the firewall to accommodate advanced applications and protocols. Increasing the layers a firewall can examine also allows the firewall to provide services such as user authentication.

Several types of firewalls or firewall environments, which consist of various hardware devices, software operating systems and applications, should be carefully designed and tightly integrated to provide a last line of defense. A typical firewall environment for a militarily critical information-processing node might be configured with a boundary router, a main firewall and intrusion detection system connected to the protected network, and the network between the router and a main firewall. Four main types of firewalls are covered in this subsection. Naming conventions have not yet been codified and vary wildly as a result of manufacturers who attempt to insinuate themselves ahead of their competitors by catchy, unique names, which are sometimes coined by their marketing elements and have little technical relevance. The four firewall names selected for this subsection were taken from the names used in the recommendations of the NIST in its guidelines on firewalls and firewall policy.¹⁰⁴

- Packet filter firewalls;
- Stateful inspection firewalls;
- Application-proxy gateway firewalls; and
- Hybrid firewalls.

The individual technology item data sheets names are adaptations of the NIST naming convention.

Packet filter firewalls. Packet filters employ the most basic method of perimeter security. Packets are examined and dropped or “filtered,” typically by a router or a firewall, when they do not meet predetermined rules or “policies” set by the network administrator. The network administrators usually can configure the packet filters to check (1) the source, (2) destination address, and (3) the type of protocol embedded in the packet. The packet filter might be configured to drop or reject any packets not coming from “trusted” sites on the Internet side of the router that contain the Telnet protocol. The Telnet protocol can be used to provide remote control of a workstation, server, or other network device. Uncontrolled Telnet access from the Internet is a major security threat and potential cyber terrorist threat. Essentially all high-speed Internet connections have a router. Most routers have the capability to perform basic packet filtering without the cost of additional hardware or software. However, a fully filtered site has little flexibility, and because all designated packets or protocols are rejected, often the site cannot be accessed at all from “trusted” users outside the firewall.¹⁰⁵ Packet filters can be complex and difficult to maintain because the

¹⁰⁴ Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, NIST, Technology Administration, U.S. Department of Commerce, January 2002.

¹⁰⁵ “Firewall Technologies Explained,” Group Internet FW®, 5 May 2002, http://www.grouplifw.com/fw_tech.html.

network administrator must manually enter all the addresses and protocols to be filtered, or the router hosting the filter can be configured to exclude all packets from all addresses, in which case the information on sites that are allowed access must be maintained, which rapidly becomes an unmanageable and inefficient process.

Stateful inspection firewalls. The stateful packet inspection function consists of monitoring and assessing all packets associated with a specific communication session. Communication sessions between two computers will often consist of several thousand packets, each of which is identified by a unique “source” and “destination” address and a “sequence” number, which makes it possible for all of the packets to be reassembled into the correct data file at the destination computer. Sometimes thousands of sessions may be happening at the same time. A stateful inspection firewall keeps track of these concurrent sessions, and each packet of data is checked to ensure that it belongs to the proper session. Any stray packets that are not part of an established session are rejected. Each of the communication sessions is checked and validated by the source and destination addresses of the machines in the session to ensure that all packets belong to the proper session. This firewall also screens the packets at the software “port”¹⁰⁶ level. A software port is a unique address extension that the application software uses to communicate with other addresses. A software application port-level filter provides an additional way for the network administrator to control the traffic and ensure that only authorized transactions are allowed through the firewall. A high level of protection is provided to users communicating with systems external to the “trusted” network because stateful inspection ensures that all packets are part of an authorized communication session. stateful inspection also provides additional security controls by enabling the enforcement of security policies at the “application socket” or port layer levels as well as the protocol and address levels. Unfortunately, there are usually significant additional costs associated with stateful inspection. Stateful inspection functionality currently requires the purchase of additional software or hardware, or both, because this functionality is not typically bundled with other network devices on the market today.

Application-proxy firewalls. Because application proxies examine packets at the application program level, a very fine level of security and access control can be enforced and a high level of protection can be provided against “denial of service” attacks. An application proxy firewall can be configured to reject all inbound packets that contain common executable file types such as .EXE or .COM files, which hackers or “crackers” often use to introduce dangerous virus and worm files into a network. Basically, a proxy software program or device makes software requests on behalf of another device on the network. A typical proxy server is configured to perform Internet browser functions in response to software requests from workstations on the trusted, or internal, network side of the firewall. The workstation browser sends its browsing requests to the proxy server rather than directly to the destination Web server on the Internet. The proxy then forwards the browsing request to the destination Webserver and examines the packets that are returned from the remote Web server. The proxy server examines the actual application program data contained within the packets to reject or pass them on to the originating workstation based on the security policy set by the network administrator.

Hybrid Firewalls. The type of firewall, or firewall environment, required for adequate protection depends on the size of the node, the amount of network traffic, the sensitivity of the systems and data, and the applications required by the node. The final basis for the choice of a firewall should be its feature set. A standard firewall configuration usually consists of a router with an access-control capability at the boundary of the organization’s network and then a more powerful firewall located behind the router. If secure remote access is required, the firewall may have to incorporate a virtual private network (VPN) server to provide the cryptographic functions required for the encrypted traffic between the firewall and remote sites in the organization or between the firewall and other sites on the Internet. The security system engineering for the configuration of the firewall environment should start with a carefully thought out SPP and be performed so that complexity is minimized and management demands are limited, while providing adequate protection for the organization’s networks.

Network firewall technologies are moving very fast, with typical development cycles of 9 months, tending toward 6 months. The industry is growing rapidly in more than 100 countries, and there is the usual rush to market in order to be first to market, first to capture mind-share and the largest market position, almost without regard to quality. The watchwords for those considering firewall acquisition are *caveat emptor*.¹⁰⁷

¹⁰⁶ The TCP/IP protocol suite includes the notion of *ports*, which can be viewed as end points for sessions.

¹⁰⁷ Buyer beware.

LIST OF MCTL TECHNOLOGY DATA SHEETS
17.4. NETWORK FIREWALL TECHNOLOGY

17.4-1	Packet-Filtering Technology.....	MCTL-17-71
17.4-2	Stateful Packet Inspection Technology.....	MCTL-17-74
17.4-3	Application Proxy Technology	MCTL-17-76
17.4-4	Hybrid Firewall Technology.....	MCTL-17-78

MCTL DATA SHEET 17.4-1. PACKET-FILTERING TECHNOLOGY

Critical Technology Parameter(s)	Military and national-defense packet-filtering firewall versions shall have the specified military and national-defense security policies for performing guard and classified functions. Packet filters shall pass data at connection rates equal to or greater than T1. ¹⁰⁸ Packet filters shall be “hardened” with special tamper-resistant hardware technology built or tailored to meet specified protection profiles. If firewalls are integrated with other network security functions such as cryptographic, identity management, authentication, access authorization, and network backup and recovery functions, the specified protection profile shall be appropriate for the highest classification of the integrated functions performed and information inside the firewall, but shall be no less than a certified ¹⁰⁹ Common-Criteria-level EAL 4. ¹¹⁰
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential, untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Most commercial enterprises now consider the acquisition and maintenance of firewalls essential under the prudential rule. However, many companies seem to resist actually turning on the firewall or developing the ruleset correctly. Because of the great difficulty in configuring and testing firewalls without interfering with legitimate network traffic, firewalls are often not effective (i.e., they are permissively configured with a poor ruleset and easily exploited or bypassed by attackers). The COTS marketplace drives down prices, especially for software-only network firewalls, but COTS products do little to increase firewall utility and effectiveness in complex, near-real-time networks.
Affordability Issues	Affordability is not an issue for COTS products because the highly competitive marketplace keeps margins small. However, the technology is moving so fast that there are often unusually high, nonrecurring-engineering costs; a high probability of product obsolescence even before deployment; and all the associated systems and logistics problems, especially in the case of those products that the manufacturer can no longer afford to support.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

¹⁰⁸ 1.5 Megabits per second.

¹⁰⁹ Certified by a member of the National Voluntary Laboratory Accreditation Program (NVLAP), organized by NIST, which provides accredited laboratories that perform FIPS 140-1 compliance testing.

¹¹⁰ Based on Version 2.1 of the *Common Criteria*, International Standard 15408. The *Common Criteria* can be found at <http://csrc.nist.gov/cc>. EAL 4 compares to the TCSEC B1: Labeled Security and ITSEC E3; however, Common Criteria provides a security requirement and specification criteria for product differentiation and assurance not offered by other schemes.

BACKGROUND

Packet Filtering firewalls are software, or hardware and software combinations, that function at the interfaces between the assets to be protected and entities outside the firewall. Assets to be protected are workstations, local-area and enterprise networks that must be protected from larger external potentially hostile or uncontrolled networks, and open systems such as the Internet. Packet filters are the most basic and fundamental type of firewall. They include access-control functionality for system addresses and communications sessions. Packet filters are normally located in routers to provide control and direction for IP addresses and to designate the correct ports¹¹¹ for connections. This simple functionality is a fundamental adjunct to more sophisticated protection applications. The packet filter access control functionality is governed by a set of directives collectively referred to as a *ruleset*.

A ruleset is a software or firmware table of instructions that the firewall uses for determining how packets are to be routed across its interfaces. The ruleset is examined from top to bottom when making routing decisions. When a packet firewall accepts a packet, it determines the protocol in use and the packet's source and destination addresses and ports. The firewall then runs down through the rules to determine the disposition of the packet. When a rule permits or denies the packet entry, the firewall takes one of three general actions:

1. If the rule specifies “*Allow*,” the firewall *accepts* the packet and passes it through the firewall as requested, performing the logging functions incorporated in the firewall software.
2. If the rule specifies “*Deny*,” the firewall *denies* the packet entry, dropping the packet and generating an error message to the source system, if required by the ruleset.
3. If the rule specifies “*Discard*,” the firewall *drops* the packet into the “bit bucket,” but does not generate an error message to the source system and may or may not generate a log entry, depending on the ruleset specification. The discard action implements the so-called “*black hole*” strategy of not revealing the presence of a firewall to an outsider.

The number of rules in a ruleset varies widely, and a typical ruleset is much longer and more detailed than the illustration in Table 17.4-1. The packet filter software always reads the ruleset table from top to bottom.

Table 17.4-1. Packet Filter Firewall Ruleset Illustration

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	137.123.2.0*	> 1023*	Allow	Rule to allow return TCP Connections to internal subnet.
2	Any	Any	137.123.2.0*	Any	Deny	Prevent external user from directly accessing the Firewall system.
3	137.123.2.0*	Any	Any	Any	Deny	Prevents the firewall system from directly connecting to anything.
<i>n</i>	Any	Any	Any	Any	Deny	Everything not previously allowed is explicitly denied.
* Arbitrary notional number.						

The first rule is the “*Return Connection*” rule, which requires that responding packets from external systems be allowed to return to originating internal systems to complete the connection, assuming that the connection is authorized. If connection with the external system is allowed, the connection-oriented TCP rules require that responding packets from an external system must be allowed to complete the connection. Packet-filter firewalls must allow inbound responding TCP network traffic packets that return from a selected destination system to enter,

¹¹¹ The TCP/IP protocol suite includes the notion of *ports*, which can be viewed as end points for sessions.

usually through any port with number higher¹¹² than 1,023, as shown in the first rule in Table 17.4-1. The second rule prevents any packet from any source outside the packet-filter firewall from accessing the firewall directly. Rule three prevents the firewall from directly connecting to any outside source. The other rules that are required to enforce the specified security policy followed. The rule in the last row (*n*) of the ruleset table simply blocks all other packets from outside sources not specifically allowed by the ruleset. If this last rule in the ruleset table were accidentally not included, all traffic originating from outside the firewall not covered by the ruleset would be allowed to enter!

With long, detailed rulesets, it is only human to make mistakes in developing and maintaining the ruleset that could be disastrous. The ruleset should be reviewed very carefully and thoroughly tested before implementation. In addition, the ruleset should be reviewed at regular intervals after installation to ensure that the specified ruleset protocols still meet the organization's ever-changing requirements and to minimize the possibility of logical errors when new rules are added and old rules are changed or deleted. Basic packet filters are not aware of "state." For performance or other reasons, ordinary packet filters do not attempt to remember previous states of packets, connections, and patterns to make access and security decisions.¹¹³

¹¹² The convention is that any port less than 1,024 is likely to be a low-numbered port at the destination on the remote host.

¹¹³ Ascend has adopted "Stateful Packet Inspection" (a descriptor also used by Checkpoint), which it calls Dynamic Firewall Technology (also called "Secure Access" and "Perimeter Firewall") and ships in a router product. Stateful Packet Inspection is a far more powerful control, but does not attempt processor-intensive functions such as e-mail virus scanning.

MCTL DATA SHEET 17.4-2. STATEFUL PACKET INSPECTION TECHNOLOGY

Critical Technology Parameter(s)	Military and national-defense stateful packet inspection firewall versions shall have the specified military and national defense security policies for performing guard and classified functions. Stateful packet inspection firewalls shall pass data at connection rates equal to or greater than T1. ¹¹⁴ Stateful packet inspection firewalls shall be “hardened” with special tamper-resistant hardware technology built or tailored to meet specified protection profiles. If stateful packet inspection firewalls are integrated with other network security functions such as cryptographic, identity management, authentication, access authorization, and network backup and recovery functions, the specified protection profile shall be appropriate for the highest classification of the integrated functions performed and information inside the firewall, but shall be no less than a certified ¹¹⁵ common criteria level EAL 4. ¹¹⁶
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Most commercial enterprises now consider the acquisition and maintenance of firewalls essential under the prudential rule.
Affordability Issues	Affordability is not an issue for COTS products because the highly competitive marketplace keeps margins small; however, the technology is moving so fast that there are often unusually high, nonrecurring-engineering costs, and a high probability of product obsolescence even before deployment, with all the associated systems and logistics problems, especially in the case of those products that the manufacturer can no longer afford to support.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

BACKGROUND

A *stateful packet inspection* firewall is a packet filter that incorporates the added awareness of the OSI model Layer 4 data. Layer 4 is the *transport layer*, the middle layer of the OSI seven-layer model. The transport layer determines how to use the network layer to provide a virtual error-free, point-to-point connection so that host A can send messages to host B, and they will arrive uncorrupted and in the correct order. It also establishes and dissolves connections between hosts. Layer 4 supports the *session Layer 5*.¹¹⁷ Layer 4 is used to identify specific network applications and communication *sessions*, as opposed to network address. A system may have any number of Layer

¹¹⁴ 1.5 Megabits per second.

¹¹⁵ Certified by a member of the NVLAP, organized by NIST, which provides accredited laboratories that perform FIPS 140-1 compliance testing.

¹¹⁶ Based on Version 2.1 of the “Common Criteria,” International Standard 15408. The Common Criteria can be found at <http://csrc.nist.gov/cc>. EAL 4 compares to the TCSEC B1: Labeled Security and ITSEC E3; however, Common Criteria provides a level of product differentiation and assurance not offered by other schemes.

¹¹⁷ The upper layers of the OSI model (5, 6, and 7) are for end-user applications and systems.

4 sessions with other systems on the same network. Terminology associated with the TCP/IP protocol suite includes the notion of *ports*, which can be viewed as end points for sessions. A *source port* number identifies the communication session at the originating system. A *destination port* identifies the communications session of the destination system. Stateful packet inspection firewalls evolved from the requirement to accommodate certain features of the TCP/IP protocol suite that made firewall deployment difficult. When a TCP, connection-oriented, transport application creates a session with a remote host system, a port is also created on the source system for the purpose of receiving network traffic from the destination system.

The stateful packet inspection function consists of monitoring and assessing all packets associated with a specific communication session. Communication sessions between two computers will often consist of several thousand packets, each of which is identified by a unique “*source*” and “*destination*” address and a “*sequence*” number, which makes it possible for all of the packets to be reassembled into the correct data file at the destination computer. The TCP specification requires that the client source port be some number greater than 1,023 and less than 16,384.¹¹⁸ Packet filters must allow inbound connection-oriented return packets to connect through high numbered ports from destination systems. The first row of Table 17.4-1 from the Packet Filtering Technology item is reproduced below for ready reference. It allows any inbound connection to enter, if the destination port is greater than 1,023, as required by the TCP specification “*Return Connection*” rule, which requires that responding packets from external systems be allowed to return to originating internal systems to complete the connection, assuming the connection is one that is authorized.

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	137.123.2.0*	> 1023*	Allow	Rule to allow return TCP Connections to internal subnet.

Source: Table 17.4-1, Packet Filter Firewall Ruleset Illustration.

Sometimes thousands of sessions may be happening at the same time. A stateful inspection firewall keeps track of these concurrent sessions, and each packet of data is checked to ensure that it belongs to the proper session. Any stray packets that are not part of an established session are rejected. Each of the communication sessions is checked and validated by the source and destination addresses of the machines in the session to ensure that all packets belong to the proper session. Opening a large number of high-numbered ports creates an immense risk of intrusion by unauthorized users who may employ a variety of techniques to abuse the expected conventions. Stateful packet inspection firewalls solve this problem by creating a directory of outbound TCP connections, along with each session’s corresponding client port number. This “*state table*” is then used to validate any inbound traffic. This stateful inspection solution is more secure than packet filters alone because the stateful packet firewall tracks client ports individually to restrict access to responses to requested sessions rather than simply opening all high-numbered ports to any external access request.

¹¹⁸ For the Simple Mail Transport Protocol (SMTP), the TCP/IP convention requires that the low-numbered port be 25.

MCTL DATA SHEET 17.4-3. APPLICATION PROXY TECHNOLOGY

Critical Technology Parameter(s)	Military and national-defense application proxy firewall versions shall have the specified military and national-defense security policies for performing gateway functions. Application-proxy firewalls shall pass data at connection rates equal to or greater than T1. ¹¹⁹ Application-proxy firewall software shall be “hardened” and special tamper-resistant hardware built or tailored to meet the specified protection profiles. Application-proxy firewalls will be integrated with other network firewalls and tailored to support specific protocols and applications, such as cryptographic, identity management, authentication, and access authorization security functions, as well as network backup and recovery functions, as required. The specified protection profile shall be appropriate for the highest classification of the integrated functions performed and information to be protected, but shall be no less than a certified ¹²⁰ common criteria level EAL 4. ¹²¹
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Large commercial enterprises now consider the acquisition and maintenance of application-proxy gateway firewalls essential, and there are strong business cases supporting their use for the protection of high-value assets.
Affordability Issues	Affordability is usually not an issue for COTS products because the highly competitive marketplace keeps margins small. However, the technology is moving so fast that there are often unusually high, nonrecurring-engineering costs, and a high probability of product obsolescence even before deployment, with all the associated systems and logistics problems, especially in the case of those products that the manufacturer can no longer afford to support. Application proxies must be tailored for specific applications and protocols and must be changed when these applications and protocols are updated or further developed to incorporate additional features. The operation and maintenance of application proxy gateways can be a significant cost.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

BACKGROUND

Application-proxy servers are software or software-and-hardware processors that operate between external and internal networks, which usually operate in concert with other types of firewalls. In many cases, internal systems

¹¹⁹ 1.5 Megabits per second.

¹²⁰ Certified by a member of the NVLAP, organized by NIST, which provides accredited laboratories that perform FIPS 140-1 compliance testing.

¹²¹ Based on Version 2.1 of the “Common Criteria,” International Standard 15408. The Common Criteria can be found at <http://www.csrc.nist.gov/cc>. EAL 4 compares to the TCSEC B1: Labeled Security and ITSEC E3; however, Common Criteria provides a level of product differentiation and assurance not offered by other schemes.

may go on operating as if directly connected to external networks while actually having their communications inspected and protected by the proxy. With correct tailoring, the proxy can be transparent and of sufficient capacity to see all necessary control information (encryption can prevent such full inspection). Each conventional network service, such as Telnet and FTP, should be proxied. Proxies can perform additional useful functions such as network address translation.

Application-proxy firewalls are advanced gateway firewalls that combine access control with application Layer 4 functionality. Application proxies do not require a network layer 3 route between the inside and outside interfaces of the firewall because the firewall software performs the routing. If application-proxy gateway software ceases to function, the firewall system is unable to pass network packets through the firewall system. All network packets that traverse the firewall must do so under application-proxy software control. Each individual application proxy also referred to as a “*proxy agent*” interfaces directly with the firewall access control ruleset to determine whether a packet should be permitted to transit the firewall. In addition to the ruleset reference, each proxy agent has the ability to require authentication of each individual network user. This user authentication can be

- User ID and password authentication;
- Hardware or software token authentication;
- Secure address authentication; and
- Biometric authentication.

An application-proxy firewall can be set up to take one class C address and map it to another class C address. Various products can use this feature to map one address from the Internet service provider (ISP) into multiple unregistered *packet* addresses on the internal network. DARPA and NSA have piloted the *secure network server* and *secure message guard* intended for DMS use. Similarly, industry is pursuing prototype software technology-transfer efforts for national defense and other government and commercial use.¹²² Assuming technical obstacles can be overcome, prototypes should be available soon; but widespread use in the next 5 years is not expected because of government COTS acquisition policies.¹²³

¹²² Secure Computing Corporation’s *dynamic type-enforcement “sidewinder” firewall* is an example of one form of “hardening” referred to in the Military Critical Parameter row of the data table.

¹²³ See Col. Alan D. Campen, USAF (Ret.), “COTS Is Only as Good as the Shelf,” *SIGNAL Magazine*, January 2001, at <http://www.us.net/signal/Archive/Jan01/cots-jan.html>

MCTL DATA SHEET 17.4-4. HYBRID FIREWALL TECHNOLOGY

Critical Technology Parameter(s)	Military and national-defense hybrid firewall versions shall have the specified military and national-defense security policies for performing gateway functions. Hybrid firewalls shall pass data at connection rates equal to or greater than T1. ¹²⁴ Hybrid firewall software shall be “hardened” and special tamper-resistant hardware built or tailored to meet the specified protection profiles. Hybrid firewalls will be integrated with other network firewalls and tailored to support specific protocols and applications such as cryptographic, identity management, authentication, and access authorization security functions, as well as network backup and recovery functions, as required. The specified protection profile shall be appropriate for the highest classification of the integrated functions performed and information to be protected, but shall be no less than a certified ¹²⁵ common criteria level EAL 4. ¹²⁶
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Elaborate network and security test beds are required for the development of military and national security products, some of which are highly classified.
Unique Software	Especially robust operating systems capable of safely running essential untrusted application software, including applications intended for selected COTS operating systems and specially integrated security and cryptographic software from classified sources.
Major Commercial Applications	Commercial Internet applications drive this technology. Large commercial enterprises now consider the acquisition and maintenance of hybrid firewalls essential, and there are strong business cases supporting their use for the protection of high-value assets.
Affordability Issues	Affordability is usually not an issue for COTS products because the highly competitive marketplace keeps margins small; however, the technology is moving so fast that there are often unusually high, nonrecurring-engineering costs, and a high probability of product obsolescence even before deployment, with all the associated systems and logistics problems, especially in the case of those products that the manufacturer can no longer afford to support. Application proxies must be tailored for specific applications and protocols and must be changed when these applications and protocols are updated or further developed to incorporate additional features. The operation and maintenance of hybrid firewalls can be a significant cost.
Export Control References	WA Cat 5, 5E2; CCL Cat 5E; WA ML 11; USML XI and XIII.

BACKGROUND

Hybrid firewalls is a name used to collectively identify a type of firewall that recent computer science advances and inspired system engineering have made possible in response to the increasing variety of military *information dominance* requirements and business requirements resulting from the growth in e-commerce on the Internet. Advances in network infrastructure system engineering, computer science, and information-security system

¹²⁴ 1.5 Megabits per second.

¹²⁵ Certified by a member of the NVLAP, organized by NIST, which provides accredited laboratories that perform FIPS 140-1 compliance testing.

¹²⁶ Based on Version 2.1 of the “Common Criteria,” International Standard 15408. The Common Criteria can be found at <http://www.csrc.nist.gov/cc>. EAL 4 compares to the TCSEC B1: Labeled Security and ITSEC E3; however, Common Criteria provides a level of product differentiation and assurance not offered by other schemes.

engineering have resulted in a blurring of the original distinctions that differentiated the once fairly pure first-generation firewall types: *packet filter* (17.4.1), *stateful packet inspection* (17.4.2), and *application proxy* (17.4.3).

Many of the major products in COTS Network Firewalls are *combinations* of proxies and application-level gateways,¹²⁷ which are a powerful but complex and expensive form of network firewalls, because packet inspection operations are performed on the data payload of the packet. This is the information that the application programs process, allowing, for example:

- Virus Scanning of incoming FTP files and e-mail.
- Control over what FTP commands the user is permitted to execute.
- Control over which commands are to be allowed for the execution of any particular service.

DARPA and NSA have sponsored the secure network server and secure message guard intended for DMS use. Industry also is investing in R&D efforts. Secure Computing Corporation's dynamic-type enforcement "*Sidewinder*" firewall is an example. Industry is pursuing software technology transfer for national defense and other government as well as commercial use. Assuming technical obstacles are overcome, prototypes should be appearing soon, but widespread federal system use of these new products in the next 5 years is likely to be frustrated by government COTS acquisition policies.¹²⁸

¹²⁷ Raptor Eagle, NAI/TIS' Gauntlet, Harris' Nighthawk, and SCC's Sidewinder.

¹²⁸ See Col. Alan D. Campen, USAF (Ret.), "COTS Is Only as Good as the Shelf," *SIGNAL Magazine*, January 2001, at <http://www.us.net/signal/Archive/Jan01/cots-jan.html>

INDEX OF MCTL TECHNOLOGY DATA SHEETS

INDEX OF MCTL TECHNOLOGY DATA SHEETS

18.1-12	Acoustic Signature: Active Systems	MCTL-18-14
18.1-11	Acoustic Signature: Noise Reduction Techniques	MCTL-18-14
18.2-3	Acoustic Systems	MCTL-18-23
16.4-10	Active Electromagnetic Sensors	MCTL-16-76
18.1-15	Active Systems to Control Magnetic Signature	MCTL-18-16
12.2-8	Aerostatic Bearings	MCTL-12-34
16.1-16	Angular or Rotational Accelerometers	MCTL-16-28
17.4-3	Application Proxy Technology	MCTL-17-76
17.1-2	Asymmetric Key Technology	MCTL-17-24
16.5-2	Atomic/Ion Clocks	MCTL-16-84
16.6-4	Automatic Target Recognition	MCTL-16-96
16.1-4	Azimuth (North-Pointing) Determination Systems	MCTL-16-14
12.2-7	Bearings, Active Magnetic	MCTL-12-33
12.2-6	Bearings, Gas Lubricated Foil	MCTL-12-32
12.2-5	Bearings, Needle Roller	MCTL-12-31
12.2-4	Bearings, Solid Tapered Roller	MCTL-12-30
17.3-1	Biometric Technology	MCTL-17-49
5.2-13	C4I Systems	MCTL-5-33
12.5-19	CBN-Coated Cutting Tools	MCTL-12-75
12.6-1	Chemical Vapor Deposition (CVD) Equipment	MCTL-12-81
5.1-4	Collective Protection	MCTL-5-12
12.1-9	Composite Filament-Winding Equipment	MCTL-12-17
12.1-10	Composite Tape-Laying Equipment	MCTL-12-18
12.1-11	Composite Weaving, Stitching, or Interlacing Equipment	MCTL-12-19
12.4-4	Computed Tomography (CT)	MCTL-12-52
18.3-2	Control Surfaces	MCTL-18-30
12.3-1	Coordinate Measuring Machine (CMM)	MCTL-12-41
17.1-3	Cryptanalytic Technology	MCTL-17-28
12.5-17	Cubic-Boron-Nitride (CBN) Grinding Wheels for Hardened Steel Gears and Bearings	MCTL-12-73
16.3-7	Date-Based Referenced Navigation Systems (Digital Terrain, Bathymetric, Magnetic, Gravity, and Stellar)	MCTL-16-58
5.1-6	Decontaminants—Equipment	MCTL-5-14

5.1-7	Decontaminants—Personnel	MCTL-5-15
12.5-5	Deep-Hole Drilling Machines	MCTL-12-61
12.5-14	Diamond Cutting Tool Inserts	MCTL-12-70
18.1-3	Dielectric RAM	MCTL-18-10
16.3-3	Differential Global Navigation Satellite System Receivers	MCTL-16-52
12.4-3	Digital Holographic Nondestructive Testing	MCTL-12-51
12.4-1	Digital Shearography	MCTL-12-49
17.2-2	Digital Steganalytic Technology	MCTL-17-41
17.2-1	Digital Steganographic Technology	MCTL-17-39
16.3-6	Direction-Finding Equipment	MCTL-16-57
16.3-5	Doppler (Radar and Sonar) Navigation Systems and Passive Acoustic Navigation Systems	MCTL-16-56
16.1-7	Dynamically Tuned Gyroscopes	MCTL-16-17
12.5-8	Electrodischarge Machines of Nonwire Type	MCTL-12-64
12.5-7	Electrodischarge Machines of Wire-Feed Type	MCTL-12-63
16.1-8	Electrostatically Supported Gyroscopes	MCTL-16-18
17.1-4	Embeddable Programmable Cryptographic Processor Technology	MCTL-17-32
5.2-9	Enzymatic Chemistry and Colorimetric Chemistry	MCTL-5-29
12.1-12	Equipment for Manufacturing Microelectromechanical Devices (i.e., MEMS)	MCTL-12-20
12.1-5	Equipment for Producing Prepregs by the Hot-Melt Method	MCTL-12-13
16.1-11	Fiber-Optic Gyroscopes	MCTL-16-22
5.2-1	Flame Photometry and Gas Chromatography/Flame Photometry (GC-FPD)	MCTL-5-21
16.1-6	Floated Gyroscopes	MCTL-16-16
5.1-3	Full Protection (Encapsulation) Suit	MCTL-5-11
16.1-5	Generic Gyroscopes	MCTL-16-15
16.1-13	Generic Linear Accelerometers	MCTL-16-25
16.3-1	Global Navigation Satellite System Receivers	MCTL-16-49
16.2-4	Gravity Gradiometers for Moving-Base Measurements	MCTL-16-40
16.2-3	Gravity Gradiometers for Static Measurements	MCTL-16-39
16.2-2	Gravity Meters (Gravimeters) for Moving-Base Measurements	MCTL-16-38
16.2-1	Gravity Meters (Gravimeters) for Static Measurements	MCTL-16-37
12.5-6	Grinding Machine With Three or More Axes for Removing or Cutting Metals, Ceramics, or Composites	MCTL-12-62
16.1-3	Gyro Astro-Tracking Devices	MCTL-16-13
16.1-9	Hemispherical Resonator Gyroscopes	MCTL-16-19

12.2-1	High-Speed Bearings, Ball or Solid Roller, Except Tapered	MCTL-12-27
12.6-7	High-Temperature Protection Coatings for Engine Parts	MCTL-12-87
12.1-6	Hot Isostatic Presses (HIPs)	MCTL-12-14
17.4-4	Hybrid Firewall Technology	MCTL-17-78
16.1-2	Hybrid Inertial Navigation Systems (Including GNSS)	MCTL-16-11
16.3-4	Hybrid Radio and Data-Based Referenced Navigation Systems (Other than Inertial Navigation Systems)	MCTL-16-54
12.2-9	Hydrostatic Bearings	MCTL-12-35
16.1-1	Inertial Navigation Systems	MCTL-16-9
18.2-2	Infrared, Electro-Optical and Visual	MCTL-18-22
12.6-4	Ion Assisted Resistive Heating Vapor Deposition (Ion Plating) Production Equipment	MCTL-12-84
12.6-3	Ion Implantation Production Equipment	MCTL-12-83
5.2-3	Ion Mobility Spectrometry (IMS)	MCTL-5-23
5.2-10	Ion Trap Secondary Ion Mass Spectrometry	MCTL-5-30
18.1-10	IR Prediction Codes	MCTL-18-13
18.1-5	IR Signature Control Techniques	MCTL-18-11
18.1-7	Laser and Electro-optic	MCTL-18-12
16.6-2	Laser Identification Systems	MCTL-16-94
12.3-4	Laser Location Systems	MCTL-12-44
16.1-15	Linear Accelerometers (Including MEMS Accelerometers)	MCTL-16-27
16.1-14	Linear Accelerometers (Other than Micromachined)	MCTL-16-26
12.3-2	Linear and Angular Displacement Measuring Devices	MCTL-12-42
12.5-13	Linear Guide Assemblies for Machine Tools and Inspection Equipment	MCTL-12-69
12.5-11	Linear Position Feedback Units (e.g., Inductive-Type Devices, Graduated Scales, or Laser Systems)	MCTL-12-67
16.5-3	Low-Power Clocks and Oscillators	MCTL-16-85
12.2-2	Low-Torque, Antifriction Bearing, Ball or Solid Roller, Except Tapered	MCTL-12-28
16.3-8	LPI/LPD Radar Altimeters and Fathometers	MCTL-16-59
12.5-9	Machine Tools for Removing Metals, Ceramics, or Composites by Means of Water, Other Liquid Jets, Electron Beam (E Beam), or Laser Beam	MCTL-12-65
16.4-11	Magnetic and Electric Field Sensor Arrays	MCTL-16-77
16.4-8	Magnetic Gradiometers	MCTL-16-74
18.1-2	Magnetic RAM	MCTL-18-9
16.4-6	Magnetometers—Fiber Optic	MCTL-16-72
16.4-5	Magnetometers—Flux Gate	MCTL-16-71

16.4-4	Magnetometers—Induction Coil	MCTL-16-70
16.4-7	Magnetometers—Magnetoresistive	MCTL-16-73
16.4-3	Magnetometers—Nuclear Precession (Proton/Overhauser/Helium-3)	MCTL-16-69
16.4-2	Magnetometers—Optically Pumped/Electron Resonance (Helium-4, Potassium, Rubidium, or Cesium)	MCTL-16-67
16.4-1	Magnetometers—Superconducting Quantum Interference Devices	MCTL-16-65
5.2-2	Mass Spectrometry (MS) and Gas Chromatography/Mass Spectrometry (GC-MS)	MCTL-5-22
12.3-3	Metrology Equipment for Spectral Characterization of Reflectance, Transmission, Absorption, and Scatter	MCTL-12-43
12.5-18	Microelectromechanical Systems (MEMS)	MCTL-12-74
16.1-12	Microelectromechanical Systems (MEMS) Gyroscopes	MCTL-16-23
5.3-1	Mid- and Far-Infrared—Scattering, Absorbing	MCTL-5-39
5.3-3	Millimeter Wave—Absorbing	MCTL-5-41
5.3-2	Millimeter Wave—Scattering	MCTL-5-40
12.5-1	Milling Machine With Five or More Axes for Removing or Cutting Metals, Ceramics, or Composites	MCTL-12-57
12.5-2	Milling Machine With Three Linear Axes and Either One Rotary Axis or a Rotating Table, for Removing or Cutting Metals, Ceramics, or Composites	MCTL-12-58
18.3-4	Mission Equipment Integration	MCTL-18-31
16.3-2	Multichip Module Technology (GPS Receiver on a Chip)	MCTL-16-51
16.1-17	Multifunction Inertial Sensors	MCTL-16-30
16.6-5	Multisensor Fusion	MCTL-16-97
12.5-16	Multitask Machine Tools	MCTL-12-72
16.5-4	Optical Clocks	MCTL-16-87
16.6-3	Optical Identification Systems	MCTL-16-95
17.4-1	Packet-Filtering Technology	MCTL-17-71
18.2-4	Passive Coherent Location	MCTL-18-24
5.2-4	Passive Infrared	MCTL-5-24
18.1-14	Passive Mounts and Supports	MCTL-18-15
18.1-16	Passive Systems to Control Magnetic Signature	MCTL-18-16
12.6-2	Physical Vapor Deposition (PVD) Equipment	MCTL-12-82
18.3-1	Planform/Outer Surface	MCTL-18-29
5.2-6	Portable Isotopic Neutron Spectroscopy	MCTL-5-26
12.2-3	Precision Ball Bearings and Solid Roller Bearings	MCTL-12-29
18.1-13	Prediction Models Multispectral Signatures Surface and Subsurface Vessels	MCTL-18-15

18.3-5	Propulsion System	MCTL-18-31
5.1-2	Protective Clothing, Battlefield	MCTL-5-10
5.1-1	Protective Masks	MCTL-5-9
12.1-8	Pyrolytic Deposition Equipment	MCTL-12-16
18.1-4	Radar Absorbing Structure	MCTL-18-10
16.6-1	Radio-Frequency Identification Systems	MCTL-16-93
5.2-7	Raman Spectroscopy	MCTL-5-27
12.1-13	Rapid Prototyping Manufacturing (RPM)	MCTL-12-21
18.1-9	RCS Prediction Codes	MCTL-18-13
5.2-14	Reconnaissance Systems	MCTL-5-34
5.1-5	Regenerative Filtration—Pressure Swing Adsorption	MCTL-5-13
16.1-10	Ring Laser Gyroscopes	MCTL-16-21
12.5-12	Rotary Position Feedback Units (e.g., Inductive-Type Devices, Graduated Scales, or Laser Systems)	MCTL-12-68
5.2-11	Sample Collection	MCTL-5-31
5.2-12	Sample Processing	MCTL-5-32
17.3-3	Secure Identity-Management System Technology	MCTL-17-57
18.1-1	Sheets and Thin Films	MCTL-18-9
12.1-7	Single Crystal (SC) Alloy Casting Equipment	MCTL-12-15
17.3-2	Smart-Card Technology	MCTL-17-54
12.5-15	Software for Electronic Devices that Have Grater Than or Equal to Four-Axis Simultaneous Contouring Control	MCTL-12-71
12.1-1	Spin, Flow-, and Shear-Forming Machines	MCTL-12-9
12.5-10	Spindle Assemblies, Consisting of Spindles and Bearings, Specially Designed for Machine Tools	MCTL-12-66
12.6-5	Sputter Deposition Equipment	MCTL-12-85
17.4-2	Stateful Packet Inspection Technology	MCTL-17-74
18.3-3	Subsystem Apertures	MCTL-18-30
12.1-2	Superplastic Forming/Diffusion Bonding (SPF/DB)	MCTL-12-10
5.2-5	Surface Acoustic Wave (SAW)	MCTL-5-25
5.2-8	Swept Frequency Acoustic Interferometry (SFAI)	MCTL-5-28
17.1-1	Symmetric Key Cryptographic Technology	MCTL-17-21
12.6-12	Technology for Antireflection Optical Coatings for Guidance Systems	MCTL-12-92
12.6-13	Technology for Bandpass Coatings for Sensors	MCTL-12-93
12.6-8	Technology for Corrosion and High-Temperature Protection Coatings for Engine Parts	MCTL-12-88
12.6-10	Technology for Increased-Wear Coatings for Domes and Missile	MCTL-12-90

12.6-9	Technology for Increased-Wear Coatings for Engines	MCTL-12-89
12.6-11	Technology for Wear-Resistance Coatings and Surface Modification for Bearings	MCTL-12-91
18.1-8	Test and Inspection Equipment	MCTL-18-12
12.6-6	Thermal Spray Equipment	MCTL-12-86
16.5-1	Time-Distribution Systems	MCTL-16-83
12.5-3	Turning Machine With Two or More Axes for Removing or Cutting Metals, Ceramics, or Composites	MCTL-12-59
12.5-4	Ultra-Precision Machine Tools: Single-Point Diamond Turning (SPDT) Machines Fly-Cutting Machines, and Microgrinders	MCTL-12-60
12.4-2	Ultrasound Nondestructive Testing	MCTL-12-50
16.4-9	Underwater Electric Field Sensors	MCTL-16-75
12.1-4	Vacuum or Controlled-Atmosphere Metallurgical Melting and Casting Furnaces	MCTL-12-12
12.1-3	Vacuum or Controlled-Environment Induction Furnaces	MCTL-12-11
18.1-6	Visual Signature Reduction	MCTL-18-11
18.3-6	Weapons Integration	MCTL-18-32
18.2-1	Wideband Radar	MCTL-18-21