17.1. Cryptographic Fundamentals

Objective

17.1.1. Agencies use cryptographic products, algorithms and protocols that are approved by the GCSB and are implemented in accordance with this guidance.

Context

Scope

17.1.2. This section covers information on the fundamentals of cryptography including the use of encryption to protect data at rest and in transit. Detailed information on algorithms and protocols approved to protect classified information can be found in Section 17.2 - Approved Cryptographic Algorithms and Section 17.3 - Approved Cryptographic Protocols.

Purpose of cryptography

17.1.3. Cryptography is primarily used to support:

- Confidentiality – protecting against the risk of information being disclosed to an unauthorised person;
- Authentication – ensuring a person or entity is who they claim to be;
- Integrity – ensuring information has not been compromised, either deliberately or accidentally; and
- Non-repudiation – proving who (or what) performed an action.

17.1.4. Cryptography is an important control for data protection. The encryption selected may change depending on the classification of the data. It is important to note that classification, in itself, provides no protection but is merely a labelling mechanism to indicate the degree of protection and care required in handling that data.

17.1.5. Cryptography is frequently used in the establishment of secure connectivity (e.g. IPSec VPNs) and in trust frameworks such as those supported by Public Key Infrastructure (PKI).

17.1.6. With the increases in speed and computing power and the cost reductions of modern computing, older cryptographic algorithms are increasingly vulnerable. It is vital that recommendations and controls in the NZISM are followed.

17.1.7. Mitigation of the risks when using older cryptographic algorithms, often takes the form of increased key lengths. Agencies should also note the increasing threat posed by the evolution and development of quantum computing (see 17.1.19 - Quantum Computing and Encryption).

Encryption

17.1.8. Encryption is the process of converting plain (readable) text to an unintelligible form (cipher text). The term encryption is often used synonymously with cryptography.

17.1.9. The use of approved encryption will generally reduce the likelihood of an unauthorised party gaining access to the information contained within the encrypted data.

17.1.10. When data is at rest, encryption can be used to reduce the physical protection and handling requirements of media or systems. This does not change the classification of the underlying data system or equipment.

17.1.11. Care needs to be taken with encryption systems that do not encrypt the entire media content to ensure that either all of the classified data is encrypted or that the media is handled in accordance with the highest classification of the unencrypted data.

17.1.12. Encryption of data in transit can be used to provide protection for information being communicated over insecure media and hence reduce the security requirements of the communication process.

17.1.13. It is important to note that when agencies use encryption for data at rest or in transit, they are **not** reducing the **classification** of the information. When encryption is used the potential risk of disclosure of the information is reduced.

17.1.14. As the classification of the information **does not** change when encrypted, agencies cannot use lowered storage, physical transfer or security requirements as a baseline to further lower requirements with an additional cryptographic product.

17.1.15. In general terms, the level of assurance of specific encryption protocols and algorithms is defined in terms of Common Criteria, Protection Profiles or, in some cases, approved cryptographic evaluations. It is important to note that evaluations of cryptographic protocols and algorithms are **NOT** universally conducted when security products are evaluated, relying rather on previous approved evaluations of cryptographic protocols and algorithms.

Risk Assessments

17.1.16. Encryption algorithms apply data transformations that are designed to be difficult to reverse by unauthorised users. Today's software will usually provide several algorithmic options, but may include some older algorithms provided for backward compatibility with older (legacy) systems. In many cases the older algorithms are deprecated, are considered time-expired and are not fit for purpose in modern systems. Deprecated algorithms should not be used.

17.1.17. In all cases a comprehensive risk assessment should be undertaken before configurations are selected. Some general principles to be considered are:

- Cryptographic strength is determined by a combination of the encryption algorithm being used, the encryption protocol and the key length. Longer keys generally provide increased encryption strength over shorter keys when using the same encryption algorithm;
- Asymmetric cryptographic algorithms are slower than symmetric cryptographic algorithms at an equivalent cryptographic strength;
- Asymmetric cryptographic algorithms are recommended for the exchange of symmetric cryptographic keys when they are needed to be shared across communication channels;
- Encrypted data cannot usually be compressed, but compressed data can be encrypted. Data should be compressed before encryption;
- Encryption keys have the same requirements for handling and storage as the unencrypted data they are being used to protect;
- Any risk assessment should include consideration of key management – refer to section 17.9 Key Management.

17.1.18. It is important to note that the NZISM prescribes approved algorithms and protocols and users must select combinations from these lists.

Quantum Computing and Encryption

17.1.19. Developments in quantum computing have highlighted threats to classical cryptography whereby a quantum computing, can undermine all of the widely used public key algorithms used for key establishment and digital signatures. While this may be not an immediate issue, quantum developments are likely to undermine the effectiveness of encryption being used today to protect confidentiality of information.

17.1.20. A further implication is that historical and archived data protected by encryption may be at risk.

17.1.21. It is generally accepted that symmetric encryption, with sufficiently long keys, will remain quantum resistant in the short term but that quantum resistant replacements for digital signature and key establishment algorithms will be required in the near future.

17.1.22. In the longer term, quantum resistant algorithms are expected to be developed, standardised and approved for use. Until such time, however, agencies should be positioning themselves to be ready to migrate to a "post-quantum encryption" environment.

17.1.23. As it is now recognised that agencies will need to undertake future migration activities related to post-quantum encryption, it is no longer specifically advised to invest in migration from RSA to ECC-based algorithms if that has not already taken place. Emphasis should instead be placed on ensuring minimum key lengths specified in the NZISM are adhered to.

Transitioning Cryptographic Algorithms and Protocols

17.1.24. It is important to use algorithms that adequately protect sensitive information. It is also important to recognise that all cryptographic algorithms and protocols have a finite life. Challenges are posed by new cryptanalysis techniques and methods, the increasing power of classical computing technology, and the continuing work on the development of quantum computers. In addition, there is an active field of work that continuously seeks to compromise algorithms and protocols currently in use.

17.1.25. Planning for changes in the use of cryptography because of algorithm breaks, the availability of more powerful computing techniques or new technologies is an important consideration for agencies. Awareness of retirement or deprecation of algorithms and associated protocols is essential.

RSA

17.1.26. RSA was announced in 1976 and is now over 45 years old. Several flaws and attacks have been identified since creation, each of which required specific mitigations, careful implementation and management. Unfortunately there is ample evidence that implementers continue to have difficulties in securely implementing, using and managing RSA.

17.1.27. To counter identified threats from shorter RSA key lengths, longer key lengths have been specified in the NZISM since 2010. Minimum key lengths have been subsequently increased over time.

17.1.28. For a number of years there had been several indicators that RSA was likely to be deprecated by the cryptographic community and standards bodies. For example, TLS 1.3 has deprecated the use of RSA for key exchange in favour of elliptic curve cryptography, but RSA is still supported for digital signatures in the current standard. Previous guidance from NIST was also indicative of the impending deprecation of RSA. However, subsequent guidance no longer recommends moving from RSA to elliptic curve if that has not already been done.

17.1.29. Therefore, while RSA is not fully deprecated in the NZISM, it is approved ONLY for a limited set of uses as described in Section 17.2 – Approved Cryptographic Algorithms.

Product specific cryptographic requirements

17.1.30. This section provides requirements for the use of cryptography to protect classified information. Requirements, in addition to those in this Manual, can exist in consumer guides for products once they have completed an approved evaluation. Vendor specifications supplement this manual and where conflict in controls occurs the product specific requirements take precedence. Any policy or compliance conflicts are to be incorporated into the risk assessment.

Exceptions for using cryptographic products

17.1.31. Where Agencies implement a product that uses an Approved Cryptographic Algorithm or Approved Cryptographic Protocol to provide protection of unclassified data at rest or in transit, that product does not require a separate, approved evaluation. Correct implementation of the cryptographic protocol is fundamental to the proper operation of the Approved Cryptographic Algorithm or Approved Cryptographic Protocol and is part of the checking conducted during system certification.

Federal Information Processing Standard 140

17.1.32. FIPS 140 is a United States standard for the evaluation and validation of both hardware and software cryptographic modules.

17.1.33. FIPS 140 is in its third iteration and is formally referred to as FIPS 140-3. This section refers to the standard as FIPS 140 but this should be considered to encompass FIPS 140-1, FIPS 140-2 and FIPS 140-3.

17.1.34. FIPS 140 is not a substitute for an approved evaluation of a product with cryptographic functionality. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.

17.1.35. Cryptographic evaluations of products will normally be conducted by an approved agency. Where a product's cryptographic functionality has been validated under FIPS 140, the GCSB can, at its discretion, and in consultation with the vendor, reduce the scope of a cryptographic evaluation.

New Zealand National Policy for High Assurance Cryptographic Equipment and Key Management

17.1.36. The New Zealand National Standard for High Assurance Cryptographic Equipment (HACE) and related key management is contained in the **New Zealand Communications Security Policy No. 301 – Safeguarding of Communications Security (COMSEC) Material**. This prescribes national doctrine for the safeguarding of COMSEC materials. New Zealand Communications Security Policy No. 301 – Safeguarding of Communications Security (COMSEC) Material, replaces New Zealand Communications Security Standard No. 300 – Control of COMSEC Material which is now withdrawn. Note NZCSP 301 is a RESTRICTED document.

Protection of RESTRICTED/SENSITIVE information in transit over public systems

17.1.37. The physical requirements for protection of information classified RESTRICTED/SENSITIVE are provided by the classification system and PSR guidance.

17.1.38. Where such information is generated and held on information systems (any computer device, including laptops, mobile phones, tablets, desktop and networked systems), the requirements of the NZISM apply. Of particular note is the requirement to encrypt RESTRICTED/SENSITIVE data when in transit over public systems, including any Internet connection, public network or any other network NOT directly controlled by the agency.

Encryption and Key Management

17.1.39. Direct agency control is described as the immediate and continuous physical and logical control, responsibility for, protection and operation of agency information systems and data (see 2.2.4).

17.1.40. Indirect agency control is described as when information is not under the direct control of the agency, this may be through outsourcing, ICT management or services, third party facilities such as data centre co-locations, or consumption of cloud services (see 2.2.5 – 2.2.7).

17.1.41. Encryption can be used to protect information not under the direct control of the agency.

17.1.42. The use of encryption (including data encryption, use of a VPN or any other form of protection using cryptography) requires cryptographic key management and the retention of control of both keys and key management processes.

17.1.43. Where agencies make use of VPNs or other forms of network connectivity that protect data in transit, the control and management of the cryptographic key is fundamental to the integrity and confidentiality of the encrypted data.

17.1.44. If encryption keys are compromised, then any authentication and encryption mechanisms that rely on those keys, no matter how robust or comprehensive, are futile.

17.1.45. If encryption keys are lost, damaged, or fail then access to data encrypted using those keys will also be lost. If control of encryption keys is lost, then those keys should be considered to be compromised and must be replaced or superseded urgently.

17.1.46. The selection of the cryptographic protocol and algorithm is described in this chapter and specified in 17.1.55.C.02. It is essential that agencies select and use only approved cryptographic algorithms and protocols (see section 17.2 – Approved Cryptographic Protocols) and apply the cryptographic key management requirements of the NZISM (see section 17.9 - Key Management).

VPN connection Security

17.1.47. The types of encryption, protocols, and cryptographic algorithms applied in the establishment and maintenance of a VPN connection are fundamental to the security and integrity of the connection.

17.1.48. Key aspects of VPN security include:

- The encryption algorithm and protocol used;
- Cryptographic key length;
- The authentication protocol
- Key Exchange protocol;
- Selection of VPN protocol;
- VPN monitoring and a “kill switch” to deter IP leakage and snooping;
- Cryptographic key management.

17.1.49. It is important to understand that a variety of VPN services can use a variety of mechanisms. Agencies should also consider the service provider’s use of hash authentication, perfect forward secrecy, and the difference in encryption settings on both the data and control channels. The NZISM specifies the cryptographic protocols and cryptographic algorithms that should be used (see sections 17.2 – Approved Cryptographic Algorithms and 17.3 – Approved Cryptographic Protocols) and agencies must ensure the VPN connection conforms with these requirements.

References

17.1.50. Further references can be found at:

Reference	Title	Publisher	Source
NZCSP 301	New Zealand Communications Security Policy 301 - Safeguarding of Communications Security (COMSEC) Material, NZCSP 301 replaces NZCSS 300	GCSB	Contact the GCSB RESTRICTED document available on application to authorised personnel
PSR	Handling requirements for protectively marked information and equipment	NZ Government Protective Security Requirements	https://protectivesecurity.govt.nz/classification-system/how-to-protect
	Transport Layer Security (tls)	IETF	https://datatracker.ietf.org/wg/tls/documents/
	TLS 1.3	IETF	https://www.ietf.org/blog/tls13/
	The Transport Layer Security (TLS) Protocol Version 1.3 March 2018	IETF	https://tlswg.github.io/tls13-spec/draft-ietf-tls-tls13.html
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	IETF	https://tools.ietf.org/html/rfc2407
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	IETF	https://tools.ietf.org/html/rfc2408
RFC 2409	The Internet Key Exchange (IKE)	IETF	https://tools.ietf.org/html/rfc2409
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3	IETF	https://datatracker.ietf.org/doc/html/rfc8446
RFC 8996	Deprecating TLS 1.0 and TLS 1.1 – Best Current Practise	IETF	https://datatracker.ietf.org/doc/html/rfc8996
FIPS 140-3 (March 2019)	Security Requirements for Cryptographic Modules	NIST	https://csrc.nist.gov/publications/detail/fips/140/3/final
FIPS 186-4 (July 2013)	Digital Signature Standard (DSS)	NIST	https://csrc.nist.gov/publications/detail/fips/186/4/draft
FIPS 186-5 (Draft, January 2020)	Digital Signature Standard (DSS)	NIST	https://csrc.nist.gov/publications/detail/fips/186/5/draft
FIPS 197 (November 2001)	Advanced Encryption Standard (AES) (This publication is under review)	NIST	https://csrc.nist.gov/publications/detail/fips/197/final
NIST SP 800-56A Rev. 3 (April 2018)	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography	NIST	https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
NIST SP 800-56B Rev. 2 (March 2019)	Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography	NIST	https://csrc.nist.gov/publications/detail/sp/800-56b/rev-2/final
NIST SP 800-131A Rev. 2 (March 2019)	Transitioning the Use of Cryptographic Algorithms and Key Lengths	NIST	https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final
NIST SP 800-57 Part 1 Rev. 5 (May 2020)	Recommendation for Key Management: Part 1 – General	NIST	https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
NIST SP 800-57 Part 2 Rev. 1 (May 2019)	Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations	NIST	https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final
NIST SP 800-57 Part 3 Rev. 1 (January 2015)	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	NIST	https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

NIST 800-175A (August 2016)	Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf [PDF, 470 KB]
NIST SP 800-175B Rev. 1 (March 2020)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	NIST	https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final
CNSS Policy 15 (October 2016)	Use of Public Standards for Secure Information Sharing	Committee on National Security Systems (CNSS)	https://www.cnss.gov/CNSS/issuances/Policies.cfm
NSA Quantum Computing FAQ (August 2021)	Quantum Computing and Post-Quantum Cryptography	NSA	https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.pdf [PDF, 258 KB]
VPNCP Version 3.1 March 2015	Virtual Private Network Capability Package Version 3.1 March 2015	NSA	https://www.nsa.gov/ia/_files/VPN_CP_3_1.pdf
	Suite B Implementer's Guide to NIST SP 800-56A, July 28, 2009	NSA	http://docplayer.net/204368-Suite-b-implementer-s-guide-to-nist-sp-800-56a-july-28-2009.html
EPC342-08 Version 7.0 4 November 2017	Guidelines on Cryptographic Algorithms Usage and Key Management	European Payments Council	https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/guidelines-cryptographic-algorithms-usage-and-key-management
	Choose an Encryption Algorithm	Microsoft	https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-2017
	Transport Layer Protection Cheat Sheet	OWASP	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
	Guide to Cryptography	OWASP	https://www.owasp.org/index.php/Guide_to_Cryptography
	New Directions in Cryptography - IEEE Transactions on Information Theory Vol IT22 November 1976	Diffie, Hellman	https://ee.stanford.edu/~hellman/publications/24.pdf [PDF, 2.1 MB]

Rationale & Controls

Using cryptographic products

17.1.51.R.01. **Rationale**

No real-world product can ever be guaranteed to be free of vulnerabilities. The best that can be done is to increase the level of assurance in a product to a point that represents satisfactory risk management.

17.1.51.R.02. **Rationale**

Refer to Chapter 12 - Product Security for a discussion on product evaluation and assurance.

17.1.51.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:2070]**

Agencies using cryptographic functionality within a product to protect the confidentiality, authentication, non-repudiation or integrity of information, MUST ensure that the product has completed a cryptographic evaluation recognised by the GCSB.

Data recovery

17.1.52.R.01. **Rationale**

It is important for continuity and operational stability that cryptographic products provide a means of data recovery to allow for the recovery of data in circumstances such as where the encryption key is unavailable due to loss, damage or failure. This includes production, storage, backup and virtual systems. This is sometimes described as "key escrow".

17.1.52.C.01.

Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must [CID:2074]

Cryptographic products MUST provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

17.1.52.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2075]

Cryptographic products SHOULD provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

Reducing storage and physical transfer requirements

17.1.53.R.01. **Rationale**

When encryption is applied to storage media (whether portable or residing within IT equipment or systems) it provides an additional layer of defence. Whilst such measures do not reduce or alter the classification of the information itself, physical storage, handling and transfer requirements may be reduced to those of a lesser classification for the media or equipment (but not the data itself).

17.1.53.R.02. **Rationale**

Approved Cryptographic Algorithms are discussed in section 17.2.

17.1.53.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2079]

Encryption used to reduce storage or physical handling protection requirements MUST be an approved cryptographic algorithm in an EAL2 (or higher) encryption product.

17.1.53.C.02. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:2080]

If an agency wishes to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they MUST encrypt the classified information using High Assurance Cryptographic Equipment (HACE). It is important to note that the classification of the information itself remains unchanged.

17.1.53.C.03. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2081]

If an agency wishes to use encryption to reduce the storage, handling or physical transfer requirements for IT equipment or media that contains classified information, they MUST use:

- full disk encryption; or
- partial disk encryption where the access control will allow writing ONLY to the encrypted partition holding the classified information.

17.1.53.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2082]

If an agency wishes to use encryption to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they SHOULD use:

- full disk encryption; or
- partial disk encryption where the access control will allow writing ONLY to the encrypted partition holding the classified information.

Encrypting NZEO information at rest

17.1.54.R.01. **Rationale**

NZEO information is particularly sensitive and it requires additional protection in the form of encryption, when at rest. This includes production, storage, backup and virtual systems.

17.1.54.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2085]

Agencies MUST use an Approved Cryptographic Algorithm to protect NZEO information when at rest on a system.

Information and Systems Protection

17.1.55.R.01. **Rationale**

When encryption is applied to information being communicated over networks, less assurance is required for the physical protection of the communications infrastructure. In some cases, no physical security can be applied to the communications infrastructure such as public infrastructure, the Internet or non-agency controlled infrastructure. In other cases no direct assurance can be obtained and reliance is placed on third party reviews and reporting. In such cases encryption of information is the only practical mechanism to provide sufficient assurance that the agency information systems are adequately protected.

17.1.55.R.02.

Rationale

Data duplication for backups or data replication aggregates agency information and will generally increase the impact of an unauthorised party gaining access to, or otherwise compromising, the data. This includes where outsourced services are undertaken.

17.1.55.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2089]

Agencies MUST use HACE if they wish to communicate or pass information over UNCLASSIFIED, insecure or unprotected networks.

17.1.55.C.02. **Control System Classifications(s): Restricted/Sensitive; Compliance: Must** [CID:2090]

Information or systems classified RESTRICTED or SENSITIVE MUST be encrypted with an Approved Cryptographic Algorithm and Protocol if information is transmitted or systems are communicating over insecure or unprotected networks, such as the Internet, public networks or non-agency controlled networks.

17.1.55.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2091]

Agencies MUST encrypt aggregated agency data using an approved algorithm and protocol over insecure or unprotected networks such as the Internet, public infrastructure or non-agency controlled networks when the compromise of the aggregated data would present a significant impact to the agency.

17.1.55.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2092]

Agencies SHOULD encrypt agency data using an approved algorithm and protocol if they wish to communicate over insecure or unprotected networks such as the Internet, public networks or non-agency controlled networks.

IT equipment using Encryption

17.1.56.R.01. **Rationale**

In general terms, when IT equipment employing encryption functionality is turned on and authenticated all information becomes accessible to the system user. At such a time the IT equipment will need to be handled in accordance with the highest classification of information on the system. Special technology architectures and implementations exist where accessibility continues to be limited when first powered on. Agencies should consult the GCSB for further advice on special architectures and implementations.

17.1.56.R.02. **Rationale**

The classification of the equipment when powered off will depend on the equipment type, cryptographic algorithms and protocols used and whether cryptographic key has been removed. Agencies should consult the GCSB for further advice on treatment of specific software, systems and IT equipment.

17.1.56.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2096]

When IT equipment storing encrypted information is turned on and authenticated, it MUST be treated as per the original classification of the information.

17.1.56.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2097]

Agencies MUST consult the GCSB for further advice on the powered off status and treatment of specific software, systems and IT equipment.

Encrypting NZEO information in transit

17.1.57.R.01. **Rationale**

NZEO information is particularly sensitive and requires additional protection. It must be encrypted when in transit.

17.1.57.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2100]

In addition to any encryption already in place for communication mediums, agencies MUST use an Approved Cryptographic Protocol and Algorithm to protect NZEO information when in transit.

Key Refresh and Retirement

17.1.58.R.01. **Rationale**

All cryptographic keys have a limited useful life after which the key should be replaced or retired. Typically the useful life of the cryptographic key (cryptoperiod) is use, product and situation dependant. Product guidance is the best source of information on establishing cryptoperiods for individual products. A more practical control is the use of data, disk or volume encryption where key changes are more easily managed. Selection of cryptoperiods should be based on a risk assessment. Refer also to section 17.9 – Key Management.

17.1.58.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2103]

Agencies SHOULD establish cryptoperiods for all keys and cryptographic implementations in their systems and operations.

17.1.58.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2104]

Agencies SHOULD use risk assessment techniques and guidance to establish cryptoperiods.

17.1.58.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2105]

Agencies using HACE MUST consult the GCSB for key management requirements.