Comments Received on the Second Review of SP 800-131 (Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths)

Date: 7/12/10 6:58 AM
From: "King II, Lovell" <KingL@state.gov>

The U.S. Department of State concurs with the proposed draft without comments.

Date: 7/13/10 12:24 PM
From: "Popa, Claudia L." <Claudia.Popa@cse-cst.gc.ca>

Section 3 Digital Signatures

The CMVP Implementation Guidance *A.6 CAVP Requirements for Vendor Affirmation of FIPS 186-3 Digital Signature Standard* still allows for the use of FIPS 186-2 Digital Signature Standard, January 2000 in FIPS mode of operation.

SP 80-131 document refers only to FIPS 186-3 Digital Signature Standard, 2009.

Section 4 Random Number Generation

It is not clear why this sentence:

"Note that in 2005, a revision of [X9.62] was approved that includes the HMAC_DRBG specified in [SP 800-90], and does not include the RNGs in the1998 version."

was included.

The CAVP testing covers the ANS X9.62-1998 and not the 2005 version. Is the HMAC_DRBG from X9.62 the same as the HMAC_DRBG specification from SP 800-90?

Section 5 Key Agreement Using Diffie-Hellman and MQV

The CMVP Implementation Guidance *D.2 Acceptable Key Establishment Protocols* specifies the 5 scenarios that are currently accepted for use in the FIPS mode of operation.

I copy below the information from this implementation guidance:

"In lieu of a transition plan for **key agreement schemes**, there are currently five scenarios that are valid and allowed in an Approved FIPS mode of operation. The first four apply when a key is established (i.e. key agreement) and the fifth when only the DLC primitive is implemented (e.g. in a software toolkit):

1. CAVP KAS Certificate

2. Vendor Affirmation per IG D.1 – Transition for submitting CST Laboratory test reports ended March 24, 2009

3. non-Approved but allowed per this IG (DLC primitive as defined in SP 800-56A with a KDF specified in this IG)

4. non-Approved but allowed legacy implementation

5. non-Approved DLC primitive only from SP 800-56A. "

I don’t believe that the information for *Non-56A-compliant DH and MQV schemes* in SP 800-131 covers item 4 and 5 from the list above. If these two scenarios will not be addressed by SP 800-131 they should be addressed in the new document, specified in the Note to the Reviewers, the document specific for the FIPS 140-2 validation process.

Date: 7/14/10 10:54 AM

From: "Olson, Robert (Al) (CDC/OCOO/OD)" <hiy8@cdc.gov> wrote:

Greetings.

CDC has no comments regarding the Draft NIST SP 800-131. Thank you for the opportunity to review and comment.

Date: 7/15/10 8:26 AM

From: "Jennifer.Evans@fms.treas.gov" <Jennifer.Evans@fms.treas.gov> wrote:

The revised SP 800-131 allows more time for agencies to upgrade their Windows OS, in support of SHA2 signatures, but the dates for elimination of SHA1 seem too closely connected to when Windows XP is officially sunsetted. Some timing clarification may be appropriate.

Date: 7/15/10 10:05 AM
From: "Anthony Busciglio (abuscigl)" <abuscigl@cisco.com>

Thank you for the opportunity to review and comment on the second draft of SP 800-131. As always, Cisco appreciates NIST's openness and willingness to engage with industry to develop standards and policies which are both technically sound and feasible to implement.

The following list includes the comments identified during Cisco's review of the second draft of SP 800-131,

1. Thank you for the update to SP 800-131. It is very evident that each submitted comment was considered. The resulting document has laid out a very reasonable transition plan that will allow industry to smoothly transition to the higher security strengths.

2. It is Cisco's opinion that there will continue to be several use cases for which SHA-1 based signatures would continue to provide adequate security for the foreseeable future. These short duration signatures, such as those used during the SSL/TLS handshake, only exist for a matter of seconds and do not provide an attacker ample opportunity for compromise. Not allowing the continued use of short duration SHA-1 based signatures will prevent the Federal Government from leveraging any of a number of secure protocols. It is our recommendation that SHA-1 based short duration signature be explicitly allowed.

3. It is unclear how SP 800-131 applies to RSA-3072 since it is not SP 800-56B compliant. Since, it provides greater then 112-bits of security it would be appropriate for NIST to clarify that it will continue to be allowed.

4. A more clear definition of deprecated in the document would be appreciated. For example, if a specific algorithm is deprecated, can it continue to be FIPS validated?

5. What does a company/user need to do in term of accepting the risk associated with deprecated algorithms? Is there an official procedure that a company and user will need to go through?

Date: 7/16/10 2:22 AM
From: "Tabram, Nicky" <Nicky.Tabram@thales-esecurity.com>

We recognize and appreciate the effort that has gone into this new version which allows for a staged transition of devices and deployments. We believe that the new concessions (c.f. "legacy use") will actually improve security during the transition period. Our comments on the draft are presented in the table to follow.

Please contact nicky.tabram@thales-esecurity.com for further correspondence regarding this document.

No.	Type	Section	Comment
1.	General	Note to reviewers/ Front matter	There appears to be a contradiction in a couple of places regarding the precedence of SP 800-131 versus other published standards such as SP 800-57. Note to Reviewers, item 7 states: "Note that many of the NIST publications (e.g., FIPS 186-3) currently include key lengths that will be phased out as specified in SP 800-131. At this time there is no intention of immediately revising those documents to exclude those key lengths. It is assumed that SP 800-131, and eventually the revised SP 800-57, will serve this purpose." However, "Authority" on page iii, states: "Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official."

2.	General	Note to reviewers/ General	We understand that issues related to FIPS 140-2/3 CMVP and CAVP validation are now outside the remit of SP 800-131. While this change is in itself a reasonable move, as developers we would really appreciate a speedy resolution of the recommendation's application to FIPS validation. In particular, we have concerns about how an algorithm regarded as "legacy" or "restricted" will affect existing certificates and its use in FIPS mode. Obviously, accommodating appropriate FIPS status indication in older modules implies a change in a device that cannot be done without affecting its FIPS validation, necessitating revalidation effort and cost whilst bringing little actual security benefit. We therefore would very much like to know at the earliest opportunity exactly how CMVP/CAVP plan to reclassify existing FIPS validation certificates at each landmark in the roadmap, and the plan's implication (if any) on developers. For new modules, does the statement "user must accept some risk" combined with the details on "restricted" algorithms mean that the CAVP will not be modified this time round? This is to say that will two-key TDES and other '"legacy" or "restricted" algorithms be fully allowed in FIPS mode, with the end user fully responsible for choosing rather than the vendor or test house?
3.	Editorial	ToC	Some headings are hyperlinked but some not. Preferably they should all be hyperlinks for ease of navigation.
4.	Editorial/ technical	Several places	In cases where timelines are provided for restrictions (e.g. signature generation with 80 bit keys "Deprecated 2011-2013") it would be good to explicitly state in the summary table what happens after that timeframe (e.g. "Shall not be used after 2013"). As it is the table provides an incomplete reflection of the information in the body text. Similarly the acceptability of DH Key Agreement for "≥112-bit non-SP800-56A compliant" (FF and EC) is not currently defined between 2011 and 2013.
5.	Technical	5	Table 4, Non-56A compliant EC DH/MQV Is "$\|n\| \geq 160$" meant to read "$160 \leq \|n\| \leq 223$"?

6.	General	8, A.1	Payments uses of two-key TDES not explicitly mentioned, although during the last round of comments there were some rumours of an exemption from the two-key TDES withdrawal for payments algorithms. Is this now expected to be covered by the more general advice (including the 2^{20} block restriction) with the expectation that the payment industry come to a solution by 2015? In particular, in section 8 the document clearly states: "Two-key Triple DES shall not be used to derive keying material after December 31, 2015". This means that payments algorithms will definitely be unacceptable for a FIPS accreditation after 2015. While we appreciate that payments security is not really the business of FIPS it will aid our planning greatly if we could understand whether there is explicit consideration of commercial use of FIPS accreditations. The above comment may be better understood in the context of Thales's original comment 2.5 from the last review round: "2.5 Allowance of Sub-112-Bit Algorithms in Specific Applications SHA-1 is still allowed to be implemented in cryptographic modules for non-signature uses, so an SP800-131 compliant module running in a FIPS 140-2 level 3 mode will contain an active implementation of SHA-1. Similarly, we understand from informal discussions with NIST that two-key TDES keys are allowed for payments applications but not for generic data encipherment so an SP800-131 compliant module running in a FIPS level 3 mode can also contain an active two-key TDES implementation. How will the CMVP assess compliance to level 3 when these algorithms are present? Will the module have to contain active code that restricts usage to an explicit 'white list' of higher-level applications, or an explicit black list, or nothing, or something else?"
7.	Editorial	10	First paragraph: reads "… The authenticated encryption modes in [SP 800-38] are not discussed..." The reference is ambiguous. It would be better to explicitly state CCM [SP 800-38C] and GCM and GMAC [SP 800-38D].
8.	Content	Appendix A	We fully agree with the analysis and conclusions on the uses of SHA-1, however we wonder why the rationale is not provided with the same level of appendix text treatment as the other decisions.
9.			

10.	Content	Appendix B.1	Appendix B.1 (on the security of information wrapped with two-key TDES) misses another important aspect of risk mitigation. It is unfortunately common to find cryptographic systems "in the wild" that operate under the false assumption that encryption provides confidentiality ***and integrity***, particularly when the underlying plaintext is strongly formatted. While this is more the domain of SP 800-130 than -131, it would be useful to point out in this educational appendix that if the encryption key is compromised then an attacker can trivially substitute his own plaintext, with clear bad consequences. We recommend that this section should remind readers that along with re- or super-encryption, their risk profile mitigations should take account of separate strong integrity protection.

Date: 7/16/10 5:02 AM
From: "Takashi Mukasa" <ta-mukasa@kddi.com>

We support the Draft Recommendation SP800-131, as it proposes the 1024bit RSA key and SHA-1 are "deprecated" from 2011 through 2013.

The 1024bit RSA key and/or SHA-1 are still widely used at a lot of the embedded devices such as mobile phones in our society. At least several-year-period will be required for the entire transition of key length and/or algorithms to the new ones at those devices. We thus consider that the use of 1024bit RSA key and SHA-1 should remain within the options in any Recommendation for a few more years, until at least 2013.

Date: 7/16/10 9:07 PM
From: "Vijay Bharadwaj" <Vijay.Bharadwaj@microsoft.com> wrote:

Thank you for the opportunity to review this document. We support the goals of the crypto transition, and appreciate NIST's efforts in making this as smooth as possible. Our feedback on this draft follows:

1. It is good that NIST is recognizing the need for giving different types of guidance to US Government agencies, who are customers of encryption, and to vendors. The present draft does indicate that information targeted at vendors, including how the transition will affect FIPS validations, is forthcoming. We would like to emphasize that having this information available well in advance of the transition (ideally at the same time as SP800-131 is released) is critical so that vendors can prepare for the transition as well.

2. In general, the use of the term "Approved" to mean "FIPS-approved or NIST-recommended" is confusing, especially since FIPS 140-2 and related publications often use "Approved" to mean simply "FIPS-approved" when discussing security functions. More consistency around this terminology would be appreciated. We would recommend creating a separate term to indicate "FIPS-approved or NIST-recommended", since "Approved" already has a set meaning within the community of FIPS vendors and customers.

3. The draft designates a phased transition for some algorithms, with statements such as "deprecated from 2011 through 2013". However, it is not always consistent about explicitly stating that these algorithms shall not be used after this additional interval. For instance, Section 4 doesn't state what should happen to the FIPS 186-2 RNG after 2015, and none of the tables point out that certain algorithms shall not be used after a certain end date.

4. To add to the previous point, it would be useful to define a term (such as "Disallowed") to indicate algorithms that shall not be used, and to have explicit statements in the tables and text where an algorithm will be Disallowed after a certain date.

5. The draft gives no guidance on block cipher modes. It would be good to add this, even if only to indicate that there are no transition issues with the currently Approved cipher modes.

6. Our experience has been that in general, recommendations at the algorithm level tend to be too low-level for most customers. Such recommendations are much more helpful when accompanied with guidance that illustrates how to apply them to common protocols (e.g. how to use this guidance in choosing acceptable TLS ciphersuites). It would be useful to supplement SP800-131 with such guidance or relevant pointers to such guidance in related documents such as SP 800-57.

7. As a corollary to the above point, it seems that some of the recommendations in the draft are not in tune with the current reality of protocol standardization. One particularly important example of this is the phasing out of non-SP800-56B RSA key transport schemes after 2013. As we (and others) have pointed out earlier, use of PKCS#1v1.5 is widely prevalent in protocols and in many cases there is no SP800-56B-compliant option defined in the protocol for customers to transition to. We believe that this deadline should be relaxed, until such options have been established. Similar comments apply to the KDF section.

8. Finally, SHA-224 has not seen wide adoption in industry or in government standards such as Suite B, and from an implementation perspective it has the same resource requirements as SHA-256. With its security strength of 112 bits, this algorithm will likely have to be phased out in the next crypto transition. We suggest deprecating this algorithm now, so that vendors can simplify their test matrices and focus on more prevalent algorithms.

Date: 7/19/10 10:36 AM
From: "Anthony Busciglio (abuscigl)" <abuscigl@cisco.com

Based on additional review of the SP 800-131 Draft 2 we would like to make the following change to the comments submitted last week.

Please replace comment #2 below with the following comment:

"There are no known weaknesses against the uses of SHA-1 signatures in TLS versions 1.0 and 1.1 (where it is used in the ServerKeyExchange and CertificateVerify messages). Because these versions are prevalent, and TLS version 1.2 has not yet seen wide deployment and is highly unlikely to reach this goal by January, 2011, we suggest that the use of SHA-1 in those TLS messages be explicitly allowed for a time period extending beyond that date. The use of SHA-1 signatures in those messages is different from typical digital signature applications in that both the signer and the verifier provide input to the message being signed, and in that the limited duration of a TLS session limits the time that an attacker could use to attempt to find a collision."

InfoGard Comments

SP 800-131: Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths, June 2010

July 16, 2010

InfoGard appreciates the opportunity to provide further comments to the SP 800-131 document. We are very pleased with the latest revision of the draft. The changes made by the CT Group provide a reasonable path to success for government agencies and the vendors providing solutions.

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
1	Section 1.2.1 and Section 3	The terms "DSA", "ECDSA", and "RSA" are used when discussing FIPS 186-3 algorithms.	Change terminology to "DSA2", "ECDSA2", and "RSA2" when discussing FIPS 186-3 algorithms.	This terminology is consistent with FIPS 140-2 Annex A and the CAVS tool.
2	Section 3	There is no mention of the old DSA, ECDSA, and RSA (i.e., FIPS 186-2).	Assure that this is taken into consideration either in SP 800-131 or in the upcoming FIPS validation process document.	Most modules still use the old DSA, ECDSA, and RSA, so clarity is necessary.
3	Section 5, Table 4	For Non-56A-compliant DH and MQV schemes, the use is "Deprecated after 2013". This is very different from the initial requirement of forcing SP 800-56A by 2013. Is the intent to	Consider enforcing a date for compliance to SP 800-56A (primitives only at least). Perhaps by the end of 2015 or 2017.	The indefinite allowance of untested DH, ECDH, and MQV implementations seems insecure.

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
		indefinitely allow the gray area of "allowed" DH, ECDH, and MQV?		
4	Section 6, Table 6	For Non-56B-compliant Key Transport schemes, the use is "Deprecated after 2013". This is very different from the initial requirement of forcing SP 800-56B by 2013. Is the intent to indefinitely allow the gray area of "allowed" RSA key wrap?	Consider enforcing a date for compliance to SP 800-56B. Perhaps by the end of 2015 or 2017.	The indefinite allowance of untested RSA key transport implementations seems insecure.
5	Section 7, Table 7	All key wrapping schemes from IG D.2 are not addressed (i.e., DLC-based key transport).	Complete this table or modify the key wrapping schemes in IG D.2.	Consistency is essential.
6	Section 10, Table 10	CMAC Verification lists 2-key TDES twice.	Remove 2-key TDES from the second row.	This will fix the error.
7	General	There is a major concern regarding transitioning algorithms defined as "Required" by protocols such as IKE and SSH.	A separate effort needs to be put in place to ensure the release of updated protocol RFCs to align with transition dates.	If revisions are not made to certain protocols RFCs, there will be a contradiction between what algorithms are required by protocols and what algorithms

#	Section, Paragraph, or Page	Comment	Suggested Revisions	Rationale for Revisions
				are allowed by NIST.

Date: 7/16/10 7:30 AM
From: "Benjamin Gittins" <cto@pqs.io> wrote:

1. General Comments

1.1 Timelines

I anticipate a user of draft SP 800-131 may ask three related questions:

1) What date should EVERYBODY STOP generating material with an algorithm?
2) What date should my project PLAN TO STOP generating material with a security rating if I need it to be secure X years into the future?
3) What date should EVERYBODY STOP relying on ciphertext/digests/signatures generated by a given security rating?

To my mind:

1)Question 1 appears to be addressed very clearly.
2)Question 2 is not clear to me in the body of the text.
3)Question 3 is addressed clearly for "deprecated, restricted and legacy" security ratings. However, it is not clear to me what the answer is with regard to "acceptable" security ratings.

I hope aspects of questions 2 and 3 could be clarified throughout the document.

1.2 Considering both Classical and Quantum environments

The document appears to written implicitly within the context of classical computing model. I feel the document would be improved if it explicitly addressed quantum computing attack vectors. See comment 2.2 regarding {page 1, section 1.2.1} below.

See also the following quote from: ECRYPT2, "*Yearly Report on Algorithms and Keysizes*" Deliverable D.SPA.7, Revision 1.0, ECRYPT ICT-2007-216676, July **2009**. Available at http://www.ecrypt.eu.org/documents/D.SPA.7.pdf

> "Both of the fundamental intractability assumptions on integer factoring and discrete logarithms break down if a (large) quantum computer could be built as demonstrated by Shor." - page 25, section 6.4
>
> "Advances have often been done in steps (e.g. the improvement from QS to NFS), and beyond approximately 10 years into the future, the general feeling among ECRYPT2 partners is that recommendations made today should be assigned a rather small confidence level, **perhaps in particular for asymmetric primitives**." - page 31, section 7.3

I anticipate that many Agencies deploying NIST primitives will need to secure data for 10 years and longer. It would be helpful if the document could provide advice, or link to advice, for those organisations requiring long term security when re-evaluating what cryptographic security ratings (and types of primitives) they need.

2. Comments on specific sections in the document

2.1 - Page 1, section 1.1:

"*The appropriate security strength to be used depends on the sensitivity of the data being protected, and needs to be determined by the owner of that data (e.g., a person or an organization).*"

This might be addressed in another NIST standard, however it is it possible to add statements (or links to statements) regarding how to calculate the minimum security levels of a cryptographic system that needs x years security. To clarify what I mean, I provide some straw-man mock-up text below:

"The life cycle of a key is intrinsically linked to the life cycle of the data it protects. That is the durability of all key management and cryptographic operations must at a minimum satisfy the duration of security and integrity required for that datum. For example this may be the term of a contract + 7 years, the natural lifetime of a person + 7 years, long-lived archiving periods, and so on.

The operational life cycle of a key management system, is intrinsically linked to the life cycle of the project it operates with. The operational life cycle of a key management system may or may not exceed the security lifecycle of the data it protects. For example a system may need to remain operational for 50 years, in which case either we select cryptographic primitives that remain secure for either a) the larger of (at least for during the period of it's planned operation) and (security life cycle of the datum) or b) we must explicitly plan and budget for the algorithms used in the system (and all dependent systems) to be upgraded at a given time."

2.2 - Page 1, section 1.2.1:

"The security strength of an algorithm with a particular key length is measured in bits and is, basically, a measure of the difficulty of discovering the key."

The reader may wonder if the key length is rated against classical brute-force attacks or Grover's brute force quantum algorithm?

Would NIST consider adopting a standard terminology in the next revision so that the document is "ready" for describing the security of systems against code-breaking quantum adversaries when they arrive.

Could the document please qualify security ratings "against a classical adversary" in each occurrence where appropriate.

2.3 - Page 2, section 1.2.1

Consider replacing:

"Based on the latest understanding of the state-of-the-art for breaking the cryptographic algorithms, given particular key lengths, the transition to the 112-bit security strength shall be accomplished by 2014, except where specifically indicated." with:

"Based on the latest understanding of the state-of-the-art for breaking the cryptographic algorithms **using classical computing attacks**, *given particular key lengths, the transition to* **a minimum** *112-bit* ***classical*** *security strength shall be accomplished by 2014, except where specifically indicated."*

2.4 - Page 2, section 1.2.2, the table of terms

"Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. Note that as the designated end-date approaches, the level of risk becomes higher. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature)."

Have you considered adding text to state something along the lines of "deprecated security ratings may not be selected by new projects."?

2.5 - Page 2, section 1.2.2, the table of terms.

There does not appear to be an advisory on WHAT new security ratings should be chosen when upgrading from a deprecated, restricted or legacy security rating.

I anticipate that the choice of security rating for new systems (particularly if a system was, or is to be, implemented at just use one security rating) will impact the cost of a cryptographic key management system over it□s planned and actual operational lifetime.

Could we create the term "**preferred**", which might be defined as "**the strongest cryptographic primitive currently approved by NIST**."

That is, when a transition decision is to be made on selecting a security rating, the strongest security rating (**preferred** ciphers) should be used, unless there is a cost-effective case-use argued based on the operational life cycle of the key management cycle.

Maybe we could also include text that says: *"in cases where* ***preferred*** *ciphers are not used operationally today, all software should implement support for preferred security ratings, so the transition is a configuration switch change that does not require implementing new security modules / changing code / changing hardware".*

2.6 - Page 4, section 3:

I quote two portions of text:

"Digital signatures are used to provide assurance of origin authentication and data integrity. These assurances are sometimes extended to provide assurance that a party in a dispute (the signatory) cannot repudiate (i.e., refute) the validity of the signed document; this is commonly known as non-repudiation."

and in the table:

"Digital Signature Verification", ">= 112 bits of security strength", "Acceptable".

The digital signature verification appears to lack an upper bound for 112-bit secure algorithms. For example, it could be read that 112-bit secure, DSA, RSA, EC digital signatures will maintain their non-repudiation properties for 10, 20, 30, 50, 100, 1000 years into the future? Can you provide advice on how long the signature algorithms are anticipated to retain their integrity for?

2.7 - Page 6, section 4:

"In 2007, a new set of RNGs were approved in SP 800-90 [SP 800-90] that provide higher levels of security than the previously-approved RNGs."

Question: Are the new random numbers "more secure" (generate more entropy) than the old ones, or do they simply provider us greater confidence/assurance of being secure?

Question: Are the future security ratings of RNG calculated differently to privacy and integrity operations? If they are, could the document briefly advise how so? That is, how should Agencies evaluate the future security of an RNG over it□s operational life? Should they plan to upgrade RNG every x years to the latest standard due to a perceived weaknesses known today? Is there some notion that cryptographic operations performed by users of the old RNG standard may become insecure in x years?

2.8 - Page 10, appendix b.1

I really liked the detail in this section.

2.8 - Page 10, appendix b.2

"In order for the signed information to continue to be verifiable as valid, both the signed information and the digital signature need to be protected against possible modification (e.g., placed in secure storage) or against modification without detection (e.g., time-stamped and signed with an additional signature)."

Another strategy may be to recommend that applications reliant on legacy primitives perform additional work on validating legacy messages by considering contextual information available to them. Instead of relying purely on the cryptographic mechanism, employ a system of checks-and-balances to ensure that the transaction, when evaluated in context, appears correct...

e.g., isolated modified financial transactions might go unnoticed, but may be identified when considered in the context of other transactions.

You might also consider advising that legacy data could be "tagged" as it flows through the system. That is, in the same way as we might provide a +/- error rating on the precision of a given measurement, we can set a flag to indicate "could be modified in transit", which could facilitate auditing mechanisms if something is found amiss.

Date: 7/16/10 7:30 AM
From: "Benjamin Gittins" <cto@pqs.io> wrote:

I also submit the questions I raised in the Q+A session [at the]IEEE KMS 2010 presentation on draft SP 800-131 as follows.

Question 1:

I found it really interesting with regards to useby a certain date, then please don't use it. In particular with regard to archived data. it seems like at some point, someone is going to have to read all the old data archives and transcode them and dump them out. How do you manage that?

The second part of the question is, is it possible, or have you considered, forcing them, when they do the transcoding, that unfortunatetly you must use the strongest algorithms and key lengths available, because it is going to be a really hard process in 25 years from now to go re-archive and read all that data back and go through the motions again. So maybe it is more cost effective, in the archival process u use the largest nist algorithms/kelengths available at the time.

Question 2:
Thinking not so much in the archive, but in terms of the life-cycle. You are now going through the process of moving people out of the first lifecycle (DES, 2DES), is there text in the document stating, when you transition, it's not just about what is acceptable. When you transition please use the strongest available unless you can provide some really good reason not to. Because i think this will save costs later on.

That is, the choice of algorithm must take into consideration the Anticipated and projected costs of the next transition period TODAY.

Please find an additional question from me:

How do you make sure that data is not 'exposed' during transcoding operation to change key/cipher?

I am aware of at least one paper that talks about using 2 block ciphers in counter mode of operation. This lets one device, operating with a first key, to remove their old keystream and apply a new keystream, while not exposing the original value of the plaintext, that modified ciphertext being provided to the second device that replaces it's keystream with a newer keystream. In this way, if the devices are seperated/compartimentalised/operated by different parties (or HSM), then you reduce the risk of exposure to the plaintext (it is never in the clear).

So we can imagine a "3 key AES" mode of operation which is AES-CTR(K1) xor AES-CTR(K2) xor AES-CTR(K3) for archive purposes. If each of those keys is 256-bits long in length, this might be ideal for secure archiving purposes and mitigating against insider

attacks. This then supports transitioning to "any other stream cipher mode of operation" in the future.

I will try to find the paper which talks about this basic technique and forward it later.