Le NIST vient de publier dans la série "800 Series" le draft d'une "Special Publication" SP 800-131 : "DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes" . Cette publication est intéressante car elle parcourt les différentes primitives cryptographiques en indiquant quelles sont celles qui continueront après 2010 à être valides. Bien entendu non seulement les algorithmes sont précisés, mais aussi les tailles des clés.

Voici l'abstract de ce document, qui en expose les buts:

"At the start of the 21st century, the National Institute of Standards and Technology (NIST) began the task of providing cryptographic key management guidance, which includes defining and implementing appropriate key management procedures, using algorithms that adequately protect sensitive information, and planning ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. NIST Special Publication (SP) 800-57, Part 1 was the first document produced in this effort, and includes a general approach for transitioning from one algorithm or key length to another. This Recommendation (SP 800-131) provides more specific guidance for transitions to stronger cryptographic keys and more robust algorithms".