ENDNOTES for RECOMMENDATIONS

Endnotes i-x for Executive Summary on page 5.

1 See Endnote x.


3 See Endnote iii: section 3.7.

4 See Endnote i.


6 See Endnote iii: sections 1.1 and 1.2.

7 When he signed Executive Order 13526, the President mandated agencies to undertake a Fundamental Classification Guidance Review to review the accuracy of their current classification guides. He required agencies to complete their reviews by June 27, 2012 and submit their final reports to the Information Security Oversight Office (ISOO). See Endnote iii: section 1.9.

8 See Endnote ii.

9 The Information Security Oversight Office (ISOO) is engaged in dialogue with United Kingdom counterparts on the topic of simplifying and rationalizing information security policy in our respective governments. United Kingdom experience has shown that the proliferation of levels of classification and methods of restriction require redress to reduce costs and improve information sharing access across Government. As a result, the United Kingdom is formally developing a new classification model that contemplates using only two levels of classification. In addition, United Kingdom officials have engaged other Commonwealth partners on these topics and found similar efforts to identify and adopt a streamlined classification system.

10 As part of its study, the Board found that information classified as Confidential is created, stored, disseminated and safeguarded on Secret systems in the current classification system.

11 See Endnote v.


13 The classified electronic network systems for the intelligence and defense communities are the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet). The unclassified electronic network system is the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET).

14 Agencies have established procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. Classification challenges rarely occur as reported in ISOO’s Annual Report to the President. See Endnote iii: section 1.8 and Endnote v.

15 Under the auspices of the National Declassification Center, the implementing directive of E.O. 13526 allows agencies up to three years to complete a review their information for declassification. See 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001.34.

16 A digital asset is digital content owned by an individual or organization. Digital assets are any digital material owned by an enterprise or individual including text, graphics, audio, video, and animations. Digital content includes individual files such as images, photos, videos, and text files, and also other digital content, such as data in a database. Today, enterprises have a huge amount of digital assets that require managing. PC Magazine, (http://www.pcmag.com/encyclopedia_term/0,1237,t=digital+assets,i=41283,00.asp), Copyright © 1981–2012, The Computer Language Company, Inc.

17 One intelligence agency estimates that one terabyte of data is equivalent to approximately 112 million pages of information.


22 See Endnote iii: section 3.7.


24 The President gave the NDC a December 31, 2013 deadline to review for declassification and process for release the 400 million page backlog of archival records. See Endnote i: section 2.

25 The NDC streamlined its declassification review process by using the Six Sigma business philosophy to focus on meeting customer requirements and sustaining business products and services. The Six Sigma business management strategy seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization (“Black Belts,” “Green Belts,” etc.) who are experts in these methods. Antony, Jiju. “Pros


28 See Endnote 3.7 (b) (3).

29 See Endnote 3.7 (b) (4).

30 Although the President’s Memorandum on Managing Government Records and its Directive requires senior agency officials to identify records for eventual transfer to the National Archives, the agencies should also be required to collaborate with records officers from National Archives and the NDC to develop prioritization plans that ensure timely transfer of records for improved access to historically significant records. See Endnote x, section 2.

31 See Endnote vi.

32 See Endnote 15.

33 See Endnote iii: section 6.2.

34 See Endnote iii: section 3.7 (b) (3).

35 See Endnote iii: section 3.7 (b) (4).

36 “Center concepts” in this context refers to the declassification programming and prioritization plans associated with historical centers that operate across Government. This alignment will ensure interagency and across-agency collaboration. Some examples include the National Declassification Center and the Center for the Study of Intelligence.

37 See Endnote 39.

38 Context accumulation is the incremental process of relating new data to previous data and remembering these relationships, for improved data accuracy. It is an advanced computing process related to entity analytics in which a system is able to predict relevance and importance dynamically, based on the accumulation and persistence of context produced by ingested data. Algorithms are generated using this contextual data and then employed to determine whether newly introduced data have a place or relationship with historical data. Once this determination is made, the system then saves and uses this new observation when evaluating other introduced data. Source: Using Entity Analytics to Greatly Increase the Accuracy of Your Models Quickly and Easily, 2012, IBM®, Redbooks®, (http://www.redbooks.ibm.com/redpapers/pdfs/redp4913.pdf).

39 See Endnote x.