

## ENDNOTES *for* RECOMMENDATIONS

- Endnotes i-x for Executive Summary on page 5.
- <sup>1</sup> See Endnote x.
  - <sup>2</sup> *Improving Declassification, A Report to the President from the Public Interest Declassification Board*, (<http://www.archives.gov/declassification/pidb/improving-declassification.pdf>), January 2008.
  - <sup>3</sup> See Endnote iii: section 3.7.
  - <sup>4</sup> See Endnote i.
  - <sup>5</sup> *Transforming Classification*, (<http://blogs.archives.gov/transformingclassification/>), March 2011.
  - <sup>6</sup> See Endnote iii: sections 1.1 and 1.2.
  - <sup>7</sup> 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.
  - <sup>8</sup> See Endnote ii.
  - <sup>9</sup> 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.
  - <sup>10</sup> 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.
  - <sup>11</sup> See Endnote v.
  - <sup>12</sup> Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq. See also Endnote iii: section 6.2 and Endnote 30.
  - <sup>13</sup> 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)*.
  - <sup>14</sup> 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.
  - <sup>15</sup> 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.
  - <sup>16</sup> 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+asset&i=41283,00.asp](http://www.pcmag.com/encyclopedia_term/0,1237,t=digital+asset&i=41283,00.asp)), Copyright © 1981–2012, The Computer Language Company, Inc.
  - <sup>17</sup> One intelligence agency estimates that one terabyte of data is equivalent to approximately 112 million pages of information.
  - <sup>18</sup> “How Large is a Petabyte?” GIZMODO Storage. (<http://gizmodo.com/5309889/how-large-is-a-petabyte>), July 2012.
  - <sup>19</sup> Digital Preservation Management Workshop, Cornell University Library. Digital Preservation Management: Implementing Short-Term Strategies for Long-Term Solutions, online tutorial developed for the Digital Preservation Management workshop, developed and maintained by Cornell University Library, 2003-2006; extended and maintained by ICPSSR, 2007-on. (<http://www.dpworkshop.org/index.html>), 2012.
  - <sup>20</sup> See Endnote iii. Predecessor orders to E.O. 13526 include Executive Order 12958 of April 17, 1995, and its amendment, Executive Order 13292 of March 25, 2003.
  - <sup>21</sup> Public Interest Declassification Board's Letter to the President, March 6, 2009. (<http://www.archives.gov/declassification/pidb/letter03-06-09.pdf>) 2012.
  - <sup>22</sup> See Endnote iii: section 3.7.
  - <sup>23</sup> The Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a, as amended.
  - <sup>24</sup> 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.
  - <sup>25</sup> 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. “Pro



and cons of Six Sigma: an academic perspective”. Archived from the original on July 23, 2008. Retrieved August 5, 2010.

<sup>26</sup> National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004.

<sup>27</sup> Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.: section 142 and 10 C.F.R. PART 1045 Nuclear Classification and Declassification; Final Rule, section 1045.3.

<sup>28</sup> Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.: section 11 10 C.F.R. PART 1045 Nuclear Classification and Declassification; Final Rule, section 1045.3.

<sup>29</sup> See Endnote iii: section 6.2.

<sup>30</sup> The Atomic Energy Act of 1954 gives equity to the Department of Energy over all atomic energy and nuclear information, and stipulates that this information is automatically classified in a separate system. The two classification categories—RD and FRD—were created pursuant to the Atomic Energy Act and its implementing regulation 10 C.F.R. 1045, Nuclear Classification and Declassification. There was recognition that it was imperative to closely safeguard and protect information on the design of nuclear weapons. There was also recognition that, while the military did not need to know how to design and build a weapon, it had the responsibility to safeguard, maintain, and plan for use of the actual weapons. Thus, the implementing regulations to this act specify that FRD information is to be administered jointly by the Department of Energy and the Department of Defense.

<sup>31</sup> See Endnote vi.

<sup>32</sup> See Endnote 15.

<sup>33</sup> See Endnote iii: section 3.7 (b) (3).

<sup>34</sup> See Endnote iii: section 3.7 (b) (4).

<sup>35</sup> 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.

<sup>36</sup> See Endnote 16, “A Snapshot of the Looming Digital Challenge.”

<sup>37</sup> See Endnote x.

<sup>38</sup> The Board learned there are cases when information is so tightly controlled that agency records officers are prohibited clearance or access, and consequently are unable to evaluate the records.

<sup>39</sup> Contemplation of recommendations regarding records management practices should include determination if legislative changes are needed, specifically regarding the Federal Records Act of 1950, as amended, and the Presidential Records Act. The Federal Records Act of 1950, as amended, codified at 44 U.S.C. Chapters 29, 31 and 33, *establishes the framework for records management programs in Federal Agencies. It was last amended on October 21, 1976.* The Presidential Records Act of 1978, codified at 44 U.S.C. Chapter 22, governs the official records of Presidents and Vice Presidents created or received after January 20, 1981. It mandates the preservation of all presidential records, changing the legal ownership of the official records of the President from private to public, and implements a new statutory structure under which all presidential records must be managed. It has not been amended.

<sup>40</sup> “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.

<sup>41</sup> See Endnote 39.

<sup>42</sup> 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>).

<sup>43</sup> See Endnote x.