April 6, 2012

National Institute of Standards and Technology
100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899-1070

Re: Special Publication 800-53 Revision 4, Security Controls of Federal Information Systems and Organizations: Appendix J, Privacy Control Catalog

In response to the National Institute of Standards and Technology ("NIST") 2012 revision of the Special Publication 800-53, The Constitution Project submits these comments regarding privacy controls for federal information systems.

The Constitution Project (TCP) is a nonprofit organization in Washington, DC, that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. The Constitution Project's bipartisan Liberty and Security Committee, launched in the aftermath of September 11th, brings together members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security.

As part of this work, The Constitution Project's Liberty and Security Committee has released a report entitled *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age*.[1] This report urges the government to adopt policy reforms to ensure that we protect individuals' privacy interests and proposes specific recommendations for measures to incorporate safeguards into government data mining programs while preserving their benefits.

The report provides background on the federal government's expanded reliance on data mining, which the report defines as any use of computing technology to examine large amounts of data to reveal relationships, classifications, or patterns. While TCP's report recognizes that data mining can offer significant benefits, it also outlines the potential for such programs to encroach on privacy rights and civil liberties. To combat these concerns, it recommends, among other proposals, that agencies responsible for data mining perform regular internal evaluations of each program's effectiveness and costs, and that the government provide comprehensive accountability and oversight to prevent overreach and allow for substantive redress.

Therefore, The Constitution Project commends NIST's efforts to develop a catalog of privacy controls to assist federal agencies in upholding privacy rights and values. As discussed below, TCP welcomes the organization of the control catalog according to the Fair Information Practice Principals ("FIPPs"). The individual privacy

[1] The Constitution Project's Liberty and Security Committee, *Principles for Government Data Mining: Preserving Civil Liberties in the Information Age* (2010) (hereafter "*Principles*"), available at http://www.constitutionproject.org/pdf/DataMiningPublication.pdf

control recommendations are also laudable for their specificity and comprehensiveness. However, TCP has identified several areas where the privacy controls should be expanded or improved, including use limitations, accountability for data misuse, data security, and regulation of data practices for government contractors.

Positive Aspects of Appendix J Privacy Controls

The privacy controls in Appendix J, and the overall effort to develop a standard catalog of privacy controls for federal agencies, comport with the recommendations of TCP's data mining report. TCP commends the utilization of the FIPPs to organize and inform the privacy controls, the emphasis on privacy as a guiding value distinct from security, and the comprehensiveness of the initial privacy control catalog.

1. **Appendix J is structured according to the FIPPs.** TCP welcomes NIST's creation of an independent catalog of privacy controls for federal agencies based on the FIPPs and its emphasis on the importance of privacy "as a value distinct from, but highly interrelated with, information security."[2] Data mining may be a critical tool for measuring program performance, monitoring compliance, pursing law enforcement and counter-terrorism investigations, and other legitimate government purposes. However, as TCP's report explains, "without adequate processes and controls, [data mining] can encroach on constitutional rights and values."[3] To ensure data accuracy and security, and to protect the privacy rights of individuals whose data is used in government data mining programs, TCP's report recommends that government agencies establish privacy controls consistent with "constitutional values and the Fair Information Practice Principles."[4] Specifically, TCP recommends that during the development of data mining programs, an organization or agency should develop a comprehensive plan for the program, including its privacy protections and its impact on civil liberties and constitutional values.[5] TCP is pleased that NIST has provided a roadmap for government agencies to implement privacy protections, and that Appendix J is structured to reflect the FIPPs. The use of the FIPPs as the "backbone" of Appendix J reflects NIST's awareness of the importance of information privacy, and also ensures that federal agency personnel will be reminded of the FIPPs in the course of implementing privacy protections.

2. **Appendix J reduces barriers to the implementation of privacy protections.** Like the security control catalog of Appendix F, the privacy

[2] NATIONAL INSTITUTION FOR STANDARDS AND TECHNOLOGY, SPECIAL PUBLICATION 800-53 REV. 4: SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (Feb. 28, 2012) (hereafter "SPECIAL PUBLICATION 800-53"), at J-1.

[3] *Principles*, at 4.

[4] *Id.*

[5] *Id.* at 5.

controls of Appendix J are pre-designed tools for federal agencies to implement privacy protections in a customized way that meets their technical and program-based needs. First, the privacy control catalog helps agency personnel overcome knowledge barriers by offering pre-designed privacy protocols. This may reduce reliance on ad hoc or ill-designed privacy protocols. Second, the Appendix J offers agency decision-makers the ability to customize privacy protections to the needs and capacities of their individual programs, rather than take an all-or-nothing approach to privacy. TCP hopes that Appendix J, by presenting pre-packaged technical and procedural recommendations, will eliminate these hurdles for government agencies seeking to protect their data systems and the privacy rights of individuals whose data the agencies collect and manage.

Recommendations for Additions and Changes to Appendix J

Despite the broad scope of the proposed draft of Appendix J, several areas remain where additional or more extensive privacy controls should be implemented to ensure the catalog provides robust protections for privacy. TCP offers the following recommendations for enhancing Appendix J and increasing data privacy and security in federal government programs:

1. **Ensuring data privacy by holding contractors to identical standards as those for government personnel.** A significant concern identified by TCP's Liberty and Security Committee in the data mining report is the security and privacy risks posed by government contractors, who may not have the same privacy training or accountability for privacy violations as agency personnel. The report recommends that "contractors working on behalf of the government should be bound to incorporate [privacy protection] measures at least a strong as those described here [for government programs]," that "government employees *and contractors* should undergo thorough training prior to gaining access to personal data" (emphasis added), and that "agencies should require through contract that each contractor adopt policies and procedures to effectuate [privacy protection] principles."[6] Contractor access to and use of PII implicates the same, if not greater, privacy concerns as government access to and use of PII. Moreover, engaging contractors for data collection, use, and retention services should not be a method for avoiding the administrative and statutory privacy standards that would be applied to government personnel.

   Appendix J acknowledges the importance of privacy requirements for private contractors in privacy control AR-3, which recommends (a) the establishment of privacy roles and responsibilities for contractors, and (b) the inclusion of privacy requirements in contracts and other acquisition documents.[7] The inclusion of this privacy control is laudable; however, it is

[6] *Principles,* 26 – 28.

[7] SPECIAL PUBLICATION 800-53, at J-7.

currently inadequate to promote rigorous data privacy and security when PII is in the hands of private contractors. The AR-3 control should be enhanced in two ways, or, alternatively, NIST should create additional contractor-related privacy controls. First, the control should include a recommendation for training of contractor personnel who have access to PII. This training, whether conducted in-house by the contractor or by the government agency, should be at least as comprehensive and rigorous as the training given to government personnel with similar occupation responsibilities for PII, and should be required before a contractor is allowed access to PII.

Second, privacy control AR-3, or an additional privacy control addressing contractors, should explicitly recommend that privacy requirements for contractors be as comprehensive and rigorous as those applied to government employees in comparable positions of responsibility for and access to PII. These standards should be comprehensive, including but not limited to training, need-to-know access restrictions, data retention restrictions, internal auditing, external oversight, and penalties for violations of privacy standards.

2. **Accountability and data security through metadata/audit trails.** Our constitutional system of checks and balances requires accountability, and this concept is also recognized by inclusion of accountability as a Fair Information Practice Principle. Accountability is critical to enable the enforcement of privacy protections, permit discovery of any data security breaches, and prevent or deter intentional abuse of data. TCP's report recommends the use of audit trails to record information such as who accessed what data, when, and for what purpose.[8] This "metadata," or data about data, enables supervisors and oversight authorities to monitor data programs for misuse and security breaches, and to identify which user(s) might be responsible for such violations. TCP therefore recommends that NIST add privacy controls regarding the development of metadata and audit trails to enable accountability and monitoring, and to recommend the tracking of individual user activity in audit trails. Although NIST does include a privacy control, AR-4, that recommends implementation of technology to "ensure PII is being maintained and used only for the legally authorized purposes,"[9] the control catalog should specifically recommend user-level audit trails.

   Additionally, TCP's data mining report recommends that, to the greatest extent feasible and consistent with national security concerns, agencies should "[c]onduct and publish the results of regular audits, and report regularly to Congress."[10] These audits should track compliance with applicable statutes, administrative standards, and program-level policies for data collection, use, and retention. Therefore, TCP commends NIST for

[8] *Principles,* at 26.

[9] SPECIAL PUBLICATION 800-53, at J-8.

[10] *Id.,* at 24.

including privacy control AR-6 to encourage regular reporting to Congress. However, this control should be supplemented to encourage agencies to report the results of the regular audits we suggest here to committees of jurisdiction in Congress.

3. **Data security through encryption and anonymization in all downstream uses.** TCP recommends that the Data Minimization and Retention family of the proposed privacy controls be enhanced with an additional control, or an expansion of the DM-1 control, regarding data encryption and anonymization. As TCP's report explains, encrypting or anonymizing data to the extent possible can significantly reduce the harm caused by a data breach. "[A]nonymization engines, data masking, or data transformation can help shield sensitive data from human operators," which reduces the ability of government personnel or contractors to engage accidental or malicious misuse of data.[11] These security measures should be maintained throughout all downstream uses and transmission of the underlying data.

4. **Accountability through establishment and enforcement of penalties for misuse of data.** Enforceable penalties for the misuse of data, whether by those to whom it is formally entrusted or by those whose access is unauthorized, is critical to effective deterrence and privacy protections. TCP's report recommends that "[o]perators who do not follow the [established privacy] standards, or who otherwise misuse or abuse personal data or data mining systems" should be subject to enforceable penalties.[12] Although the agency personnel implementing privacy controls may have limited authority to establish penalties, TCP recommends that NIST include a privacy control related to the establishment and enforcement of clear penalties for data misuse, even if they these penalties are administrative only.

TCP commends the development of Appendix J and its comprehensive catalog of privacy controls, many of which comport with the recommendations of TCP's Liberty and Security Committee report. Appendix J is a valuable toolbox for federal government agencies and is an important step towards increasing data security and privacy in government programs. The Constitution Project encourages NIST to revise and expand Appendix J, taking into consideration these comments and TCP's data mining report.

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036

[11] *Principles,* at 8.

[12] *Id.,* at 23.