RECOMMENDATIONS FOR STANDARDIZED IMPLEMENTATION OF DIGITAL PRIVACY CONTROLS

DECEMBER 2012

Product of the Federal Chief Information Officers Council

Contents

I. Introduction

A. Background and Overview

The Digital Government Strategy[1] issued by U.S. Chief Information Officer (CIO) Steven VanRoekel on May 23, 2012 sets forth a new vision of how Government is to connect with and provide services to the American people, harnessing the power of digital technology and enabling citizens and the Federal workforce to securely access Government digital information, data, and services anywhere, anytime, and on any device. In helping to create a 21st Century Digital Government, the Strategy recognizes that Federal agencies, as good data stewards, must adopt strong privacy, confidentiality, and security safeguards to prevent the improper collection, use, retention or disclosure of personally identifiable information (PII)[2] when developing and delivering such digital services and programs. Services and programs that incorporate digital content, platforms, mobile applications (apps), application programming interfaces (APIs), and other new and emerging technologies must be designed and operated in a manner that fosters trust, accountability, and transparency in how personal information is collected, retained, used, and disclosed through the information's life cycle.[3]

To help meet this obligation, Milestone Action #10.3 of the Strategy calls upon the Privacy Committee of the Federal CIO Council, the National Institute of Standards and Technology (NIST), and the National Archives and Records Administration (NARA) to "develop guidelines for standardized implementation of digital privacy controls and educate agency privacy and legal officials on options for addressing digital privacy, records retention, and security issues."[4] Several efforts relating to this milestone have already been undertaken:

- NIST, in consultation with the Office of Management and Budget (OMB) and the Best Practices Subcommittee of the CIO Council Privacy Committee, has proposed recommended families of privacy controls.[5] These controls supplement and

[1] *Digital Government: Building a 21st Century Platform to Better Serve the American People* (May 23, 2012), http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf (Strategy). This document has been coordinated by CIO Council staff and prepared by members of the Innovation and Emerging Technology Subcommittee of the CIO Council Privacy Committee, in consultation with representatives of NIST and NARA. In this document, "digital" refers generally to data in electronic or other non-paper format, and "mobile" denotes data access, processing, communications, and storage by users in a dynamically located, real-time fashion, typically through portable devices and remote platforms. Internet sites, platforms, software, applications, databases, devices, and other electronic information technologies that an agency may sponsor or use to promote digital collaboration, participation, and transparency are described collectively in this document as "digital services and programs."

[2] The definition of "PII" is discussed in further detail later in this document.

[3] "The term 'information life cycle' means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition." Office of Management and Budget (OMB) Circular No. A-130 Revised.

[4] *See* Digital Government Strategy*, supra* note 1, at 25.

[5] *See Security and Privacy Controls for Federal Information Systems and Organizations,* NIST Special Publ. (SP) 800-53, Rev. 4 (Feb. 28, 2012) (initial public draft), http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf. Appendix J sets forth a catalog of eight privacy control families, based on widely accepted Fair Information Practice Principles (FIPPs) embodied in Federal privacy law and policy, including the Privacy Act of 1974, E-Government Act of 2002 (E-Gov Act), and OMB guidance. The eight privacy control families are: Authority

complement NIST's recommended security control families, and apply to traditional information technology platforms (e.g., Web sites) as well as newer digital and mobile technologies (e.g., hand-held devices).

- NARA has issued Electronic Records Management (ERM) guidance for digital content created, collected, or maintained by Federal agencies.[6] NARA also serves as managing partner of the E-Government (E-Gov) ERM Initiative, coordinating the development and issuance of enterprise-wide ERM tools and electronic information standards, to support the interoperability of Federal agency record systems and improve customer service (e.g., digital records access).[7]

Building on these privacy, security, and records management efforts, this document explains how privacy controls[8] help enable and promote the Strategy's data- and customer-centric approach, and the importance of integrating such controls into the risk management process to ensure that privacy is fully incorporated in the planning and development of digital services and programs.[9] This document then discusses three key privacy controls: (1) **PII Inventory**; (2) **Privacy Impact Assessment (PIA)**; and (3) **Privacy Notice**.[10] These fundamental privacy controls require that agencies identify and consider all PII that may be collected or otherwise exposed through a particular digital technology, analyze the privacy risks through the data life cycle by conducting and updating a PIA (as needed), and provide notice to individuals of when and how their PII will be collected, used, retained, and disclosed.

This document is not a formal guidance document and does not establish or alter official Federal Government policies. It does, however, offer recommendations that can serve as a resource to help agencies meet their privacy obligations as they implement the requirements of the Strategy. Moreover, this document does not attempt to provide a "one size fits all" approach, as each digital service or program will be different. Instead, it provides tools and best practices, in the form of key considerations and checklists, to standardize and streamline the implementation of these three critical privacy controls noted above, and to educate agency personnel on options for addressing privacy issues in the complex ecosystem inherent in the evolution toward a Digital Government.

& Purpose (AP); Accountability, Audit & Risk Mgt. (AR); Data Quality & Integrity (DI); Data Minimization & Retention (DI); Individual Participation & Redress (IP); Security (SE); Transparency (TR); and Use Limitation (UL). In addition, the Security Controls Subcommittee for the Committee on National Security Systems (CNSS) has developed a draft "Privacy Overlay" of security controls for those systems, based on the draft NIST publication to safeguard different sensitivity levels of PII.

[6] http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html.

[7] http://www.archives.gov/records-mgmt/initiatives/erm-overview.html.

[8] *See supra* note 5.

[9] This document does not address the implementation of specific security controls such as mobile device management (MDM) software or other methods to secure and protect digital data and content. For a discussion of security controls generally, *see supra* note 5 (NIST SP 800-53, Rev. 4), and consult other NIST guidance documents for specific data security recommendations. *See, e.g.,* NIST, *Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)*, NIST SP 800-124, Rev. 1 (July 2012), http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

[10] *See* SE-1 (Inventory of PII), AR-2 (Privacy Impact and Risk Assessment), and TR-1 (Privacy Notice). These controls are part of the Security (SE), Audit & Risk Mgt. (AR) and Transparency (TR) privacy control families, respectively, as set forth in NIST SP 800-53, Rev. 4, App. J, *supra* note 5.

B. How Privacy Enables A Data- and Customer-Centric Approach

The Strategy requires that Federal agencies move from managing "documents" to a more "data-centric" approach, emphasizing discrete pieces of open data and content. Under this approach, data may be broken down into smaller units or elements, tagged, shared, secured, recombined and presented in a variety of ways most useful to users of that data.[11] The Strategy also urges agencies to adopt a "customer-centric" approach to digital services by creating, managing, and presenting data through many different delivery modes (e.g., Web sites, mobile applications, raw datasets), so that users can shape, share, and consume that data whenever and however they want.[12]

The Strategy recognizes that a data- and customer-centric approach cannot be at the expense of privacy, security, or other legal or policy requirements, and should generally attempt to meet privacy expectations to preserve public trust. As discussed below, to enable the most open and flexible use of data, Federal agencies must identify and address privacy issues and risks at the earliest stages of developing digital services and programs—*well before* data about individuals are collected, used, retained, or disclosed. Individuals' privacy expectations when interacting with an agency's digital service or program will differ depending on a variety of factors, including: the specific technologies (e.g., Web site, mobile app) that the agency is using to engage with the individual; the context in, and purpose for, which the individual's data may be collected, used, or disclosed; the individual's right to control or to exercise choice in the collection, use, or disclosure of his or her data under applicable law or policy; and what notice or understanding the individual has about the agency's privacy and security practices with respect to his or her data.[13] Addressing privacy issues in designing the data collection will enable the agency to build into the data collection and processing procedures the data-centric privacy controls needed for the agency to better meet individuals' privacy expectations, e.g., honoring any choices they may have made concerning data sharing.[14] Failure to manage and protect data in light of these privacy expectations (e.g., lack of adequate controls leading to a data breach) can seriously undercut public trust in the agency's digital services and programs and result in liability if applicable legal restrictions are violated.[15]

---

[11] *See* Digital Government Strategy, *supra* note 1, at 5.

[12] *Id.*

[13] *See generally Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy* (White House, Feb. 2012) (*Consumer Privacy Bill of Rights*) at 1-2 (providing a privacy framework that applies to the commercial sector, rather than the Federal Government, but including a useful discussion of key FIPPS, such as notice, individual control, respect for context, and transparency), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[14] *See* www.niem.gov (National Information Exchange Model, promoting collaboration in developing technical rules and syntaxes for sharing digital data). Although the technological tools in this area are evolving, it may be possible in some instances for administrative, technical, or physical privacy controls to follow the data or content, independent of particular data format, platform, or mode of presentation or delivery (e.g., HTML). If collections of data are later disaggregated or recombined, such controls could be carried forward with the relevant data elements to ensure the data are handled in ways that are consistent with individuals' expectations and applicable legal and policy restrictions.

[15] There may be a risk of violating applicable privacy laws (e.g., the Privacy Act of 1974, laws governing Federal health, tax, census and student data) and confidentiality laws (e.g., Confidential Information Protection and Statistical Efficiency Act (CIPSEA)) if data about individuals are not maintained and managed in a fashion that

C. Addressing Privacy Through A Risk Management Process

Digital and mobile technologies present complex and novel challenges to protecting individual privacy. Table 1, at the end of this document, describes key players or stakeholders in the mobile and digital "ecosystem" and the many points in that system or environment where PII might be collected, used, retained, or disclosed, and might be vulnerable to misuse or unauthorized disclosure. Table 2 sets forth examples of some new and emerging digital and mobile technologies and the special privacy risks they present.

NIST's Risk Management Framework[16] provides a process for concurrently identifying and addressing information security and privacy[17] risks in the planning and design of digital services and programs, particularly those deploying new or emerging technologies. Like the process for managing risks to the *information security* of an agency's information system, a PIA, conducted in the early planning and design stages of a digital service or program, identifies and assesses risks to *privacy* that the service or program may raise. An agency can then determine how best to control and mitigate these risks as part of the design and development process. (This concept is often referred to as "privacy by design.")[18] Effective management of privacy risks also requires determining how such risks will be continuously monitored—including whether designated privacy controls remain functioning and effective—once the agency's service or program is operational.[19]

---

reliably allows the agency and other intended data users to know what specific uses or sharing is permitted or prohibited under such laws. For example, data collected solely for statistical purposes under CIPSEA may not be used for non-statistical purposes.

[16] NIST's Risk Management Framework for Federal agencies involves: (1) analyzing and determining the impact (sensitivity) of a system and its data; (2) selecting appropriate controls; (3) implementing and documenting such controls; (4) assessing whether they have been implemented properly; (5) authorizing the system or program (i.e., determining that the remaining level of risk after controls are applied is acceptable); and (6) monitoring and assessing the continued effectiveness of the selected controls. *See* http://csrc.nist.gov/groups/SMA/fisma/framework.html; NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, rev. 1 (Feb. 2010).

[17] "Information security" refers to the protection of the confidentiality, integrity, and availability of data. *See* 44 U.S.C. 3542 (Federal Information Security Management Act). "Privacy" is a broader term encompassing security as well as other "privacy" interests enumerated in the FIPPs (*see supra* note 5), including, for example, notice, access, choice, and accountability. "Confidentiality" refers to the protection of information from disclosure and can apply to information about individuals (*see, e.g.*, NIST Special Publication 800-122, discussed *infra*) or about non-individuals (e.g., confidential data about businesses).

[18] *See generally* Federal Trade Commission (FTC), *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (March 2012) (recommending that businesses incorporate privacy throughout the organization at all stages of product and service development, including for example, data security, reasonable collection limits, sound retention and disposal practices, data accuracy, and comprehensive, life cycle data management procedures), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; FTC, *Marketing Your Mobile App: Get It Right From The Start* (Aug. 2012) (mobile apps should be designed to include tools that individuals can easily find and use, to provide them with choice, such as privacy settings, options, and other ways users can control how their information is used and shared), http://business.ftc.gov/documents/bus81-marketing-your-mobile-app; *see also Consumer Privacy Bill of Rights, supra* note 13, at 1 (respect for context and individual control).

[19] *See* NIST, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* SP 800-137 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf; *see also supra* NIST SP 800-37, Rev. 1, sec. 3.36 and App. G (continuous monitoring); *see supra* note 3, NIST SP 800-53, Rev. 4 (security control CA-7 for continuous monitoring).

To incorporate privacy into the risk management process, agencies will need to address each of the privacy controls recommended by NIST,[20] and determine how they apply to their agency-specific circumstances. As noted, while each digital service or program will be different, agencies can streamline the implementation of privacy controls by adopting standardized approaches for a PII inventory, a PIA, and privacy notice. This document discusses each of those privacy controls in detail, [21] and then sets forth: a suggested checklist or inventory of common types of PII collected or used by digital services or programs (Table 3); specific privacy questions that agencies should ask when conducting a PIA for such digital services and programs (Table 4); and required elements of a privacy notice to individuals in the context of such services and programs, consistent with applicable Federal privacy law (e.g., the Privacy Act of 1974), regulations, and policy (Table 5).

[20] By employing the privacy controls in App. J and the security controls in App. F, agencies can achieve comprehensive security and privacy protection. *See* NIST SP 800-53, Rev., 4, at 5 n.26.

[21] The term "digital," when used below to describe PII inventories, PIAs, and privacy notices, indicates that digital services and programs often pose privacy considerations or challenges not presented by non-digital services or programs. At the same time, the specific requirements of Federal law, regulation, and policy for PII inventories, PIAs, and privacy notices remain unaltered.

II. Digital PII Inventory

To properly assess and mitigate the privacy risk of its digital services or programs, an agency must first know what PII may be collected, maintained, used, or disclosed. While a PII inventory normally means a catalog of *existing* PII holdings,[22] agencies should, as part of their privacy risk management process, conduct a *prospective* inventory of PII that may be collected, used, or disclosed. Doing so early in the PIA process (*see Section III)* will help agencies avoid unanticipated privacy risks later. This pre-collection inventory allows an analysis and determination of the sensitivity or "impact" level of the PII (i.e., low, moderate, or high) in order to determine how strictly the data should be controlled for privacy and security purposes.[23]

No PII inventory or catalog can be adequate or complete without a sufficiently broad understanding of what personal information should be considered "identifiable." A common misconception is that PII only includes data that can be used to directly identify or contact an individual (e.g., name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number). The OMB and NIST definition of PII is broader.[24] The definition is also dynamic, and can depend on context. Data elements that may not identify an individual directly (e.g., age, height, birth date) may nonetheless constitute PII if those data elements can be combined, with or without additional data, to identify an individual. In other words, if the data are linked or can be linked ("linkable") to the specific individual, it is potentially PII.[25]

Moreover, what can be personally linked to an individual may depend upon what technology is available to do so. As technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible (this is often referred to as the "mosaic

[22] *See* OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) (requiring agencies to conduct initial and subsequent reviews of current PII holdings); NIST SP 800-53, Rev. 4, App. J at p. J-18 (describing Privacy Control SE-1, PII inventory); *see also Guide to Protecting the Confidentiality of Personally Identifiable Information*, NIST SP 800-122 at ES-1 (April 2010) ("Organizations should identify all PII residing in their environment.").

[23] The criteria and methodology for determining PII impact level are set forth in NIST SP 800-122, *see id.*

[24] *See, e.g.,* OMB Memorandum M-07-16 ("The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."); *see also* NIST SP 800-122 at 2-1; OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010) ("The definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.").

[25] While this definition leaves considerable room for interpretation, a broad rule of thumb is that data collected from or about an individual, regardless of its sensitivity (impact level), is potentially PII for purposes of performing a PIA. *See* NIST SP 800-122 for further discussion of "linked" or "linkable." Agencies should not exclude data from the risk assessment process merely because the data might be redacted, disaggregated, masked, or otherwise "de-identified" after collection.

effect"). Agencies should periodically consider re-assessing the PII status of their data holdings based on technological advances.

Table 3 provides a checklist of PII commonly collected or used in the digital or mobile environment about users of digital services and programs, or about other individuals (e.g., the user's friends, relatives, and associates).[26]

Different digital services or programs may involve collection, use, retention, or disclosure of different kinds of PII, including possible access by third parties to such PII, depending on the specific digital or mobile technology involved. For example, near field communications (NFC), facial recognition software, geotagging, augmented reality devices, services that rely upon geo-location or other device-based data, mobile payments, identity management software, and so on, all take advantage of the rich sources of data collected, provided, or stored by users' mobile devices in different ways (e.g., audio, video, photos, fingerprints, device sensors, device IDs, SD card data). See Table 2 for additional information. Moreover, as technology continues to evolve, the ability to use publicly available data to identify an individual will likely increase substantially.

Once PII has been collected from or about individuals, data loss prevention (DLP) tools (software and hardware) are critical to detecting PII network traffic or storage.[27] Such DLP tools and other technologies can help agencies automate the inventory process and ensure that the agency fully accounts for the types, amounts, and locations of its PII holdings.[28]

[26] While a checklist can be an important step in describing PII and building a disclosure risk reduction strategy, it may also give the unwanted impression that it is comprehensive in its data elements. A checklist cannot substitute for a full calculation of the potential disclosure risks as part of a PIA that requires the agency to consider, among other things, whether such data can be combined or matched with other available data, as discussed *infra*.

[27] *See supra note 19* NIST SP 800-137, at D.1.8 (discussing DLP tools to monitor data at rest, in use, and in transit, including database transaction monitoring, network traffic monitors or software agents); *see also* NIST SP 800-122, at 2.1 (noting that agencies may use various methods to identify PII, including DLP technologies such as automated PII network monitoring tools).

[28] The Best Practices Subcommittee of the Federal CIO Council Privacy Committee is developing a white paper on conducting effective PII inventories to meet a key mandate of OMB Memorandum M-07-16.

III. Digital Privacy Impact Assessment (PIA)

Under the E-Government Act of 2002, Pub. L. 107-347 (E-Gov Act), and OMB guidance,[29] a Federal agency may not develop or procure information technology to collect, maintain, or disseminate PII[30] from or about members of the public unless the agency first performs a PIA to assess and address the privacy impact of that technology. A PIA analyzes how information will be handled to ensure such handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, to determine the risks and effects of collecting, maintaining, and disseminating such information, and to examine and evaluate protections and alternative processes for handling the information to mitigate potential privacy risks.[31]

The PIA process must be documented, and must explain: (1) what PII will be collected, maintained, or disseminated, including the nature and source of the data; (2) why the PII is being collected (i.e., purpose); (3) intended use or uses of the PII; (4) with whom the information will be shared or disclosed; (5) options and methods for individuals to exercise choice or give consent for collection or use; (6) how the PII will be secured; and (7) whether a system of records is being created under the Privacy Act of 1974. A PIA may need to be performed again and updated if there are changes in the service or program that materially alter previously identified privacy risks (e.g., merging existing databases, making data available on new or different technology platforms).[32]

---

[29] *See* E-Gov Act sec. 208(b) and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003). OMB has issued a PIA template specifically for the use of social media or other third-party applications or sites by Federal agencies. *See* OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010). This document does not purport to modify, conflict with, or supersede that guidance, or other Federal privacy risk assessment guidance. *See*, *e.g.*, Federal Risk and Authorization Management Program (FedRAMP), PIA template for cloud service providers (CSPs), *available at* www.fedramp.gov. In practice, agency PIAs often include questions beyond the general scope of issues identified by E-Gov Act and OMB Memorandum M-03-22, in order to ensure a thorough and detailed privacy risk assessment, *See, e.g.,* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf (DHS PIA template).

[30] E-Gov Act uses the term "information in identifiable form" (IIF) to describe PII. *Cf.* E-Gov Act sec. 208(b) and (d) ("identifiable form" means "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means"). OMB guidance requires PIAs only for IIF about individuals who are "members of the public" and U.S. citizens or lawfully admitted aliens. *See* OMB M-03-22, secs. II.A.a (defining "individual") and II.B.a (when to conduct a PIA). This document suggests as a best practice that agencies, where appropriate and feasible, should consider performing PIAs for digital services and programs even if they involve data about individuals outside those categories (e.g., Federal employees, foreign travelers).

[31] *See* OMB M-03-22, sec. II.A.f (defining PIA). A PIA is also required before an agency initiates any electronic (digital) information collection activity posing identical questions to 10 or more persons, subject to OMB clearance and approval under the Paperwork Reduction Act (PRA). *See* E-Gov Act sec. 208(b)(1)(A)(ii)(II) (excluding collections of data from Federal agencies, instrumentalities, and employees). A discussion of PRA requirements is beyond the scope of this document. Nonetheless, it should be noted that the OMB clearance process typically requires agencies to include in their supplemental statement an explanation of what steps have been taken to protect the confidentiality of individual respondents. *See also* OMB Memorandum M-03-22 (PRA supplemental statement should incorporate and summarize the privacy analysis set forth in the agency's PIA).

[32] *Id.* (explaining circumstances in which a PIA must be updated). For accountability purposes, the PIA must be made public (e.g., on the agency's Web site), except for portions that would compromise security. The level of documentation and analysis depends on size and complexity of the service or program. *Id*. (noting that a

Table 4 sets forth a list of additional questions that agencies should ask when conducting PIAs for digital services and programs. These questions, which supplement and do not replace the PIA required under the E-Gov Act, focus on special or unique privacy issues presented in the digital and mobile environment. These questions should help agencies in assessing and determining PII impact (sensitivity) levels, minimizing the unnecessary collection of data from individuals, planning for and responding to data breach incidents, controlling and managing the use of tracking or customization technologies (e.g., cookies, beacons), determining legally when PII will be part of "agency records" for Privacy Act purposes, and identifying special considerations in "bring your own device" (BYOD) scenarios.

A key element of a PIA is assessing and calculating the disclosure risk associated with the data at issue. One particularly important consideration in this regard is assessing and calculating the risk that such data could be combined with other available data to identify or re-identify the subject individual.[33] Even if data appear to be minimally sensitive or not readily identifiable, additional data elements can make the data, if released, increasingly unique, and potentially allow subject individuals to be identified or tracked. Where the data at issue are intended to be released to the public, and therefore the use of such data would be unmonitored, the risk of identification and potential misuse is greater. Once data are released, attempts to control access or use are limited, if any.

An agency should apply statistical methods to estimate the likelihood and magnitude of this risk.[34] The agency must then consider the intended purpose of the dataset and the estimated risk of disclosure when adopting methods to reduce risk. This may include limiting specificity of data elements, limiting means of access, or applying statistical methods to reduce the likelihood of identifying an individual respondent.[35] Agencies should begin this risk management analysis

---

standardized approach (e.g., checklist or template) may be used for "routine" data that will involve "limited use and access").

[33] The potential for re-identifying, tracing, or targeting individuals may arise from the application of predictive analyses and other "data mining" techniques to "big data" (i.e., the increasing availability of vast amounts of stored and streaming digital information). *See, e.g.*, NIST Data Mining Portal (describing ongoing programs, projects, and workshops), http://www.nist.gov/data-mining-portal.cfm. Agencies should ensure that their PIAs for digital services and programs consider whether data mining could be used to identify, trace or target individuals, and be aware of statutory reporting obligations when engaged in data mining for the detection of criminal or terrorist activities. *See* GAO, *Data Mining; Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain* (Aug. 2005) (noting need for agencies to provide proper notice and perform PIAs), http://www.gao.gov/new.items/d05866.pdf; Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. 2000ee-3 (requiring the reporting to Congress of pattern-based queries, searches, or analyses of one or more databases by or on behalf of the Federal Government to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals).

[34] This risk calculation does not contemplate that risk can be determined with absolute precision, but to a known degree of certainty. The Federal Committee on Statistical Methodology (FCSM, organized by OMB, has issued guidance on this topic. *See Statistical Policy Working Paper No. 22: Report on Statistical Disclosure Limitation Methodology* (Rev. 2005) http://www.fcsm.gov/working-papers/spwp22.html.

[35] *Id.* Such an analysis can be appropriate or necessary even when data will be shared or exchanged only within the Government, since source and recipient agencies may have access to data that could be combined or matched to identify individuals and be used to determine or otherwise affect their legal or financial rights or benefits (e.g., matching activities conducted under data matching agreements subject to the Privacy Act of 1974). Likewise, agencies should consider and assess the risk that digital services and programs sponsored by the agency, particularly those requiring the involvement of contractors or nongovernment organizations or platforms, may incorporate or enable tracking technology (e.g., cookies, beacons) that could allow such third parties to collect or

before collecting data from or about individuals, and refresh this evaluation once data have been collected, before publicly releasing such data. Agencies may need to re-assess the risk as other related datasets and sources come online, which may affect the disclosure risk analysis and the controls needed to address the risk. Under OMB's *Open Government Directive*,[36] which requires that agencies evaluate previously non-public high-value datasets for possible publication, agencies are encouraged to consult guidance developed by the Open Government Initiative Privacy and Security Working Group, an interagency group led by the National Security Staff, for systematically reviewing whether any privacy and confidentiality laws, rules, or policies may permit or limit public disclosure of such previously collected data,[37] and to help determine appropriate controls to mitigate that risk and protect privacy and confidentiality (e.g., limiting access, removing identifiers, suppression, rounding, swapping and blurring of microdata), before agencies begin compiling and structuring their data for such release.[38]

In connection with their PIAs, agencies should also consider mapping (e.g., diagramming or charting) the flow of PII in and out of digital systems, as well as the interconnectivity between such systems. Such mapping can help agency privacy officials, as well as information technology officials involved in the security assessment and authorization process, to visualize and quickly pinpoint where risks (e.g., data disclosure, sharing, matching, breach) may arise and where controls may be needed.

---

combine such data with other available data to identify or track individuals, even if such tracking data are never released to or available to the public at large. The risk that data collected and made public by an agency could identify non-individuals (e.g., businesses that submitted such data under a pledge of confidentiality) falls outside the scope of this document, but is also appropriate and necessary to assess as part of the agency's risk management analysis of its information collection activities.

[36] OMB Memorandum M-10-06, *Open Government Directive* (Dec. 8, 2009).

[37] The Working Group has made available a checklist, identifying potential privacy and confidentiality issues, as well as national security issues, and other procedural guidance, at http://www.data.gov/sites/default/files/attachments/Privacy%20and%20Security%20Checklist.pdf.

[38] *See* note 34, FCSM *Statistical Policy Working Paper No. 22.*

IV. Digital Privacy Notice

Federal agencies are required by law (e.g., the Privacy Act of 1974) to give notice to individuals, when collecting information from them, of the authority, purpose, and uses of PII when such data will be maintained as agency records that will be retrieved by individual name or other identifier.[39] When agencies use a Web site to collect or share data, agencies must post a privacy policy, as required by Section 208 of the E-Gov Act and OMB guidance.[40] Additional privacy notice requirements may apply, depending on other factors such as what digital technology or platform is being used. For example, agencies must give notice when using social media or other third-party sites or applications to communicate with the public if PII will be available to the agency.[41]

Over time, agencies, digital developers, and data users may also create, discover, or propose new and innovative ways to combine, share, or otherwise leverage the power of the digital data and content collected or disseminated by their digital services or programs. If data will be re-combined, used or shared in ways that individuals did not originally contemplate or expect, agencies must consider the need, under applicable law or policy, to provide such individuals with additional or updated notice of their privacy rights and choices.[42]

In determining precisely when, where, and how to give such notice, agencies, their digital developers, and partners will need to exercise creativity and ingenuity to ensure that required notices are clearly communicated to individuals at the right time and place, and in the right manner, without unduly interfering with the user experience. The timing and format of such notices may need to vary, depending on the digital or mobile platform involved.[43] In all cases, privacy notices must be prominent, salient, clearly labeled, written in plain language, and available at all locations where notice is needed.

For example, a privacy policy designed for a Web site may not be as easily found or viewed by the individual when the same policy is displayed on a hand-held mobile device. Mobile devices and platforms may offer other options (e.g., pop-up menus, user-determined settings) for informing individuals about what data will be collected from them, and for them to quickly and

---

[39] 5 U.S.C. 552a(e)(3) (Privacy Act statement). *See also* 5 U.S.C. 552a(e)(4) (publication of system of records notice (SORN) in the *Federal Register* for agency record systems containing data subject to the Act).

[40] *See* OMB Memorandum M-03-22.

[41] *See* OMB Memorandum M-10-23. For example, to the extent feasible, agencies should include a Privacy Notice on the third-party application or service. *Id*. Other privacy notice or consent requirements may apply, depending on the type of PII to be collected (e.g., children's personal information subject to the Children's Online Privacy Protection Act (COPPA), tax, health, Census, banking, or student data).

[42] A noteworthy development in this area is the ongoing effort to modernize the "Common Rule," which provides protections for human subjects in Government-sponsored research. *See* http://www.hhs.gov/ohrp/humansubjects/anprm2011page.html; *see also infra* Table 5. That effort recognizes the importance of obtaining sufficient consent up front for future potential data uses, rather than seeking additional consent later, which may cause individuals to question whether the Government stands behind the privacy promises that it made at the time the data were originally collected.

[43] *See Consumer Privacy Bill of Rights, supra* note 13, at 14-19.

easily indicate how and whether they want their data to be collected, used, or shared. Agencies may need to explore or experiment with delivering notices and consent options in layered, serial, or other formats, so that key disclosures are sufficiently prominent and comprehensible, and not buried or obscured by less important or technical legal disclosures.

Given the variety of potentially applicable notice requirements and presentation contexts, it is not possible to prescribe a single model digital privacy notice. To help agencies begin this complex task, Table 5 provides agencies with a checklist of many of the key elements of a privacy notice. This checklist can help agencies ensure that such notices contain legally required content, are properly displayed, and are made accessible to the public and relevant individuals. Agencies must take care to consider the specific context and to carefully tailor notices to meet all applicable requirements.

V. Conclusion

The Digital Government Strategy recognizes that open use of digital data and content creates opportunities for greater collaboration, participation, and transparency—the core objectives of the Open Government Initiative. At the same time, the Strategy acknowledges that special care must be taken with data collected from or about individuals, in light of the unique and complex risks posed by the potential maintenance, use, and sharing of that data in the digital and mobile environment.

By adopting the recommended best practices outlined in this document, agencies should be better able: (1) to identify and account for such data (i.e., PII inventory); (2) to analyze and address the privacy and security risks that may be associated with such data (i.e., PIA); and (3) to provide individuals with the knowledge, assurance, and trust that their data will be collected, maintained, used and shared in a manner consistent with their expectations (i.e., privacy notice). Agencies should always address and resolve these issues early in the planning and design of their digital services and programs; this approach is more likely to achieve the Strategy's goal of a data- and customer-centric approach to digital data and content with greater speed, efficiency, and effectiveness.

This document is based upon privacy controls and best practices developed under currently applicable law, regulations, and policy. In the event such legal authority or guidance is subsequently updated or altered, agencies may need to modify or adapt the recommendations set forth in this document in order to conform to new or superseding legal and policy requirements. As always, agencies should consult existing laws and policies, and comply with all applicable requirements that pertain to privacy, confidentiality, and security.

Table 1: Federal Digital and Mobile Ecosystem

The mobile ecosystem has a number of potential vulnerabilities based on the platform or device design, the services or programs provided through the platform or device, and the user's activities on the platform or device. These vulnerabilities apply to different kinds of personal data including location, photos, contact numbers, health, and financial data that may be processed on the platform or device. Mobile functionality that requires data collection and disclosure often enables precise tracking of the user's movements and activities, and may not always have clear limits on data retention. The table below highlights some of the actors in the digital and mobile ecosystem, the kinds of data that might be collected, and associated privacy risks. Agencies must consider the entire digital and mobile ecosystem in determining what privacy (and security) controls should be implemented to protect PII against unauthorized collection, retention, use, and sharing.

Ecosystem Actor	Possible Threats and Vulnerabilities
Mobile device manufacturers or other original equipment manufacturers (OEMs)	• May make design decisions to manage user experience that create privacy vulnerabilities. For example, in order to make photo apps more efficient, an OEM may permit apps that request location data to have access to other device data (e.g., photos, address books), even if the app functionality does not require such access. • May make design decisions that limit the ability for effective notice to be provided to individual users, or fail to provide granular access controls for apps privileges or execution.
App developers and platforms	• May exploit vulnerabilities created by OEMs. For example, app developers may design applications that exfiltrate photos once the device user permits the app's access to location data. • May design applications with capabilities that are not accurately or comprehensively disclosed to the user, or that collect more than minimal information necessary to complete a transaction to provide a better user experience (e.g., linking contact books with video conferencing capabilities) or to leverage for advertising and additional sales.
Content developers and publishers (e.g., Federal agency sponsoring the digital service or program)	• May direct their content distributors to collect more information on their behalf than needed and/or without adequate notice. • May inadvertently publish sensitive or insufficiently anonymized data.
Wireless carrier or network	• May require OEMs to install software to collect user data. • May maintain cell tower or other tracking data that can provide user location and other communications records.

Ecosystem Actor	Possible Threats and Vulnerabilities
Advertisers and advertising platforms	• Commercial entities may collect and aggregate user data through apps and Web sites to create detailed user profiles for purposes of targeted advertising and sharing with other advertisers.
Equipment/device vendors	• May fail to appropriately wipe the mobile device of personal information associated with the user when refurbishing or disposing of it, or could compile, store, aggregate, or use such data for analytics or other purposes without user consent.
Device users	• May fail to implement security measures like lock features or permissions and fail to appropriately restrict device or service capabilities. • May generate and publish their own personal information through phone calls, tweets, blogs and photos; and when collaborating with others for personal or work reasons, these users may lose control of, and subject, critical information to misuse by relying on unsecure file-sharing services. • May fail to recognize phishing (e-mail) or SMSishing (text message) attacks that seek and exploit their personal information by luring or tricking them into downloading malware and/or sending their personal information. • May sell, donate, trade-in, or transfer their devices to others (e.g., charities, retailers, other individuals) without sufficiently wiping their devices of personal data. • Individuals who use their mobile and non-mobile devices and equipment to create digital content (e.g., word processing documents, photos) may be unaware of the extent or nature of metadata that is automatically generated with such content, and may not be able (or know how) to prevent the creation of such metadata or its transmission to or collection by others with their digital content. For example, word processing documents may contain metadata about author name, organization, commenters, etc., while digital photos may be encoded in Exchangeable Image File Format (EXIF) with time, date, location or other photo-related data that can be traced to the individual.
Web sites and servers (including cloud and other remote storage facilities)	• Maintain visitor log data (e.g., time, date, current and previous site visited, IP address), and may collect more detailed personal data from visitors through use of online forms, and may use temporary or persistent tracking technology (e.g., cookies, web beacons). • Cloud and other remote storage facilities may affect the Government's physical or legal control. Service level agreements (SLAs) may contain non-negotiable terms that may be inadequate to protect the privacy and security of such data.

Ecosystem Actor	Possible Threats and Vulnerabilities
Internet service providers	• Can track customer's usage, including Web sites and services visited or used, and may share this information with other parties in ways that customer or subscriber may not be aware of.
Third-party data sources (e.g., data brokers)	• May provide, or be used as a source for, digital data for use in conjunction with platform, device, or program functionality, or may collect PII from devices and users as part of that process. Data may not be accurate and reliable, and adverse actions or decisions regarding the individuals or others may result. • Data collected from or about individuals by the third party may be combined with or imported into other databases to create more detailed profiles of individuals without their knowledge or consent.
Third-party individuals or entities seeking to obtain unauthorized access	• This category may include hackers, foreign intelligence, organized crime, and others who may seek to exploit vulnerabilities in devices, networks, or programs to obtain unauthorized data access.

Table 2: Digital and Mobile Technologies and Privacy Risks

This table highlights some new and emerging Web and mobile device technologies and the special or unique privacy risks they may present.

Technology	Privacy Risks
Mobile apps: Software pre-installed or downloaded on demand to a mobile device in order to enable or facilitate specific types of transactions or data access (e.g., mobile payments, social networking, access to Government services or accounts).	• Some apps may contain malware (see supra Table 1) that may compromise the host device, including any PII that the device stores or transmits. • Apps may not fully or properly disclose what PII they are accessing from the device, or may access more PII than needed. • App security may not be fully vetted by the platform provider. • Users may routinely provide or share financial account or other sensitive data to use the app (e.g., credit card number).
Mobile Device Hardware (e.g., cameras, microphones)	• Can capture and record audio, video, or other data, including the generation of metadata about the user (e.g., digital photos may also contain metadata such as name, location, device ID, etc.). Could be hijacked, turned on or off, and otherwise controlled remotely to spy on the user or others. • Wireless communications channels intended for wireless earphone equipment (e.g., Bluetooth) may allow an attacker to install malware through that connection or activate the microphone/camera to eavesdrop on a user.
Quick Response (QR) codes: Matrix-style geometric barcodes displayed in magazines, on billboards and posters. Scanning them with a mobile device, such as a smartphone, directs that device to a specific URL, providing highly convenient access to information.	• Easy to create and produce, fraudulent QR codes can be placed as stickers over genuine QR codes. Users may be unaware that they are being directed to phishing sites that may collect PII to commit identity theft or other fraud, or to sites that deliver malware or other untrusted content to their devices, putting any PII on those devices at risk. If those devices are then connected to other equipment (e.g., laptops, PCs), the malware may infect that equipment and any stored PII. • Mobile applications for processing QR codes can also collect PII without user knowledge or express consent.[44]

[44] *See* NIST *Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)*, NIST SP 800-124, Rev. 1 (July 2012), sec. 2.2.8, http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

Technology	Privacy Risks
Geotagging: Locational data that, usually by default, is embedded in photos and videos taken with Global Positioning System (GPS)-equipped digital cameras, smart phones, and other mobile devices. Some smart phones also attach a geotag to text messages. GPS data may also be routinely broadcast by such devices and intercepted by others.	• Can allow others to identify the location where a picture was taken (e.g., using free browser plug-ins), to track an individual's location, or to correlate such data with other information. • The use of locational data to report an individual's movements, whereabouts or actions online in real time (e.g., on social networking sites or other public platforms, to track where an individual may be shopping, eating, sleeping, etc.) can enable "cyberstalking" or "cybercasing" (i.e., use of such information to commit real-world crimes).
Near Field Communications (NFC): Wireless communication interface that allows mobile devices to connect with each another or other electronic devices by physical proximity without the need for a direct physical connection. This technology may also be embedded and used by smart cards (e.g., mass transit passes).	• Data on NFC cards or other NFC-enabled devices can be extracted or intercepted by unauthorized readers (wireless eavesdropping), or may be maliciously disrupted, destroyed, or modified in transmission (e.g., inserting fraudulent information into an otherwise legitimate data transfer).
Augmented reality devices: Eyeglasses-type apparatuses or other wearable computers or devices that superimpose or provide virtual data to "augment" the physical objects or scenes viewed or perceived through such devices. Smart phones or other mobile devices may also perform similar augmented reality functions (e.g., displaying Internet-based data relating to objects viewed through the device's camera).	• May collect or share detailed data about a user's physical state (e.g., pulse, body temperature), location, or actions. Privacy policies governing the use of such data may not be clear or readily available. • Devices may collect, process, or transmit photographic or other data about other individuals without their knowledge or consent. May be used for targeted advertising, as real-time location data is highly valuable for marketers, or may be combined with other personal data about the individual. • Live data transmissions or stored data might be hacked or otherwise accessed remotely by unauthorized parties.
Facial Recognition: The detection, categorization, or direct identification of individuals by their facial features through computerized analysis of visual data (e.g., photos, video) or comparison with existing databases about such individuals. This technology may be used to recognize and deliver tailored messages to shoppers	• Data collected and used to conduct facial recognition may be combined and compiled into larger databases without the individual's knowledge and consent and potentially shared with other Government and non-Government parties to provide more specific and targeted data profiles of individuals. • Such technology could enable improper discrimination against individuals (e.g., based on race or sex).

Technology	Privacy Risks
entering a retail store, for identity management and authentication purposes, and in social networking applications (e.g., to automatically tag or associate individual names with photos).	• Individuals who wish or expect to remain anonymous may be less able to control whether others can identify them (e.g., using visual-based search engines).[45]
Identity Authentication and Management: Electronic systems and protocols (e.g., digital signatures or trusted credentials) for verifying and authenticating the identity of an individual for purposes of granting authorization and physical or logical access to services, data, and facilities requiring controlled access.[46]	• These systems often collect and store PII that is potentially sensitive and unique about an individual (e.g., fingerprints, photos, Social Security or financial account numbers). If compromised, identity management credentials or data can be used to gain unauthorized access, or be stolen and sold for profit or used for identity theft.
Smart Grid: The ability of public utility grids or networks (e.g., electric grid) to provide customers with individualized online control and access to billing, payment, usage or other personal account data, and potentially over major appliances/electrical devices in the home. Allows users to control devices, order service, adjust their service level, or communicate with the service provider. Also refers to the ability of the service provider to pool, analyze, and use individual account and system data to shift resources and react efficiently and quickly to demands on the network.	• Unauthorized access to energy consumption data may allow others to monitor an individual's activities (e.g., detecting when he or she may be home, at work, or on vacation based on usage patterns, or when and what appliances are being used based on known energy use profiles), to make changes to the account (e.g., shut off the customer's service), or to divert or steal services or personal data (e.g., autopay bank account number on file).[47]
Biometrics: Data measuring physical characteristics of individuals (e.g., voice, DNA, hand print, iris/retina, walking gait, keystrokes, other behavior) that are used for identity management (e.g., gaining access to controlled facilities or networks).[48] Similar data may also be	• Biometric data about an individual's physical attributes may enable targeted advertising or other potentially adverse consequences (e.g., higher insurance redlining). • Data used to identify individuals in unique and persistent ways that also have a potentially significant impact on privacy and civil liberties if accessed by

[45] *See* http://ftc.gov/os/testimony/120718facialrecognition.pdf (July 18, 2012) (FTC testimony on technology and privacy risks).
[46] *See, e.g.,* http://www.idmanagement.gov/
[47] *See, e.g.,* NISTIR 7628, *Guidelines for Smart Grid Security, vol. 2, Privacy and the Smart Grid* (NIST, Aug. 2010), http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.
[48] *See* http://www.nist.gov/itl/biometrics/index.cfm.

Technology	Privacy Risks
collected or used for other purposes (e.g., medical, social, psychological, entertainment). Also see "Facial Recognition" above.	Government (e.g., criminal enforcement, immigration). Once compromised, the physical characteristic is generally impossible for an individual to change.
Bring Your Own Device (BYOD): The introduction and use of personally owned equipment (e.g., mobile devices, laptops, tablets) in a system or network enterprise for communications, processing, or storage.	• Equipment with insufficient, incompatible, or disabled security controls may expose and compromise data (e.g., PII of others) that the user communicates, processes, or stores on such a device.[49] • Personal data is potentially at risk of being deleted if the device must be wiped remotely or otherwise to protect agency work-product or data if the device is lost, stolen, or otherwise compromised. • User data could be subject to third-party electronic discovery and FOIA requests.[50]
Remote (shared) data storage and processing (e.g., "cloud" services)	• While such services may provide advantages of cost, security, and disaster recovery, service providers may not properly segregate sensitive data stored on behalf of the Government from data of other customers and may impose terms of service that do not provide adequate notice or other legal protections in the event of a security incident or breach or third-party litigation and raise issues regarding which law applies, i.e., conflicts of law. Cloud users may have limited rights to inspect or audit the service provider's compliance with applicable privacy or security controls and requirements, as well as its adherence to proper records management and disposal policies. • Cloud providers may aggregate multiple service functions (e.g., online air, travel, hotel booking on one site), thereby increasing the complexity of privacy risk management. Service providers could also attempt to analyze or use data stored for the Government in undisclosed and unauthorized ways.[51]

[49] *See supra* NIST SP 800-124, Rev. 1, sec. 2.2.2.

[50] *See* Federal CIO Council, *Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring your Own Device (BYOD) Programs* (Aug. 2012), http://www.whitehouse.gov/digitalgov/bring-your-own-device; *see generally supra* NIST SP 800-124, Rev. 1 (Draft) (Guidelines for Managing and Securing Mobile Devices in the Enterprise); *see* also NIST *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)*, NSIT SP 800-164 (Oct. 2012), http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[51] *See* NIST, *Guidelines on Security and Privacy in Public Cloud Computing,* SP 800-144 (Dec. 2011), http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf; Federal CIO Council and Chief Acquisitions Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service* (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

Table 3: Digital PII Checklist

This table identifies some common types of data potentially linked or linkable to individuals that may be collected, maintained, shared or used in the mobile and digital environment. It is not meant to be a complete or exhaustive list. Agencies may use it as a baseline to ensure they have identified all data that may constitute PII subject to applicable Federal laws, regulations, and policy, to determine the sensitivity (impact) level of that data (low, moderate, high) and to perform a PIA analysis.

	Data Type	Impact (L, M, H)
Personal Identifiers		
	Name	
	Social Security number	
	Drivers' license number	
	Credit card numbers	
	Other financial account numbers (bank, etc.)	
	Passport numbers	
	Other Government ID # or unique identifiers	
Contact information		
	E-mail address	
	Phone number	
	Postal address	
Other personal data		
	User names, avatars, etc.	
	Mother's maiden name	
	Birth date	
	Sex	
	Age	
	Other physical descriptors (eye/hair color, height, etc.)	
	Marital status/children/relatives	
	Sexual orientation	
	Race/ethnicity	
	Religion	
	Education	
	Employment	
	Citizenship	
	Health, insurance, treatment, or medical information	
	Criminal history	
	Other PII (e.g., in unstructured data fields completed by user)	

	Data Type	Impact (L, M, H)
Biometric identifiers and similar physical-based data		
	Signature	
	Fingerprints, handprints	
	Photo, scans (retinal, facial)	
	Voice	
	Physical movements (e.g., finger swipes, keystrokes)	
	DNA markers	
Device-based or -related data		
	User names	
	Passwords	
	Unique device identifier	
	Location/GPS data	
	Camera controls (photo, video, videoconference)	
	Microphone controls	
	Other hardware/software controls	
	Photo data	
	Audio/sound data	
	Other device sensor controls or data	
	On/Off status and controls	
	Cell tower records (e.g., logs, user location, time, date)	
	Data collected by apps (itemize)	
	Contact lists and directories	
	Biometric data or related data (see above)	
	SD card or other stored data	
	Network status	
	Network communications data	
	Device settings or preferences (e.g., security, sharing, status, etc.)	
Web site or platform-related data		
	Log data (e.g., IP address, time, date, referrer site, browser type)	
	Tracking data (e.g., single- or multi-session cookies, beacons)	
	Forms data	

Table 4: Suggested Digital PIA Questions

As explained earlier, a PIA must address: (1) what PII will be collected, maintained, or disseminated, including the nature and source of the data; (2) why the information is being collected (i.e., purpose); intended use or uses; (3) with whom will the information be shared or disclosed; (4) options and methods, if any, for individuals to exercise choice or give consent for collection or use; (5) how the information will be secured; and (6) whether a system of records is being created under the Privacy Act of 1974.

The following are traditional questions raised by a PIA with revisions as needed to reflect special issues raised in the digital and mobile environment. Agencies may wish to use the questions below that relate to their specific program or service to ensure that they have identified, considered, and addressed relevant privacy risks in the specific context of agency services and programs designed and developed for the digital and mobile environment.

Question	NIST SP 800-53, App. J Controls
Data Collected and Stored Within the System	
What PII will be collected, used, shared, or maintained by the digital service or program? (See Table 3)	SE-1 (Inventory of PII), DM-1 (Minimization of PII)
What specific types of PII could be collected, generated, compiled, used, maintained, or shared *by the agency*? (See Table 3)	DM-1 (Minimization of PII)
What specific types of PII could be collected, generated, compiled, used, maintained, or shared *by third parties*, including third parties hosting a program or service, third party mobile service providers, or others? (See Table 3)	DM-1 (Minimization of PII)
What options will be available for users of the digital service or program to minimize what information is collected, used, or shared about them?	DM-1 (Minimization of PII)
What will be the sources of the information in the service or program?	SE-1 (Inventory of PII), DI-1 (Data Quality)
Why will the information be collected, used, maintained, and/or shared by the agency? By the third parties?	AP-2 (Purpose Specification)
What specific legal authorities authorize the collection of the information?	AP-1 (Authority to Collect)
Access to and Sharing of the Data	
What individuals or entities might collect, access, use, or share such PII with the agency or others, and with whom will the information be shared? (See Table 1)	UL-1 (Internal Use), UL-2 (Information Sharing with Third Parties)
If the data will be shared, how will the data be accessed by, exposed, or transmitted to the third party?	UL-2 (Information Sharing with Third Parties)
Internally within the agency, do other systems have access to the PII, and if so, how will the privacy rights of individuals affected by the interface be protected?	UL-1 (Internal Use)

Question	NIST SP 800-53, App. J Controls
Will the service or program involve the use of tracking technologies or third-party sites that will compile or make data available to the agency?	IP-1 (Consent), TR-1 (Privacy Notice)
Will other entities or individuals supporting the service or program (e.g., app market, app developer, original equipment manufacturer, network or carrier, cloud storage provider, other host servers) use tracking technology or collect other information from or about individuals?	UL-2 (Information Sharing with Third Parties)
Could the service or program enable individuals or entities other than the sponsoring agency to determine an individual's location? Could such information compromise the physical safety of the individual or security of agency operations?	UL-2 (Information Sharing with Third Parties)
If data will be publicly released (e.g., data.gov) or used in de-identified form for testing, training or research, what is the risk that the data can be combined with other data either to identify the individual (if not currently identifiable) or used in ways that the individual did not intend?	DM-3 (Minimization of PII Used in Testing, Training & Research)
When individuals employed or retained by the Government are using non-Government devices to store, access, or process Government data (BYOD), what personal data might be collected or accessible by, or exposed to, the agency or to other entities or individuals? What, if any, protections exist to segregate personal from work information, to strengthen protection of agency data, and minimize agency collection and use of personal data?	UL-1 (Internal Use), UL-2 (Information Sharing with Third Parties)
When the Government must use or rely on a third-party site or service, what third-party terms of service or privacy policies may apply, and how will they be reconciled with applicable Federal law, regulations and policy? If required by law, has the third-party site or service owner agreed contractually to abide by the Privacy Act of 1974, FISMA, and other privacy and security rules?	UL-2 (Information Sharing with Third Parties), AR-3 (Privacy Requirements for Contractors and Service Providers)
What privacy and security risks are raised by an individual's choice of Internet connection, for example, if an individual uses an unsecured wireless connection for BYOD, or to use a Government program or service? To what extent will data be stored remotely (e.g., cloud) and what are the associated risks?	AR-2 (Privacy Impact and Risk Assessment)
Notice and Choice for Individuals	
What notice will be provided to individuals about the collection, use, sharing and other processing of their personal data and information about the agency's privacy program activities generally (e.g., how to reach the Senior Agency Official for Privacy (SAOP) and/or Chief Privacy Officer (CPO)?	TR-1 (Privacy Notice), TR-3 (Dissemination of Privacy Program Information)
How will privacy policies and notices required by Federal law, regulations, and policy be conveyed to users in a clear and conspicuous manner, before personal information is collected? Does such notice cover all contemplated or possible data uses, including public release, where appropriate?	TR-1 (Privacy Notice), TR-2 (System of Records Notice and Privacy Act Statements)

Question	NIST SP 800-53, App. J Controls
What opportunities will exist for an individual to decline to provide information or to consent to particular uses of the information? If opportunities exist, how will an individual grant consent?	IP-1 (Consent)
What device- or platform-based design options are available to provide individuals with the opportunity to choose how and when their data are collected, used, or shared?	IP-1 (Consent)
Data Retention	
What data retention periods apply to mobile or digital information collected from or about individuals under applicable law, regulations, and policy? In what form will the information be retained?	DM-2 (Data Retention & Disposal)
Can the agency control, modify, or determine how long data about individuals is retained by other entities and individuals involved in the design or provision of the agency's digital service or program (e.g., carrier, OEM manufacturer, app developer, app market, advertisers)?	DM-2 (Data Retention & Disposal)
What are the plans for destruction and/or disposition of the information?	DM-2 (Data Retention & Disposal)
Privacy Act, Access and Correction	
To what extent, if any, will data collected by the agency or its contractors about individuals constitute agency records (e.g., records subject to the agency's physical or legal control)?	TR-2 (System of Records Notice and Privacy Act Statements)
If the data are agency records, will the agency or its contractors, in maintaining, using, sharing, or disseminating them, retrieve such records by name or other assigned personal identifier (e.g., ID or control number, SSN), so that it is a "system of records" within the meaning of the Privacy Act? If so, identify (or, if needed, publish) the applicable Privacy Act system of records notice (SORN).	TR-2 (System of Records Notice and Privacy Act Statements)
If the records are subject to the Privacy Act, what online or offline procedures exist or must be newly developed to afford subject individuals with the access and correction rights afforded under that Act, and how will individuals be notified of such procedures?	IP-2 (Individual Access), IP-3 (Redress)
What online or offline mechanism(s) are or will be made available to individuals who wish to complain about how their mobile or digital data are collected or used?	IP-4 (Complaint Management)
Maintenance of Controls and Accountability	
While the information is retained in the system, what will the requirements be for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	DI-1 (Data Quality), DI-2 (Data Integrity & Data Integrity Board)

Question	NIST SP 800-53, App. J Controls
What controls will be in place to prevent the misuse of the information by those having authorized access and to prevent unauthorized access, use or disclosure of the information?	DI-2 (Data Integrity & Data Integrity Board)
Are all IT security requirements and procedures required by Federal law being followed to ensure that information is appropriately secured?	DI-2 (Data Integrity & Data Integrity Board)
How will the service or program monitor and audit privacy controls and internal privacy policy to ensure effective implementation? What technology will be used to audit and monitor for the security, appropriate use, and loss of PII?	AR-4 (Privacy Auditing and Monitoring)
Describe the privacy training provided to employees of the agency and employees of any third parties with access to sensitive mobile or digital information related to individuals. Include general training and training specifically relevant to the program or system.	AR-5 (Privacy Awareness & Training)
How will the service or program develop, disseminate, and update reports to demonstrate accountability with specific statutory and regulatory privacy program mandates?	AR-6 (Privacy Reporting)
What automated privacy controls will be integrated into the service or program's BYOD implementation to mitigate privacy risks to PII?	AR-7 (Privacy-Enhanced System Design and Development)
Privacy Incident Response	
If there is a data breach by the agency or a third-party involved in providing the Government program or service, what procedures will apply to ensure the agency and affected individuals are notified of the breach in a timely manner?	SE-2 (Privacy Incident Response)
If individuals must be notified of a breach, how will they be contacted, and who will determine the form, content, and timing of the notice?	SE-2 (Privacy Incident Response)
Other Privacy Risks and Mitigation	
What privacy risks are associated with the collection, use, dissemination and maintenance of the data and have not been addressed in this PIA? How have those risks been mitigated?	AR-2 (Privacy Impact & Risk Assessment)

Table 5: Elements of Digital Privacy Notice

Digital services or programs may trigger all or only some notice requirements. (For example, launching a Government mobile app may require a Privacy Act system of records notice, a Privacy Act statement, opt-in consent, and a PIA.) Consult your legal and privacy officials for guidance. Where notice requirements overlap, duplicative elements may be combined or omitted to shorten and condense the notice. The table below provides recommendations that can help agencies begin the process of drafting a digital privacy notice; agencies should consult existing laws, regulations, and policies for specific requirements.

Generally	
	Use plain language
	Be clear and specific (e.g., types of PII, purpose, intended uses and disclosures, retention periods)
	Display OMB clearance number, if OMB review required by Paperwork Reduction Act
	Comply with section 508 (handicap access), www.section508.gov
	Offer opt-in (not opt-out) for data collection, where feasible or if required (e.g., multi-session Web tracking technology that collects or maintains PII)
	Do not use notice to collect, use, share, or retain more data than necessary (data minimization)
Privacy Act Statement (Privacy Act of 1974, 5 USC 552a(e)(3))	
	Legal authority: What law(s), rules, etc., permit or require the data to be collected?
	Purpose: Why is the information being collected?
	Routine uses: How and when are data used and disclosed, and to whom?
	Mandatory or voluntary: Does the individual have a choice whether the data are collected or not?
	Effects or consequences: What happens to the individual if the data are not collected?
	Placement: Generally, at the point of data collection (e.g., on the electronic form used to collect the data), and provide a way that the individual can also print or access the statement (e.g., by URL). On Web sites, the Privacy Act statement may alternatively be provided by link and/or in the privacy policy.
System of Records Notice [SORN] (Privacy Act of 1974, 5 USC 552a(e)(4))	
	Name, location, security classification of the agency records system
	Categories of subject individuals
	Categories of records maintained about individuals
	Authority for maintaining the records
	System purpose(s)
	Routine use(s), including categories of users and purposes of use(s)
	Disclosure to consumer reporting agencies, if any
	Policies and practices for storage, retrievability, safeguards, retention/disposal
	System manager and address
	Procedures for notification, records access, and contesting accuracy of records

	Record source categories
	Exemption(s)
	Placement: Publish in *Federal Register*, after public comment and notice to OMB and Congress. Once final, make available on agency Web site, where feasible.
Web Site Privacy Policy (E-Gov Act, OMB M-03-22, M-99-18)	
	What PII is being collected
	Why is PII being collected (purpose)
	How will the agency use it (include PII in e-mail and Web form data)
	Security (generally identify controls for security, confidentiality, and safeguards against unauthorized access, harm)
	What information is automatically collected (e.g., IP addresses, time, date of visit) and why
	What PII is optional (voluntary)
	Consent mechanism: Explain how individuals may consent to specific uses of their PII, where use is not otherwise required or allowed by law (e.g., unsubscribe link, user account settings)
	Identify PII subject to the Privacy Act of 1974
	Individuals' rights under the Privacy Act of 1974 and/or other laws (e.g., to access and correct such PII). May meet this requirement by linking to applicable agency regulation or official summary of statutory rights.
	Web measurement and customization technology used by agency (see below)
	Social media and other third-party applications used by the agency (see below)
	COPPA requirements when collecting personal information from children under 13 (see below)
	Placement: Home page, links at other major entry points, pages that collect substantial PII
	Machine-readable by browsers (e.g., P3P)
	Must be clearly labeled as "Privacy Policy"
Use of Web Measurement and Customization Technologies (OMB M-10-22)	
	Purpose of the web measurement and/or customization technology
	Usage Tier, session type, and technology used
	Nature of the information collected
	Purpose and use of the information
	Whether and to whom the information will be disclosed
	Privacy safeguards applied to the information
	Data retention policy for the information
	Whether the technology is enabled by default or not and why
	How to opt-out of the web measurement and/or customization technology
	Statement that opting-out still permits users to access comparable information or services
	Identities of all third-party vendors involved in the measurement and customization process
	Placement: Notice must be part of Privacy Policy (see above) on agency's Web site. If Tier 3 (multi-session tracking + PII), must first solicit public comment on agency's Open Gov't page for 30 days.
	Annually: prepare and post compliance review at agency's Open Government page, for public comment

Social Media and Third-Party Applications (OMB M-10-23)	
	Statement or pop-up when a link leads to third-party Web site or nongovernment domain
	Appropriate branding to distinguish agency's activities from nongovernment actors
	Agency Privacy Policy must disclose: the specific purpose of the agency's use of the third-party Web sites or applications; how the agency will use PII that becomes available through the use of the third-party Web sites or applications; who at the agency will have access to PII; with whom PII will be shared outside the agency; whether and how the agency will maintain PII, and for how long; how the agency will secure PII that it uses or maintains; and what other privacy risks exist and how the agency will mitigate those risks. Agency Privacy Policy must also link to the third-party site or application privacy policy, where feasible.
	Agency Privacy Notice, where feasible, on the third-party site or application must: (1) explain that the Web site or application is not a Government Web site or application, that it is controlled or operated by a third party, and that the agency's Privacy Policy does not apply to the third party; (2) indicate whether and how the agency will maintain, use, or share PII that becomes available through the use of the third-party Web site or application; (3) explain that by using the Web site or application to communicate with the agency, individuals may be providing nongovernment third parties access to PII; (4) direct individuals to the agency's official Web site; (5) and direct individuals to the agency's Privacy Policy as described above. Notice must be displayed at all locations where PII might be made available to the agency.
	PIA must disclose: (1) the specific purpose of the agency's use of the third-party Web site or application; (2) any PII that is likely to become available to the agency through public use of the third-party Web site or application; (3) the agency's intended or expected use of PII; (4) with whom the agency will share PII; whether and how the agency will maintain PII, and for how long; how the agency will secure PII that it uses or maintains; what other privacy risks exist and how the agency will mitigate those risks; (5) and whether the agency's activities will create or modify a "system of records" under the Privacy Act of 1974. Make PIA publicly available (e.g., on agency Web site).
Privacy Impact Assessment [PIA] (E-Gov Act, OMB M-03-22)	
	What PII will be collected, maintained, or disseminated, including the nature and source of the data
	Why (i.e., purpose)
	Intended use or uses
	Sharing and disclosure (i.e., with or to whom)
	Options and methods for individual to exercise choice or give consent to collection or use
	Security
	Privacy Act status of the data
	Placement: Make publicly available (e.g., Web site)
Children's Online Privacy Protection Act (COPPA)	
	When collecting personal information from children under 13, seek parental consent
	Placement: on Web site, at point of information collection

Other	
	Health Insurance Portability and Accountability Act (HIPAA) and HI-TECH Act (protected health information)
	"Common Rule," including Institutional Review Boards (IRBs), for the protection of human test subjects, see 45 CFR Part 46 (HHS) —when seeking the test subject's informed consent, must describe the extent, if any, to which confidentiality of records identifying the subject will be maintained, and must maintain documentation of informed consent, except in certain cases
	Gramm-Leach Bliley Act (GLBA) (customer or consumer financial information)
	Statistical data (e.g., Census Title 13, CIPSEA, etc.)
	Tax
	Educational (e.g., Federal Educational Rights and Privacy Act (FERPA), 20 USC 1232g, 34 CFR Part 99)
	Employment/EEO
	Other