

1 NIST Special Publication 800-53 Workshop on Privacy Controls: Discussion Draft

3 1. Introduction

4 The Office of Management and Budget's July 2016 update to Circular A-130¹ has clarified that
5 federal agencies' obligations with respect to managing privacy risk and information resources
6 extends beyond managing compliance with privacy laws, regulations, and policies, and that
7 agencies must apply the NIST Risk Management Framework (NIST RMF) to their privacy
8 programs.² NIST's current guidance on risk management is predominantly focused on
9 information security. Agencies will need additional guidance on how to apply those practices
10 within the full context of privacy to more effectively meet their responsibilities under Circular A-
11 130.

12 Some guidance already exists in NIST Special Publication (SP) 800-53, Revision 4 *Security and*
13 *Privacy Controls for Federal Information Systems and Organizations*.³ NIST first released SP
14 800-53 in 2005 to provide guidance to agencies on applying a catalog of controls to manage
15 information security risks in accordance with the requirements of the Federal Information
16 Security Management Act (FISMA).⁴ As part of the fourth revision of SP 800-53 in 2013, NIST
17 added an Appendix J, which comprises a set of privacy controls drafted by an interagency
18 working group of privacy officers.⁵ For three years, federal agencies have had the opportunity to
19 integrate these privacy controls into their programs and learn about the benefits and challenges.
20 With the recent update to Circular A-130 and NIST's upcoming fifth revision to SP 800-53,⁶
21 there is an opportunity to provide improved guidance to agencies about privacy controls and their
22 role in federal agencies' privacy programs.

23 Two fundamental questions about how privacy should be addressed in the next version of SP
24 800-53 are:

- 25 a. Is the current organization of Appendix J around the Fair Information Practice
26 Principles (FIPPs) sufficient for addressing agencies' increased privacy risk
27 management responsibilities?

¹ Office of Management and Budget, Circular A-130: "Managing Federal Information as a Strategic Resource" (2016), {hereinafter known as Circular A-130}. Available at:

<https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>

² NIST SP 800-37 Rev 1 (2010), available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>.

³ NIST SP 800-53 Rev 4 (2013) {herein after known as SP 800-53, available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

⁴ Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.), available at: <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

⁵ SP 800-53, Pg. iv, "Acknowledgements", available at:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

⁶ More details on the NIST FISMA Implementation Project can be found here:

<http://csrc.nist.gov/groups/SMA/fisma/>

28 b. If changes are needed, what amendments would help agencies move beyond
29 simply assessing compliance with privacy laws and regulations?

30 NIST is partnering with the Department of Transportation (DoT) to host a workshop to review
31 the privacy controls currently housed in Appendix J and gather feedback from stakeholders on
32 what changes should be made in the fifth revision.

33 The purpose of this document is to stimulate discussion at the workshop, and prompt written
34 comments from stakeholders who cannot attend, about potential areas for improvement. This
35 discussion draft covers some of the present challenges around how privacy controls are currently
36 incorporated into SP 800-53 and provides potential options for improvement.

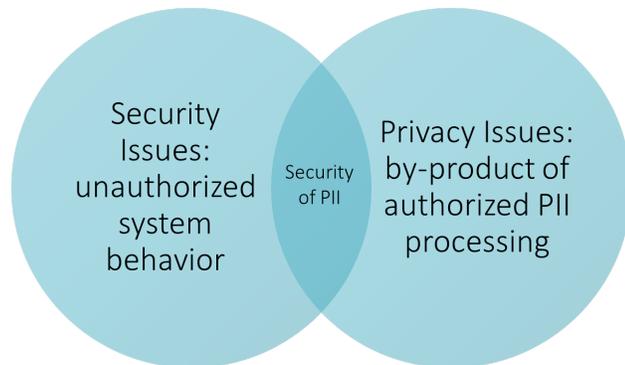
37

38 2. Challenges

39 NIST has engaged directly with many federal agency, academic, and private-sector practitioners
40 to explore aspects of effective privacy engineering practices and the challenges associated with
41 identifying and managing privacy risks.⁷ In this process, NIST has uncovered a number of key
42 challenges related to the process of selecting appropriate controls to mitigate privacy risks. These
43 challenges include: confusion about the differences between privacy and security goals and the
44 respective application of controls to achieve these goals; a need for integrated guidance on the
45 potential privacy risks arising from implementation of security controls; and the need for more
46 guidance on the application of technical measures to respond to privacy risk beyond the
47 reduction of data breaches. While this is not a comprehensive list of challenges that improving
48 the guidance in SP 800-53 could help to address, it frames many critical questions for
49 considering the scope that could best improve federal privacy practices.

50 2.1. Clarifying the Relationship Between Information Security and Privacy

51 Public discourse on the relationship
52 between security and privacy often
53 includes colloquial phrases such as
54 “security and privacy are two sides of a
55 coin” and “there is no privacy without
56 security.”⁸ In addition, security is
57 typically recognized as one of the FIPPs.⁹
58 As such, there is a clear recognition that



⁷ For more information, see the NIST Privacy Engineering page online at:
http://csrc.nist.gov/projects/privacy_engineering/index.html

⁸ For example, see “Data Privacy and Data Security; Two Sides of the Same Coin”, National Law Review, 2005, available at: <http://www.natlawreview.com/article/data-privacy-and-data-security-two-sides-same-coin-conversation-patrick-manzo-execut>; and “There is No Privacy Without Security”, F-Secure, 2015, available at: <https://business.f-secure.com/there-is-no-privacy-without-security/>

⁹ See Circular A-130 Appendix II: “Fair Information Practice Principles,” *infra* fn 1.

59 confidentiality of personally identifiable information (PII) plays an important role in the
60 protection of privacy.¹⁰

61 Nonetheless, there are issues in security that are unrelated to privacy (e.g., confidentiality of
62 trade secrets) and there are issues in privacy that are unrelated to security. For example, in the
63 energy sector, some communities have responded negatively to smart meters due largely to
64 concern that the nature of the information being collected can reveal people’s behavior inside
65 their homes, not from concerns that the utilities cannot keep the information secure.¹¹ Moreover,
66 even actions taken to protect PII can have privacy implications. For example, security tools to
67 prevent unauthorized access, such as persistent activity monitoring, can create concerns about the
68 degree to which information is revealed about individuals that is unrelated to cybersecurity
69 purposes. Existing information security risk models do not easily highlight privacy risks like
70 these that arise from information systems that are functioning in an authorized manner.

71 A clear understanding of the overlap and distinctions between privacy and information security
72 is necessary for agencies to be able to appropriately identify and assess different types of risk and
73 correspondingly select and implement appropriate controls. The description and cataloging of
74 controls can impact the effectiveness with which they can be selected and implemented to
75 address the relevant risks. A key consideration for this workshop will be determining if the
76 existing structure of Appendix J presents challenges for the selection of privacy controls in a risk
77 management process that extends beyond compliance, and what organizational changes, if any
78 could facilitate the selection and implementation of privacy and security controls to achieve
79 better outcomes for privacy.

80 **2.2. Understanding the Privacy Risks Associated with Security Controls**

81 As noted in section 2.1, privacy risks may arise from specific system design decisions. In
82 particular, measures that may be used to mitigate information security risks—such as system
83 monitoring or identity proofing—may have privacy implications. SP 800-53, Appendix F
84 provides guidance about how the security characteristics are improved (or diminished) in a
85 system by the implementation of a security control, but does not address how there may be the
86 potential for privacy risks arising from the implementation. Therefore, existing guidance does
87 not provide complete information about the consequences of using any given security control. If
88 agencies have such information, they may be able to tailor the implementation to optimize the
89 security benefit while minimizing the privacy risk.

¹⁰ See definition of PII in Circular A-130, *infra* fn 1.

¹¹ Chris Hooks, *As Towns Say No, Signs of Rising Resistance to Smart Meters*, New York Times, May 18, 2013, available at http://www.nytimes.com/2013/05/26/us/as-texas-towns-say-no-signs-of-rising-resistance-to-smart-meters.html?_r=0; Federico Guerrini, *Smart Meters: Between Economic Benefits and Privacy Concerns*, Forbes, June 1, 2014, available at <http://www.forbes.com/sites/federicoguerrini/2014/06/01/smart-meters-friends-or-foes-between-economic-benefits-and-privacy-concerns/>; Samuel J. Harvey, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. Rev. 2068, 2076-90 (2014), available at <http://www.uclalawreview.org/pdf/61-6-10.pdf>.

90 **2.3. Encouraging the Adoption of Privacy-Enhancing Technologies**

91 Of the three control catalogs in SP 800-53, Appendices F and G cover security controls, and
92 Appendix J covers privacy. Appendix F focuses on organization and system-level controls that
93 can be applied to mitigate information security risks. Appendix G catalogs program management
94 controls that can be applied across organizations to broadly affect information security.¹² The
95 combination of Appendix F and G offer organizations a broad selection of detailed system-
96 specific, hybrid, and common controls to choose from in order to mitigate information security
97 risks.¹³ In comparison to the security catalogs,
98 many of the controls in Appendix J are more akin
99 to the common, program management controls
100 listed in Appendix G than the broader range of
101 controls described in Appendix F.

102 Although the controls are intended to be
103 technology and policy-neutral, the supplemental
104 guidance in Appendix F provides much more
105 information about the application of technical
106 measures than the guidance provided in Appendix
107 J. This difference facilitates an artificial divide in
108 federal privacy practice: privacy is overly
109 perceived as the domain of policy and legal
110 practitioners, while information security is
111 understood to be managed more comprehensively
112 across policy and technical personnel.

113 Part of the value of the SP 800-53 security control
114 catalogs is how they aid system engineers in
115 understanding places in systems where technical
116 measures could be applied. If much of the privacy
117 guidance is primarily oriented around policy
118 measures, agencies are missing an important
119 vehicle for increasing their ability to apply
120 technical measures to facilitate the mitigation of
121 privacy risk.

122 The context for system design also can impact the
123 use of privacy-enhancing technologies. NIST has

**Control Catalogs in SP 800-53,
Revision 4**

Appendix F: The Security Control Catalog - Safeguards and countermeasures for organizations and information systems to address information security.

Appendix G: Information Security Programs – Complement the security controls in Appendix F and focus on the programmatic, organization- wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

Appendix J: Privacy Control Catalog - Administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.

¹² The information security program management controls described in Appendix G are typically implemented at the organization level and not directed at individual organizational information systems. The program management controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. See Appendix G, SP 800-53.

¹³ For more information about control designations, see SP 800-53, Pg. 14, Section 2.4

124 introduced a set of privacy engineering objectives (predictability, manageability, and
125 disassociability) in the draft NISTIR 8062 to better enable the development of system
126 capabilities that support agency privacy policies and requirements.¹⁴ Consideration of how
127 controls can be applied to support system capabilities could expand thinking about how privacy-
128 enhancing technologies could be used to address privacy risks and strengthen policy-based
129 measures. These privacy engineering objectives could help system engineers take into account
130 the types of controls that support privacy when the system is functioning in an authorized
131 manner, which may be overlooked in the focus on controls used to attain systems with
132 confidentiality, integrity, and availability.

133 Privacy is an interdisciplinary challenge and requires a broad set of contributors to identify and
134 mitigate risks, but the current control catalog could better support agencies' ability to understand
135 how to design systems that prevent privacy problems from occurring. In order to increase
136 agencies' adoption of privacy-enhancing technologies, workshop participants may consider
137 whether privacy engineering objectives are a useful organizing construct, as well as whether the
138 guidance could be expanded to support more use of technical measures to achieve better
139 outcomes for privacy.

140 **2.4. Overlapping Controls**

141 There are certain information security controls—and in some cases, control families—that could
142 apply directly to privacy practices. For example, the Audit and Accountability (AU) control
143 family in Appendix F includes many detailed controls for fulfilling audit requirements that are
144 also applicable to privacy. Therefore, is it necessary to maintain a separate control family on
145 “Accountability, Audit, and Risk Management” (AR) in Appendix J? Additionally, many of the
146 controls listed in Appendix J have direct parallels in the program management (PM) control
147 family in Appendix G – including several of the AR controls. Do these distinctions have
148 important benefits or do they create challenges for integrated implementation? These questions
149 illustrate how Appendix J creates some ambiguity about the roles involved in deploying privacy
150 controls. These issues could be clarified to facilitate more effective, interdisciplinary
151 collaboration in agencies.

152

¹⁴ Draft NISTIR 8062: Privacy Risk Management for Federal Information Systems, May 2015:
http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

153 **3. Considerations for Changes to NIST SP 800-53, Rev 4**

154 SP 800-53, revision 5 could better support agencies' alignment with the increased privacy risk
155 management expectations articulated in Circular A-130. These changes could reorient the
156 document to demonstrate more integrated, interdisciplinary processes for managing privacy and
157 result in more effective privacy programs as well as more effective enterprise risk management.
158 These changes would primarily impact Appendixes F, G, and J – though some explanatory
159 changes may be needed in the body of the document to reflect these alterations.

160 The organizational structure of 800-53 control families includes: 1) controls, 2) control
161 enhancements, and 3) supplemental guidance, in addition to references. This structure provides a
162 number of opportunities for modifications.

163 **3.1 Control Families**

164 As noted in sections 2.1 and 2.3, control families should support effective privacy risk
165 management in accordance with Circular A-130, and enable agencies to make more use of
166 privacy-enhancing technologies in system design. Considering how existing control families are
167 organized as well as creating new control families or controls could offer federal agencies insight
168 into how to utilize the benefits (and understand the limitations) of technical measures as well as
169 facilitate the application of the NIST RMF in privacy programs.

170 **3.1.1 Security Controls**

171 For certain security control families, there is an opportunity to add new controls to address
172 privacy risks that are not currently addressed by the existing security-focused controls. One
173 example is the awareness and training (AT) control family. An additional control specifically
174 for privacy training would complement the existing five controls and support agencies'
175 development of a more integrated training program.

176 **3.2 Control Enhancements**

177 In some control families, new controls may not be necessary because the existing controls apply
178 to both the security and privacy fields. In these cases, control enhancements might be a more
179 appropriate place to address privacy risks. Control enhancements provide alternative
180 implementations for controls that may be necessary depending on enhanced baseline security
181 needs or other contextual factors surrounding the system. Some are optional, and some are
182 required, as indicated in the baseline allocations. An example of where additional privacy-
183 focused control enhancements could be beneficial is the Identification and Authentication (IA)
184 control family. The second control, "Identification and Authentication (organizational users),"
185 provides thirteen control enhancements focused on security. Adding pseudonymous
186 authentication to these control enhancements could offer a privacy-enhancing option.

187 **3.3 Supplemental Guidance**

188 SP 800-53 uses supplemental guidance to assist agencies in implementing the relevant controls.
189 By adding more privacy-specific supplemental guidance in Appendix F, there is an opportunity
190 to note privacy considerations that are relevant to, or arise from, security controls. This is

191 particularly beneficial in control families that do not need any substantial edits, since they
192 already could apply across both the security and privacy fields. The Audit and Accountability
193 (AU) family, for example, highlights a variety of controls that are not security-specific. Rather
194 than add any additional controls or control enhancements, supplemental privacy guidance could
195 demonstrate to agencies how the control family is meant to enhance both the security and
196 privacy of an information system, and provide important privacy considerations. AU-11, “Audit
197 Record Retention,” is another control that may warrant supplemental privacy considerations to
198 ensure that data containing personal information is only retained as long as necessary for the
199 audit process, and only the most necessary information is retained at all. Supplemental guidance
200 could make clear the risks of over-retention in audit logging, and assist agencies in balancing
201 their needs for security assurances with potential privacy risks.

202

203 **4. Comment Facilitation**

204 NIST will use the following questions to facilitate discussion during breakout sessions at the
205 September workshop. Written comments are also welcome and may be submitted to
206 privacyeng@nist.gov until September 30, 2016. Output from the September workshop and
207 written comments will contribute to the process of the fifth revision of SP 800-53.

208 **4.1 Benefits and Challenges:**

209 (i) What are some of the current benefits of Appendix J? In particular, what are some
210 benefits of how privacy controls are currently integrated into SP 800-53?

211 (ii) What are some of the current challenges with Appendix J? In particular, what are
212 some challenges with how privacy controls are currently integrated into SP 800-53?

213 **4.2 Overlapping Controls:**

214 (i) How should overlapping controls be managed in the next revision of SP 800-53?

215 (ii) Are there benefits to maintaining similar controls in distinct security and privacy
216 families?

217 **4.3 Control Enhancements:**

218 (i) Should control enhancements in the security control families be used to address
219 risk mitigation for privacy?

220 **4.4 Supplemental Guidance:**

221 (i) Should supplemental guidance for the security controls be used to provide more
222 detail about the potential privacy risks associated with the deployment of a given
223 control?

224 (ii) Should supplemental guidance for the security controls be used to provide more
225 detail about the potential privacy benefits associated with the deployment of a given
226 control?

227 **4.5 Categorization:**

228 (i) Are there stand-alone privacy controls that should be categorized as program
229 management controls? Should they be integrated into Appendix G so that all program
230 management controls are located in one place in 800-53?

231 (ii) If security controls also contribute to protecting privacy, should the remaining
232 stand-alone privacy controls in Appendix J be categorized as “data governance”
233 controls (or another label)?

234 **4.6 Additional Questions:**

235 (i) On balance, should privacy controls and security controls continue to be integrated
236 into one document?

237 (ii) Are there any other changes that should be considered?