Privacy Risk Management for Federal Information Systems

#### Editors:

*Sean Brooks Ellen Nadeau*

#### Authoring Committee:

*Michael Garcia Naomi Lefkovitz Suzanne Lightman*



Privacy Risk Management for Federal Information Systems

#### Editors:

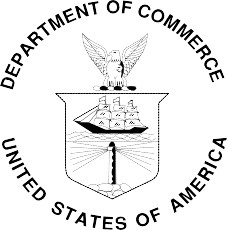
*Sean Brooks Ellen Nadeau*

#### Authoring Committee:

*Michael Garcia Naomi Lefkovitz Suzanne Lightman*

*Information Technology Laboratory, NIST*

May 2015



U.S. Department of Commerce

*Penny Pritzker, Secretary*

National Institute of Standards and Technology

*Willie May, Under Secretary of Commerce for Standards and Technology and Director*

1. National Institute of Standards and Technology Internal Report 8062
2. 64 pages (May 2015)

3

4

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at [http://csrc.nist.gov/publications.](http://csrc.nist.gov/publications)

5

6

7

8

9

10

11

12

13

14

15

16

17

1. National Institute of Standards and Technology
2. Information Technology Laboratory
3. 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899‐8930
4. Email: [privacyeng@nist.gov](mailto:privacyeng@nist.gov)

22

23

24

25

26

27

28

29

30

31

32

33

1. **Reports on Computer Systems Technology**
2. The Information Technology Laboratory (ITL) at the National Institute of Standards and
3. Technology (NIST) promotes the U.S. economy and public welfare by providing
4. technical leadership for the Nation’s measurement and standards infrastructure. ITL
5. develops tests, test methods, reference data, proof of concept implementations, and
6. technical analyses to advance the development and productive use of information
7. technology. ITL’s responsibilities include the development of management,
8. administrative, technical, and physical standards and guidelines for the cost-effective
9. security and privacy of other than national security-related information in federal
10. information systems.

44

45

46

47 **Abstract**

48

1. This document describes a privacy risk management framework for federal information
2. systems. The framework provides the basis for the establishment of a common
3. vocabulary to facilitate better understanding of and communication about privacy risks
4. and the effective implementation of privacy principles in federal information systems.
5. This publication focuses on the development of two key pillars to support the application
6. of the framework: privacy engineering objectives and a privacy risk model.

55

56

57

58

59 **Keywords**

60

61 Privacy; Information Security; Risk Management; Cybersecurity; Computer Security

62

63

64

65

66 Acknowledgements

67

1. The authors wish to thank the following individuals for participating in the preparation of
2. this document: James Dever, Simson Garfinkel, Meredith Jankowski, and Colin Soutar.
3. The authors also greatly appreciate the NSTIC pilots’ generous contribution of time and
4. insights.

72

73

74

75

76

77

[78](#_bookmark0)

# Table of Contents

* 1. **EXECUTIVE SUMMARY** **1**
  2. **1. INTRODUCTION** **3**
  3. PURPOSE 3
  4. SCOPE 3
  5. AUDIENCE 4
  6. DOCUMENT ORGANIZATION 5
  7. BACKGROUND 6
  8. **2. RISK MANAGEMENT & ITS APPLICABILITY TO PRIVACY** **12**
  9. [**3. NIST PRIVACY RISK MANAGEMENT FRAMEWORK** **15**](#_bookmark2)
  10. SYSTEM OBJECTIVES IN CYBERSECURITY RISK MANAGEMENT 17
  11. PRIVACY ENGINEERING OBJECTIVES 18
  12. A PRIVACY RISK MODEL 22
  13. **4. NEXT STEPS** **27**
  14. **APPENDICES** **28**
  15. APPENDIX A: GLOSSARY 29
  16. APPENDIX B: ACRONYMS 30
  17. APPENDIX C: FORMAL MATHEMATICAL STATEMENT OF THE PRIVACY RISK MODEL 31
  18. APPENDIX D: PRIVACY RISK ASSESSMENT METHODOLOGY 32
  19. APPENDIX E: CATALOG OF PROBLEMATIC DATA ACTIONS 54
  20. APPENDIX F: CATALOG OF PROBLEMS FOR INDIVIDUALS 55
  21. APPENDIX G: CATALOG OF CONTEXTUAL FACTORS 56
  22. APPENDIX H: REFERENCES 57

102

103

104 Executive Summary

105

1. NIST research in several areas of information technology – including cybersecurity,
2. Smart Grid, cloud computing, big data, and cyber-physical systems – improves the
3. products and services that bring great advancements to U.S. national and economic
4. security and our quality of life. Notwithstanding their benefits, public awareness about
5. these technologies and their potential impact on individuals’ privacy and societal values
6. continues to grow. This publication lays the groundwork for greater understanding of
7. privacy impacts and the capability to address them in federal information systems
8. through risk management.

114

1. Federal agencies need methods that yield repeatable and measurable results if they are to
2. be able to implement privacy protections in information systems in a consistent manner.
3. Although existing tools such as the Fair Information Practice Principles (FIPPs) and
4. privacy impact assessments (PIAs) provide a foundation for taking privacy into
5. consideration, they have not yet provided a method for federal agencies to measure
6. privacy impacts on a consistent and repeatable basis.

121

1. In other domains such as cybersecurity, safety, and finance, risk management has played
2. a key role in enabling agencies to achieve their mission goals while minimizing adverse
3. outcomes. NIST has successfully developed frameworks to assess risk, including the
4. management of cybersecurity risk through the Risk Management Framework (RMF).
5. Modeled after the RMF, this publication introduces a privacy risk management
6. framework (PRMF). In developing the PRMF, NIST sought the perspectives and
7. experiences of privacy experts across a variety of sectors in an open and transparent
8. process, including hosting workshops and public comment periods and engaging
9. stakeholders in various outreach activities.

131

1. The PRMF provides the basis for the establishment of a common vocabulary to facilitate
2. better understanding of, and communication about, privacy risks and the effective
3. implementation of privacy principles in federal information systems. In particular, this
4. publication focuses on the development of two key pillars to support the application of
5. the PRMF: privacy engineering objectives and a privacy risk model.

137

1. Privacy engineering objectives can play an important role in bridging the gap between an
2. agency’s goals for privacy and their manifestation in information systems. NIST has
3. developed three privacy engineering objectives – *predictability, manageability, and*
4. *disassociability* – for the purpose of facilitating the development and operation of
5. privacy-preserving information systems. These objectives are designed to enable system
6. designers and engineers to build information systems that implement an agency’s privacy
7. goals and support the management of privacy risk.

145

1. A critical aspect of risk management is a risk model that enables the ability to identify
2. risk. Risk is often expressed as a function of the likelihood that an adverse outcome
3. occurs multiplied by the magnitude of the adverse outcome should it occur. This
4. publication examines this conception of risk and how it can be expressed in terms that
5. facilitate improved identification and management of privacy risk. To aid agencies in
6. using the PRMF and to apply the privacy risk model, NIST has developed an initial set of
7. worksheets, collectively referred to as the Privacy Risk Assessment Methodology
8. (PRAM). This document describes the inputs to the PRAM, and provides examples for
9. agencies to follow when applying the PRAM to their own systems.

155

1. Future areas of work in privacy risk management will focus on improving the application
2. of controls – policy, operational, and technical – to mitigate risks identified with the
3. PRMF. To facilitate this research, NIST will continue to request feedback to refine the
4. privacy engineering objectives and the privacy risk equation, and to develop additional
5. guidance to assist agencies in determining the likelihood and impact of privacy risks. The
6. research process will continue to be an open and transparent process that will solicit input
7. from federal agencies, academic institutions, private organizations, and civil society
8. organizations in order to develop guidance that reflects the best practices for addressing
9. privacy risks.

165

166 1. Introduction

167

1. NIST research in information systems has identified the value of measurable and
2. repeatable methods for anticipating and addressing risks in the use of information
3. technology. Among these risks are those involving individuals’ privacy. This publication
4. lays the groundwork for greater understanding of privacy impacts and the capability to
5. address them in federal information systems through risk management.

173

174 Purpose

175

1. This publication introduces a privacy risk management framework (PRMF) for
2. anticipating and addressing privacy risk that results from the processing of personal
3. information in federal information technology systems. In particular, this publication
4. focuses on the development of two key pillars to support application of the PRMF:
5. privacy engineering objectives and a privacy risk model. In so doing, it lays the
6. foundation for the establishment of a common vocabulary to facilitate better
7. understanding of, and communication about, privacy risks and the effective
8. implementation of privacy principles in federal information systems.

184

1. The set of privacy engineering objectives defined in this document provides a conceptual
2. framework for engineers and system designers to bridge the gap between high-level
3. principles and implementation. The objectives are intended to support privacy risk
4. management by facilitating consistent, actionable, and measurable design decisions.

189

1. The privacy risk model aims to provide a repeatable and measurable method for
2. addressing privacy risk in federal information systems. The model defines an equation
3. and a series of inputs designed to enable (i) the identification of problems for individuals
4. that can arise from the processing of personal information and (ii) the calculation of how
5. such problems can be reflected in an organizational risk management approach that
6. allows for prioritization and resource allocation to achieve agency missions while
7. minimizing adverse events for individuals and agencies collectively.

197

198 Scope

199

1. This publication covers the assessment of privacy risk arising from the processing of
2. personal information within and among information systems. The PRMF is intended to
3. aid agencies in identifying and prioritizing risk so they can implement the appropriate
4. mitigations. It provides system objectives to facilitate privacy engineering, a common
5. vocabulary, and a risk equation for assessing privacy in information systems.1

205

1. The PRMF described herein does not address the processing of personal information
2. outside of information systems. It also does not examine specific controls or their
3. applicability to specific privacy risks. A future document will explore in greater detail
4. controls that an agency could use to mitigate privacy risk in information systems.

210

211 Audience

212

1. Addressing privacy is a cross-organizational challenge that requires agencies to use a
2. common language to describe privacy risk and the objectives they wish to pursue in order
3. to manifest privacy protections within the information systems they manage. This
4. document provides a common vocabulary for these discussions, as well as some
5. preliminary tools for estimating privacy risk. Thus, the audience for this document is all
6. positions involved in the development of information systems, the evaluation of privacy
7. risk in such systems or risk management in general, including:

220

1.  Individuals with privacy and/or information system oversight responsibilities
2. (e.g., senior agency officials for privacy, chief information officers, agency
3. heads);
4.  Individuals with privacy implementation and operational responsibilities in
5. information systems (e.g., mission/business owners, information system owners,
6. information owners/stewards, system administrators, information system security
7. officers);
8.  Individuals with system engineering and design responsibilities (e.g., program or
9. project managers, system engineers, chief architects); and
10.  Individuals with oversight and/or accountability responsibility for privacy (e.g.,
11. inspectors general, internal auditors).

232

1 Privacy engineering is an emerging field, but currently there is no widely-accepted definition of the discipline. For the purposes of this publication, privacy engineering is a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within information systems.

##### 233 Document Organization

234

235 This publication is organized as follows:

236

1. The remainder of **Chapter 1** explains the need for a privacy risk management framework
2. by reviewing current concerns about the impact of information technologies on
3. individuals’ privacy, existing tools to address privacy protection and their challenges, and
4. NIST privacy engineering research to date.
5. **Chapter 2** explores the use and benefits of risk management in cybersecurity, and
6. discusses its relevance to the privacy field.
7. **Chapter 3** introduces the privacy risk management framework. It defines three privacy
8. engineering objectives and a privacy risk model expressed as a privacy risk equation. It
9. introduces a privacy risk assessment methodology based on the equation to enable federal
10. agencies to identify and calculate privacy risk in their systems.
11. **Chapter 4** explains the next steps for privacy risk management work at NIST. It stresses
12. the importance of continued research in the field of privacy engineering and the need for
13. more guidance on the application of controls to mitigate privacy risk.
14. This document also includes eight appendices:
15.  Appendix A is a glossary of terms used throughout this document;
16.  Appendix B is a list of acronyms used throughout this document;
17.  Appendix C provides a formal mathematical statement of the privacy risk model;
18.  Appendix D contains a set of worksheets and illustrative data maps that comprise
19. the privacy risk assessment methodology;
20.  Appendix E is a catalog of problematic data actions for use with the privacy risk
21. assessment methodology;
22.  Appendix F is a catalog of problems for individuals for use with the privacy risk
23. assessment methodology; and
24.  Appendix G is an illustrative set of contextual factors for use with the privacy risk
25. assessment methodology;
26.  Appendix H includes a list of references used throughout the document.

263

##### Background

1. *Defining the need*

266

1. NIST research in several areas of information technology – including cybersecurity,
2. Smart Grid, cloud computing, big data, and cyber-physical systems – improves the
3. products and services that bring great advancements to U.S. national and economic
4. security and our quality of life. Notwithstanding their benefits, public awareness about
5. these technologies and their potential impact on individuals’ privacy and societal values
6. continues to grow.

273

1. For example, during its work with Smart Grid technology, NIST and its partners in the
2. electricity sector have noted that there are significant privacy implications. “While many
3. of the types of data items accessible through the smart grid are not new, there is now the
4. possibility that other parties, entities or individuals will have access to those data items;
5. and there are now many new uses for and ways to analyze the collected data, which may
6. raise substantial privacy concerns.”2 Energy data and personal information collected by
7. smart grids “can reveal something either explicitly or implicitly about individuals, groups
8. of individuals, or activi[ties of those individuals.”3](#_bookmark1)

282

1. Other examples of emerging technologies in which the federal government is facing
2. privacy concerns are cyber-physical systems (CPS) and the Internet of Things (IoT). IoT
3. and CPS will have major impacts in areas such as transportation, medicine, critical
4. manufacturing, and energy. The public working groups that NIST has convened on CPS
5. and big data included privacy as a major research area.4

288

1. Many of these issues converge in the particular privacy challenges governments are
2. confronting as they implement “smart city” technologies, such as managed traffic flow
3. and automated ticketing (i.e. red light and speed cameras) that can collect information
4. about people through “government-operated sensors and surveillance technologies
5. increasingly deployed throughout their environs.”5 Use, retention, and storage of this type
6. of data have raised citizen concerns about privacy infringement.6

2 NIST Interagency Report 7628R1 “Guidelines for Smart Grid Cybersecurity*,*: Volume *II*, p.2 – Privacy and the Smart Grid,” (SEPT 2014) at 7, *available at*  <http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>[hereinafter NISTIR 7628R1].

3 *Id.* at 25.

4 *See* “Cyber-Physical Systems Public Working Group Workshop,” NIST Homepage, accessed May 19, 2015, *available at* <http://www.nist.gov/cps/cps-pwg-workshop.cfm>; NIST Special Publication 1500-4, “DRAFT NIST Big Data Interoperability Framework: Volume 4, Security and Privacy,” (APRIL 2015)

*available at* <http://bigdatawg.nist.gov/_uploadfiles/M0395_v1_4717582962.pdf>

5 Kelsey Finch and Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected*

*Town*, 41 Fordham Urban L. J. 1581, 1595 (2015), *available at*

<https://www.dropbox.com/s/nw1nbf1uj6kq2zw/Finch%20-%20Tene_Cities.pdf?dl=0>.

6 For discussions regarding the myriad privacy issues involved in “smart city” technologies, *see* Nicole Perlroth, *Smart City Technology May Be Vulnerable to Hackers*, NY Times, Apr. 21, 2015, *available at*

<http://bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers>/; Reid Wilson, *Red-light Cameras Under Scrutiny In State Legislatures*, Wash. Post, Feb. 7, 2014, *available at*

295

1. As NIST conducts research in these and other information technologies and federal
2. agencies deploy them, it is critical to understand the potential impacts for privacy, so that
3. they can be addressed. Doing so will enable the optimization of the benefits of these
4. technologies while maintaining core values provided by the protection of individuals’
5. privacy.

301

302 *Existing Privacy Tools and Challenges*

303

1. As a result of these ubiquitous privacy concerns, NIST guidelines and reports
2. increasingly feature privacy considerations.7 To date, these efforts to address privacy
3. have generally been based on privacy principles such as the Fair Information Practice
4. Principles (FIPPs).8 Principles such as the FIPPs have helped many organizations develop
5. baseline considerations for the protection of individuals’ privacy as new technologies
6. enter the marketplace. Nonetheless, there are ongoing debates about the adaptability of
7. these principles to new technologies.9

311

1. These debates may have less to do with the FIPPs as concepts of enduring value and
2. more to do with the metaphorical problem of forcing a square peg into a round hole. That
3. is, agencies need methods that yield repeatable and measurable results if they are to be
4. able to implement privacy protections in information systems on a consistent basis. There
5. are a number of reasons why the FIPPs, notwithstanding their conceptual value, do not
6. have the characteristics of a repeatable and measurable methodology. One is that there

<http://www.washingtonpost.com/blogs/govbeat/wp/2014/02/07/red-light-cameras-under-scrutiny-in-state>- legislatures/; Luke Broadwater, *City Surveillance Camera System to Expand*, Baltimore Sun, July 21, 2012, *available at* <http://articles.baltimoresun.com/2012-07-21/news/bs-md-ci-private-cameras>- 20120721\_1\_security-cameras-crime-cameras-citiwatch-system; Jay Stanley, *Extreme Traffic Enforcement*, American Civil Liberties Union, May 24, 2012, *available at* <https://www.aclu.org/blog/extreme-traffic>- enforcement; and Phineas Baxandall, *New Report Outlines Problems with Red-Light and Speed Cameras*, The Federation of Public Research Interest Groups, Oct. 27, 2011, *available at* <http://www.uspirg.org/trafficcamreport>.

7 *See e.g.,* NISTIR 7628R1, *supra* Note 2; NIST Special Publication 800-53R4 “Security and Privacy Controls for Federal Information Systems and Organizations,” (APR 2013), *available at*

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>; and NIST “Framework for Improving Critical Infrastructure Cybersecurity,” (FEB 2014) *available at* <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

8 The FIPPs first appeared in a 1973 report by the U.S. Department of Health, Education, and Welfare and

addressed privacy concerns arising from the increasing digitization of data. *See* “Records Computers and the Rights of Citizens,” at 41-42, *available at* <http://www.justice.gov/opcl/docs/rec-com-rights.pdf>. After publication, the FIPPs became influential in shaping privacy law in the United States and around the world. Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy* 114 Colombia L. Rev. 583, 592 (2014), *available at* <http://columbialawreview.org/wp-content/uploads/2014/04/Solove>- Hartzog.pdf. The FIPPs were embodied in the Privacy Act of 1974, 5 U.S.C. § 552a, *available at* <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII>- sec552a.pdf.

9 Executive Office of the President, “Big Data: Seizing Opportunities, Preserving Values,” (MAY 2014), at 21, *available at*

<https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

1. can be wide-ranging interpretations about their meaning. For instance, the transparency
2. FIPP can be treated as a requirement that mandates that individuals be provided with
3. specific notices about the collection and use of their information. In other instances,
4. transparency is more akin to a value statement about the importance of open processes.
5. Another important reason is that the application of the FIPPs is centered on the purpose
6. or reason that personal information is being used. Since the purpose could be broad, a
7. FIPP such as data minimization does not inherently assist an agency in determining
8. which information should be minimized to mitigate risk.10 Additionally, the FIPPs are
9. usually treated as a unified set even though they may operate at different levels of the
10. organization. For example, the accountability and auditing FIPP constitutes concepts that
11. are generally applicable to a number of policy domains, not just privacy, and which are
12. typically considered as part of an overall organizational governance framework, not
13. necessarily at the systems engineering level. Thus, for system engineers, the FIPPs, on
14. their own, do not offer a consistent methodology that yields repeatable results for the
15. protection of privacy.

333

1. The National Strategy for Trusted Identities in Cyberspace (NSTIC) is one example of an
2. initiative that demonstrates both the value of the FIPPs and their challenges.11 The
3. NSTIC acknowledged that federated identity solutions could create risks for individuals’
4. privacy and civil liberties as such solutions could increase the capability for tracking and
5. profiling of online transactions.12 It calls for a holistic implementation of the FIPPs to
6. enable a privacy-enhancing identity ecosystem.13 NIST has awarded grants to pilots that
7. demonstrate alignment with the guiding principles laid out in the NSTIC.14 The pilots’
8. use of the FIPPs has generally resulted in solutions that improve individual notice and
9. consent, data security, and policy-based use limitations.15 However, they lag in
10. identification of the risks around tracking and profiling created by architectural design
11. choices or selection of technical controls to mitigate such risks.16 Thus, these pilots have
12. often sought help from NIST in conducting privacy evaluations and assessments of their
13. risk for both internal and external reporting purposes.

347

10 The FIPPs are not a risk-based framework because they do not frame privacy harms according to the actual impact on individuals. *See* Stuart S. Shapiro, PhD., “Situating Anonymization Within a Privacy Risk Model,” Homeland Security Systems Engineering and Development Institute (2012) at \*2, *available at*  <https://www.mitre.org/sites/default/files/pdf/12_0353.pdf>.

11 *See generally* “National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy,” (APR 2011), *available at*

<https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf>.

12 *Id.* at 3.

13 *Id.* at 12.

14 “Catalyzing the Marketplace: NSTIC Pilot Program,” NSTIC Homepage, accessed May 19, 2015,

*available at* <http://www.nist.gov/nstic/pilots.html>.

15 NIST Internal Report 8054 “NSTIC Pilots: Catalyzing the Identity Ecosystem,” (APR 2015), *available at*

<http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8054.pdf>.

16 To address this issue and other challenges associated with the NSTIC principle of privacy enhancing identity solutions, NIST announced its Federal Funding Opportunity in March 2015, *available at*

<http://www.nist.gov/nstic/NSTIC-Privacy-Pilot-FFO-03-2015.pdf>.

1. Agencies, because they are required to implement privacy impact assessments (PIAs)
2. under the E-Government Act of 2002, have the basis for a tool to facilitate repeatable and
3. measurable privacy protections in their systems.17 In practice though, PIAs have not
4. achieved their full potential as a process for assessing and understanding (and therefore
5. anticipating) privacy concerns in information systems.18 Where agencies focus largely on
6. using them to support regulatory compliance, it can be difficult to translate the
7. information in PIAs into actionable technical design recommendations. Enabling
8. agencies to better define privacy risk and system objectives for privacy could expand the
9. utility of PIAs and their benefits as a tool for addressing privacy concerns in federal
10. information systems.

358

359 *New Tools to Address the Challenges*

360

1. The FIPPs and other related principles remain an important part of an overall privacy
2. protection framework.19 However, experiences with the NSTIC pilots and other NIST
3. efforts have demonstrated that although principles can provide important considerations
4. for policy development, they need to be supplemented with additional tools that facilitate
5. repeatable and measurable methods for identifying, prioritizing, and mitigating privacy
6. problems. Given the lack of such tools, NIST determined that developing a consistent
7. process for addressing privacy concerns in information systems would be beneficial for
8. internal NIST work and federal agency missions.

369

1. Other disciplines (e.g., cybersecurity, safety, finance) have successfully used risk
2. management approaches to unify multiple organizational inputs and drive toward a
3. common assessment of challenges and identification of solutions.20 NIST has
4. successfully developed frameworks to assess risk in a variety of disciplines, including the
5. cybersecurity risk management model, which particularly informed the approach

17 The E-Government Act of 2002 is codified at 44 U.S.C. § 101, *available at*

<http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm>.

18 For instance, in the healthcare context, the Centers for Medicare & Medicaid Services developed and documented PIAs yet did not assess the risks associated with the handling of PII or identify mitigating

controls to address such risks. United States Government Accountability Office “Healthcare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls,” (SEPT 2014), at 44, *available at* <http://www.gao.gov/assets/670/665840.pdf>.

19 *See e.g.*, Privacy by Design principles, Ann Cavoukian, PhD., et al., “Privacy Engineering: Proactively Embedding Privacy, by Design,” Information and Privacy Commissioner Ontario, Canada, (JAN 2014), at

2-3, *available at* <https://www.privacybydesign.ca/content/uploads/2014/01/pbd-priv-engineering.pdf>. 20 *See generally* NIST Special Publication 800-37R1 “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle,” (FEB 2010), *available at*

<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>; United States Government Accountability Office “High Risk Series: An Update,” (FEB 2015), *available at* <http://www.gao.gov/assets/670/668415.pdf>; and

Federal Aviation Administration “System Safety Process Steps,” (JAN 2005), *available at*  <https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/media/ssprocdscr> p.pdf.

1. developed in this report.21 These risk management frameworks facilitate management
2. decisions about conducting business processes, achieving legal compliance, allocating
3. resources, and setting system controls. In general, agencies can more systematically align
4. their work with their mission and objectives if they have a consistent method for
5. assessing risk.

380

1. In the privacy field, a number of organizations including MITRE, the Centre for
2. Information Policy Leadership, the iMinds-DistriNet research group at the University of
3. Leuven, and others have published recent work highlighting the importance of
4. understanding privacy risk in improving privacy-preserving system engineering.22 Many
5. of these organizations have specifically cited a need for a risk model for privacy. None of
6. these organizations, however, has proposed a complete privacy risk model. 23 Therefore,
7. the first step in developing privacy engineering practices within federal agencies is to
8. establish a framework for identifying privacy risks and their impact on organizational
9. goals. With such a framework, agency officials may more effectively direct
10. organizational resources toward the mitigation of identified privacy risks while
11. supporting the mission of their agencies.

392

393 *NIST Privacy Risk Management Framework Development Process*

394

1. In developing the PRMF, NIST sought the perspectives and experiences of privacy
2. experts across a variety of sectors in an open and transparent process, including hosting
3. workshops, holding public comment periods, and engaging stakeholders in various
4. outreach activities in a broad range of fora.

399

1. NIST held three public events in April, September, and October of 2014. The first two
2. were in Gaithersburg, Maryland, and San Jose, California, respectively; the third was an
3. interactive webcast. At the April workshop, NIST led discussions focusing on
4. organizational privacy challenges. The workshop also evaluated risk models in other
5. disciplines – such as cybersecurity – and their potential to inform similar work in privacy.

21 *See e.g.,* NIST 800-37R1, *supra* Note 20; NIST Special Publication 800-39 “Managing Information Security Risk: Organization, Mission, and Information System View,” (MAR 2011), at 8, *available at*  <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>; and NIST Special Publication 800- 30R1 “Guide for Conducting Risk Assessments,” (SEPT 2012), *available at* <http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>.

22 *See generally* Stuart S. Shapiro, PhD. et al., “Privacy Engineering Framework,” MITRE Corporation (AUG 2014), *available at* <http://www.mitre.org/publications/technical-papers/privacy-engineering>-

framework; Centre for Information Policy Leadership, “Risk-based Approach to Privacy: Improving Effectiveness in Practice” Hunton & Williams LLP (JUN 2014), *available at*  <https://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf>; and LINDDUN: A Privacy Threat Assessment Framework*, available at*  [https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf](https://people.cs.kuleuven.be/%7Ekim.wuyts/LINDDUN/LINDDUN.pdf).

23 Notably, the World Economic Forum has highlighted how security risk models are inappropriate for understanding the full nature of privacy risk. World Economic Forum, “Rethinking Personal Data: A New Lens for Strengthening Trust,” (May 2014), at 18, *available at*

<http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf>*.*

1. In addition to the 240 stakeholders that attended the workshop in person, over 100 people
2. attended via webcast. These participants spanned a wide variety of sectors representing
3. the legal, policy, and technical aspects of privacy. In the April 2014 workshop, attendees
4. identified the following key issues, which helped NIST focus its attention on the
5. development of privacy engineering objectives and a risk model:
6. 1. There is a communication gap around privacy between the legal and policy,
7. design and engineering, and product and project management teams that increases
8. the difficulty for organizations to manage privacy concerns effectively,
9. understand risks and implement mitigating controls before harm occurs. A
10. contributing factor is the lack of a common vocabulary and set of tools that can be
11. used to build consistent requirements and technical standards across agencies.
12. 2. There is a need for more development tools that measure the effectiveness of
13. privacy practices.
14. 3. Risk management should be a fundamental driver of an agency’s approach to
15. privacy.
16. The second workshop had over 130 in-person attendees and an additional 500
17. participants during the October 5th webcast. At this workshop and during the webcast,
18. participants reviewed and discussed NIST’s initial draft of the privacy engineering
19. objectives and an information system privacy risk model.24 Following the September
20. workshop, NIST held an open comment period on these objectives and requested
21. additional feedback. Numerous organizations responded to the call for comments,
22. including major technology companies, civil society organizations, trade associations,
23. and federal agencies.25
24. NIST has conducted other outreach over the past year, spreading awareness about the
25. privacy risk management work while engaging stakeholders from across the fields of
26. privacy and cybersecurity. This outreach has consisted of formal presentations to a
27. number of key federal stakeholders, including the privacy committee of the U.S.
28. Government’s Chief Information Officers Council, the National Privacy Research Forum
29. of the Networking and Information Technology Research and Development (more
30. commonly known as NITRD) program, and the NIST Information Security and Privacy
31. Advisory Board. NIST has presented to numerous academic institutions, federal agencies,
32. trade associations and other stakeholders from private industry, and advocacy
33. organizations. Through this outreach, NIST has received feedback from a wide array of
34. stakeholders, better informing the development of the privacy risk methodology and the
35. supporting materials. This publication sets forth a refined version of the framework
36. originally presented in the September 2014 workshop and reflects feedback received in
37. workshop discussions, public comments and outreach.

24 The NIST workshop “Privacy Engineering Objectives and Risk Model Discussion Draft” is *available at*

<http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf>.

25 *See* “Comments on Privacy Engineering Objectives and Risk Model,” NIST Homepage, accessed May

20, 2015, *available at* <http://csrc.nist.gov/projects/privacy_engineering/public_comments.html>.

# 2. Risk Management & its Applicability to Privacy

443

1. Risk management is a comprehensive process that enables organizations to achieve their
2. mission goals while minimizing adverse

**Risk Management**

Enterprise risk management encompasses:

* Aligning risk strategy
* Enhancing risk response decisions
* Reducing operational surprises and losses
* Identifying and managing multiple and cross- enterprise risks
* Seizing opportunities
* Improving deployment of capital

1. outcomes. A risk management
2. framework helps agencies to better
3. identify, assess, and mitigate risk to their
4. organization. It assists in determining
5. which activities are most important to
6. assure critical operations and service
7. delivery. In turn, these determinations
8. aid agencies in prioritizing investments
9. and maximizing the impact of each dollar
10. spent. By providing a common

<http://www.coso.org/default.htm>

1. language to address risks present in a field, risk management is especially helpful in
2. communicating inside the organization (e.g. across management levels and operating
3. units), as well as outside the organization. A risk management framework specifically for
4. privacy can help agencies to address privacy risk within their broader enterprise risk
5. portfolio to improve these outcomes.

461

1. NIST has successfully developed frameworks to assess risk, including the risk
2. management framework for management of cybersecurity risk(s) (RMF).26 The RMF has
3. several characteristics that make it a useful model for informing the PRMF as it:
4.  concentrates on information systems;
5.  has well-established objectives, and it has a significant level of maturity;
6.  is not law or regulation-based, but can facilitate legal compliance because it does
7. not pre-suppose any particular policy or outcome and is technology-neutral; and
8.  can enable the setting of appropriate controls to mitigate potential issues.27

470

471 The PRMF models the following key components:

472  characteristics or properties of secure systems;28

473  a common vocabulary for describing cybersecurity risk; and

26 NIST 800-37R1, *supra* Note 20; *see also* NIST 800-39, *supra* Note 21; and NIST 800-30R1, *supra* Note 21.

27 *See generally* NIST 800-37R1, *supra* Note 20.

28 *Id.* at 2. For further information regarding the characteristics of secure systems to include security

objectives, *see* NIST Federal Information Processing Standards Publication Series 199 “Standards for Security Categorization of Federal Information and Information Systems,” (FEB 2004), at 1-2 *available at*  <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>. The security objectives are codified in FISMA: “integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity…confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information…availability, which means ensuring timely and reliable access to and use of information.” 44 U.S.C. § 3542, *available at* <http://www.gpo.gov/fdsys/pkg/USCODE-2008>- title44/pdf/USCODE-2008-title44-chap35-subchapIII-sec3541.pdf.

474  an equation to enable the calculation of cybersecurity risk for a given system.

475

1. NIST research suggests that equivalent components would be beneficial for the
2. management of privacy risk, as privacy risks have not been comprehensively addressed
3. by cybersecurity risk management.29 In contrast to cybersecurity, impacts on individuals
4. are intrinsic to notions of privacy.30 These impacts have generally been classified under
5. the concept of privacy invasions, but are referred to in this document more simply as
6. problems.31

482

1. As noted above, the underlying rationale for risk management is the achievement of
2. mission goals while minimizing adverse outcomes or problems. With respect to
3. individuals and information systems, the privacy problems that they may experience arise
4. from the processing of their personal information. That is to say, when information
5. systems are conducting operations that, for example, involve collecting, generating,
6. using, storing, or disclosing information about individuals, these activities can give rise to
7. the kinds of problems described in the catalog in Appendix F.32 To understand how
8. cybersecurity risk management and privacy risk management are complementary, but
9. distinct processes, agencies must consider the source of these problems. While the source
10. may be unauthorized access to systems that contain information about individuals,
11. problems can also arise from information processing operations of the systems
12. themselves. For example, in the energy sector, some communities have responded
13. negatively to smart meters due largely to concern that utilities’ collection of the
14. information itself can reveal people’s behavior inside their homes, not from concerns that
15. the utilities cannot keep the information secure.33 Moreover, even actions taken to protect
16. personal information can have privacy implications. For example, security tools to defend
17. personal information from malicious actors, such as persistent activity monitoring, can

29 *See* United States Government Accountability Office “High-Risk Series: An Update,” (FEB 2015), at \*2, *available at* <http://www.gao.gov/assets/670/668415.pdf>wherein the challenges to ensuring the privacy of personally identifiable information in the face of rapidly changing technology is underscored.

30 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. Rev. 477, 484 (2006), *available at*

<https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282> 006%29.pdf.

31 As Daniel J. Solove explains, the concept of “privacy” is a vague notion. Accordingly, he developed a useful privacy taxonomy wherein he focused on the specific activities that pose privacy problems for individuals. *Id.* at 481-82.

32 NIST developed this non-exhaustive catalog to enable the validation of the PRMF. The catalog is derived

from Daniel Solove’s, *A Taxonomy of Privacy. Supra* Note 30.

33 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>**.** For a discussion regarding privacy risks weighed against big data opportunities, *see* Jules Polonetsky and Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 Stan. L. Rev. 25 (2013), *available at* <http://www.stanfordlawreview.org/sites/default/files/online/topics/64>- SLRO-63\_1.pdf.

1. create similar concerns about the degree to which information is revealed about
2. individuals that is unrelated to cybersecurity purposes.

502

1. A privacy risk management framework, therefore, should provide the capability to assess
2. the risk of problems for individuals arising from the operations of the system that involve
3. the processing of their information. Cybersecurity risk management frameworks,
4. standards, and best practices can be used to address risks to individuals arising from
5. unauthorized access to their information. Thus, NIST assumes that an agency
6. implementing the PRMF in this publication will already be using a cybersecurity risk-
7. based approach to manage such risks. Used in conjunction with a cybersecurity risk
8. management framework, the PRMF proposed in this document offers a consistent,
9. repeatable process for evaluating and enabling communication of privacy risk to facilitate
10. the implementation of law, policy, and regulation aimed at protecting the totality of
11. individuals’ privacy.

# 3. NIST Privacy Risk Management Framework

515

516 The PRMF enables an agency to determine the sources of privacy risk to individuals in

517 an information system. An agency can repeat these processes consistently across

518 departments, providing comparable results. An agency can use this framework to first

519 identify its goals and obligations for privacy protection, assess its systems against these

520 governing requirements, prioritize mitigation mechanisms, and monitor for changes.

521

1. The NIST RMF categorizes four broad
2. processes in looped phases, as illustrated in
3. *Figure 01*: (i) *frame* risk (i.e., establish the
4. context for risk-based decisions); (ii) *assess*
5. risk; (iii) *respond* to risk once determined;
6. and (iv) *monitor* risk on an ongoing basis.34

528

529 Building on these four phases, the NIST

530 PRMF is composed of six processes that are

531 tailored for addressing privacy in

532 information systems.

533

1. The six processes are:

Figure 01: NIST Risk Management Framework

1.  **Frame business objectives**. An agency frames the business objectives for its
2. system, including the agency needs served. Such needs may include the
3. demonstration of specified privacy-preserving functionality. This process will
4. support the end-stage design and implementation of controls because appropriate
5. controls must permit the system to achieve the intended business functions while
6. demonstrating measurable results for privacy protection.
7.  **Frame organizational privacy governance**. An agency frames the
8. organizational privacy governance by identifying privacy-related legal
9. obligations, principles, organizational goals, and other commitments within which
10. the system must operate. This process is a key input into the calculation of
11. privacy risk as it allows better assessment of the impact of identified problems for
12. individuals arising from the processing of their personal information on
13. organizational privacy requirements and goals. Such an impact assessment is
14. necessary for agencies to be able to use risk management to achieve their
15. missions while minimizing adverse events for individuals and agencies
16. collectively.
17.  **Assess system design.** To assess system design from a privacy perspective,
18. agencies will need to describe the lifecycle of the system operations with respect
19. to the personal information being processed by that operation and specific
20. contextual factors that may heighten or lower the risk potential of the system
21. operation. This process documents the inputs necessary for the privacy risk

34 NIST 800-39, *Supra* Note 21 at 8.

1. model. It provides a method for making the concerns of individuals visible to
2. agencies and how these concerns correlate to the behavior of the system.
3.  **Assess privacy risk.** In this stage, an agency identifies and prioritizes privacy
4. risks. The process integrates the inputs from the previous three stages so that
5. agencies can use the privacy risk model to calculate and prioritize the privacy risk
6. of specific operations of their systems. This prioritization enables agencies to
7. determine appropriate resource allocations to address the risks.
8.  **Design privacy controls.** Having prioritized risk in the previous phase, this phase
9. is focused on the selection and implementation of controls to mitigate identified
10. privacy risks. The design process includes selection and implementation to enable
11. the development of tools and guidance for increasing agency awareness of the full
12. spectrum of available controls, including technical measures that may supplement
13. or improve upon existing policy-centric controls based on the FIPPs.35
14.  **Monitor change.** In this process, an agency assesses any changes in an
15. information system that would impact individuals’ privacy such as changes in
16. system operations involving the processing of personal information, changes in
17. the personal information being processed or changes in contextual factors, as well
18. as monitoring the effectiveness of implemented privacy controls.

574

1. While the PRMF is unique because of

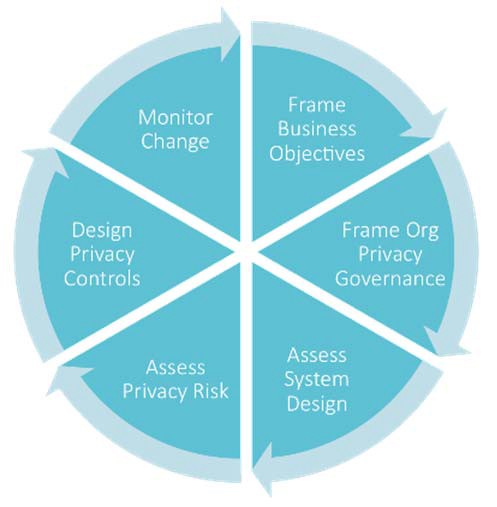


Figure 02: NIST Privacy Risk Management Framework

1. its focus on privacy, the processes are
2. similar to other types of risk
3. frameworks.**36** The distinctive nature
4. of the PRMF arises from its
5. foundation on two key
6. communication and analytical tools:
7. the privacy engineering objectives
8. and the privacy risk model described
9. in greater detail below.

585

1. To aid agencies in using the PRMF
2. and to apply the privacy risk model,
3. NIST has developed an initial set of
4. worksheets, collectively referred to as
5. the Privacy Risk Assessment
6. Methodology (PRAM). Appendix D
7. contains drafts of worksheets that support processes one through four of the PRMF. As
8. noted in the Scope section above, the selection and implementation of controls is an area
9. of future work for NIST. NIST will continue to develop the PRAM to address phase five
10. of the PRMF as this work evolves. The remainder of this document describes the privacy
11. engineering objectives, the privacy risk model, and the inputs for the PRAM worksheets.

597

35 *See* NIST 800-53R4, Appendix J, *supra* Note 7 at J-1.

36 *See. e.g.,* NIST 800-30R1, *supra* Note 21.

##### 598 System Objectives in Cybersecurity Risk Management

599

600 Following the workshop in April of 2014, NIST first focused its efforts on the

601 communication gap cited by multiple attendees as being at the core of many of their 602 organizations’ privacy challenges.37 A key question emerged that helped guide the 603 examination of other fields that had successfully bridged this gap: what do other 604 disciplines have that privacy does not? An examination of the cybersecurity field

605 highlighted one potential avenue for exploration: objectives or system properties also

606 known as confidentiality, integrity, and availability (CIA triad).38

607

608 The CIA triad was first articulated in 1975.39 While initially designed to catalog different

609 typologies of threats to information systems, with their ultimate codification in the

610 Federal Information Security Management Act of 2002 (“FISMA”), CIA triad evolved to 611 become a positive outcome-based model used to maintain security. This transition of the 612 CIA triad from their use as broad threat classifications to characteristics of secure

613 systems highlights what makes the security objectives useful to an agency.

614

615 The objectives provide a concrete way to think about security and target the points in

616 systems where engineering needs to occur in order to enable a secure system. FISMA 617 requires a risk management process for cybersecurity in federal systems.40 Agencies must 618 be able to communicate across various internal units (e.g., engineering, management,

619 policy, legal, compliance) in order to highlight areas of risk, and determine how those

620 risks impact other mission priorities. Objectives provide a tool in facilitating

621 communication across these boundaries. While a senior official may not understand the 622 technical implications of a particular cybersecurity risk, describing that risk in terms of 623 the system’s confidentiality, integrity, or availability can bridge that communication gap. 624 An engineer may not understand the policies that dictate certain design requirements, but 625 can understand how to develop a system if those requirements can be interpreted in terms 626 of confidentiality, integrity, and availability.

627

628 As described above, agencies have been reliant on principles like the FIPPs that have 629 provided a combination of values, governance principles, and requirements, but lack the 630 concrete conceptualizations that the CIA triad has provided cybersecurity. The FIPPs

37 The webcast of the April 2014 Privacy Engineering Workshop, held at the NIST offices in Gaithersburg, MD, is *available at* <http://www.nist.gov/itl/csd/privacy-engineering-workshop-webcast.cfm>.

38 NIST Special Publication 800-14 “Generally Accepted Principles and Practices for Securing Information Technology Systems,” (SEPT 1996), *available at* <http://csrc.nist.gov/publications/nistpubs/800-14/800>-

14.pdf, recognizes fundamental principles that should comprise an organization’s information security program to include protecting the confidentiality, availability and integrity of the organization’s data.

39 *See* Jerome H. Saltzer, and Michel D. Schroeder, “The Protection of Information in Computer Systems,” Proceedings of the IEEE 63(9), pp. 1278-1308, 1975 at \*2-3 *available at*

<http://www.acsac.org/secshelf/papers/protection_information.pdf>.

40 *See* 44 U.S.C. § 3541, *available at* <http://www.gpo.gov/fdsys/pkg/USCODE-2008-title44/pdf/USCODE>-

2008-title44-chap35-subchapIII-sec3541.pdf. NIST developed its Special Publication 800-30R1 as part of its FISMA Implementation program. *See* NIST 800-30R1, *supra* Note 21.

631 provide senior officials a foundation for considering privacy in information systems, but 632 do not yield an approach for consistent communication of outcome-based aspects of a 633 system that would enable engineers to assess their systems for appropriate capabilities 634 and system design options. Privacy engineering objectives can play a key role in bridging 635 the gap between an agency’s goals for privacy and their manifestation in information

636 systems.

##### 637 Privacy Engineering Objectives

638

639 NIST has developed three privacy engineering objectives for the purpose of facilitating 640 the development and operation of privacy-preserving information systems: predictability, 641 manageability, and disassociability. These objectives are designed to enable system

642 designers and engineers to build information systems that are capable of implementing an 643 agency’s privacy goals and support the management of privacy risk. As with CIA, these 644 objectives are core characteristics of information systems. A system should exhibit each 645 objective to some degree to be considered a system that could enable privacy protections 646 while achieving its functional purpose.

***Predictability*** *is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.*

***Manageability*** *is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure.*

***Disassociability*** *is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.*

647

648 *Predictability*

649

650 Predictability provides agencies with both precision and flexibility in aligning their 651 information systems to support privacy-preserving user relationships. A reliable belief 652 about what is occurring with personal information in a system is core to building trust 653 and enabling self-determination. These precepts have been the foundation of the

654 transparency FIPP. By framing this objective in terms of reliable assumptions, agencies 655 can begin to measure more concretely the expression of transparency in an information 656 system. Enabling reliable assumptions does not require that individuals know all the 657 technical details about how a system processes their personal information. Rather,

658 predictability is about designing systems such that stakeholders are not surprised by the

659 handling of personal information.41 In this way, predictability can support a range of

660 organizational interpretations of transparency from a value statement about the

661 importance of open processes to a requirements-based view that specific information

662 should be shared.

663

664 Predictability, however, is more than transparency. For system operators, predictability

665 provides a broader base for control selection when assessing a system’s privacy risk.

666 Even in a system that may create unpredictable or previously unknown results – such as a 667 large data analysis or research effort – predictability can provide a valuable set of insights 668 about how to control privacy risks that may arise. For example, if the results of a data 669 action are inherently unpredictable, operators can implement controls to restrict access to 670 or use of those results. They can also consider technical controls that could de-identify 671 individuals so that individuals can make reliable assumptions about when a system would 672 reveal certain information about them and when it would not. A variety of controls,

673 including technical controls, can facilitate implementation of predictability to produce the

674 desired outcome for privacy.

675

676 Finally, predictability supports the translation or implementation of the FIPPs for use 677 limitation and purpose specification in a manner that allows for innovation. For example, 678 inherent in the rationale for use limitation is the recognition that changes in processing of 679 personal information are loci for privacy risk. By focusing on maintaining reliable

680 assumptions about that processing, predictability enables operators to assess the impact of

681 any changes and target the application of appropriate controls. Thus, predictability

682 facilitates the maintenance of stable, trusted relationships between information systems 683 and individuals and the capability for individuals’ self-determination, while enabling 684 operators to continue to innovate and provide better services.

685

686 *Manageability*

687

688 Manageability is an important system property for enabling self-determination, as well as 689 fair treatment of individuals. If agencies cannot administer individuals’ information with 690 sufficient granularity, they cannot be confident that inaccurate information can be

691 identified and corrected, obsolete information is deleted, and only necessary information 692 is collected or disclosed. In short, if the information system does not permit fine-grained 693 control over data, agencies cannot implement key FIPPs, including maintaining data 694 quality and integrity, achieving data minimization, and implementing individuals’

695 privacy preferences.

696

1. Nonetheless, manageability is not a policy statement about the general right of
2. individuals to control their information. It creates the system capability to manifest this
3. policy, while minimizing potential conflicts in system functionality. For instance, it might

41 See e.g., Pat Conroy et al., “Building Consumer Trust: Protecting consumer data in the consumer product industry,” (NOV 2014), available at <http://dupress.com/articles/consumer-data-privacy-strategies>/ wherein Deloitte reported the results of its recent study of online consumers that showed 80% are “more likely to purchase brands from consumer product companies that they believe protect their personal information.”

1. impair the functioning of some systems for individuals to be able to edit or delete
2. information themselves (e.g., fraud detection or proof of eligibility). Manageability in
3. these systems, however, would still enable the appropriately privileged actor to
4. administer changes to maintain accuracy and fair treatment of individuals. Finally,
5. manageability could support the mapping of technical controls such as data tagging and
6. emerging standards in identity management that relate to attribute transmission.

706

707 *Disassociability*

708

1. Disassociability captures one of the essential elements of privacy-enhancing systems 
2. that the system actively protects or “blinds” an individual’s identity or associated
3. activities from unnecessary exposure. Unlike confidentiality, which is focused on
4. preventing unauthorized access to information, disassociability recognizes that privacy
5. risks can result from exposures even when access is authorized or as a byproduct of a
6. transaction.42 Disassociability advances the capabilities of a privacy-preserving system by 715 engaging system designers and engineers in a deliberate consideration of such points of 716 exposure.

717

718 Although the operational requirements may vary depending on the system, achieving this

719 objective should reflect the ability to complete the transaction without associating 720 information to individuals. For example, identity proofing or the direct provision of 721 health care services may necessitate the association of information with an individual. 722 However, operational requirements should not include the mere difficulty of

723 disassociating the information from individuals. Agencies may opt to accept the risk

724 because of the difficulty in implementing appropriate controls or institute other

725 compensating controls, but the recognition of such risk is distinct from defining specific

726 associations of information as an operational requirement.

727

728 Many cryptographic techniques that exist today or are currently being researched could 729 be mapped to disassociability.43 The adoption of disassociability as an objective could not 730 only raise awareness of the benefits of these techniques, but could increase demand for 731 more advances. A further consideration for increasing the effectiveness of

732 disassociability is whether a taxonomy could be constructed of existing identity-related

733 classifications, including anonymity, de-identification, unlinkability, unobservability,

42 Pursuant to 44 U.S.C. § 3542, *available at* <http://www.gpo.gov/fdsys/pkg/USCODE-2011>- title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf, confidentiality “means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.”

43 For instance, the use of the “zero-knowledge proof” cryptographic method could allow one party (the prover) to authenticate an identity to another party (the verifier) without the exchange of private or secret

information. *See* NIST Special Publication 800-21R2 “Guideline for Implementing Cryptography in the Federal Government,” (DEC 2005), *available at* <http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800>- 21-1\_Dec2005.pdf.

734 pseudonymity or others.44 Such a taxonomy could potentially support more precise

735 control mapping and risk mitigation.

736

737 Together, these three privacy engineering objectives, complemented by the CIA triad to 738 address unauthorized access to personal information, provide a core set of information 739 system capabilities to support the balanced attainment of agency business goals and 740 privacy goals, and assist in the mapping of controls to mitigate identified privacy risks. 741 Like the CIA triad, they provide a degree of precision and measurability, so that system 742 designers and engineers, working with policy teams, can use them to bridge the gap 743 between high-level principles and implementation within a functional system.

744

44 Some of these concepts are explored in Draft NISTIR 8053 “De-Identification of Personally Identifiable Information,” (APR 2015), *available at* <http://csrc.nist.gov/publications/drafts/nistir>- 8053/nistir\_8053\_draft.pdf. *See also* LINDDUN: A Privacy Threat Assessment Framework*, available at*  [https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf](https://people.cs.kuleuven.be/%7Ekim.wuyts/LINDDUN/LINDDUN.pdf) which outlines a method for modeling privacy-specific threats.

##### 745 A Privacy Risk Model

746

747 Risk is often expressed as a function of the likelihood that an adverse outcome occurs 748 multiplied by the magnitude of the adverse outcome should it occur.45 In information 749 security, likelihood is understood as a function of the threats to the system, the

750 vulnerabilities that can be exploited, and the consequences should those vulnerabilities be

751 exploited.46 Accordingly, security risk assessments focus on where in the system

752 damaging events could cause problems. Excepting the issue of unauthorized access to

753 personal information, privacy risk differs. 754 As noted earlier, the adverse outcomes, or 755 problems for individuals, can arise from the 756 operations of the system itself, regardless of 757 external factors and even in the absence of 758 a technical vulnerability, such as poor

**Data Actions**

Data actions are information system operations that process personal information. “Processing” can include, but is not limited to, the collection, retention, logging, generation, transformation, disclosure, transfer, and disposal of personal information.

759 software design or implementation. Thus, 760 the terms “threat” and “vulnerability” fail to 761 capture the essence of many privacy

762 problems for individuals.

763

764 Consequently, a privacy risk model that can help organizations identify privacy risk as

765 distinct from security risk requires terminology more suited to the nature of the risk. 766 Given the focus on the operations of the system when processing personal information, 767 an information system’s privacy risk, therefore can be described as a function of the

768 likelihood that a data action (a system operation processing personal information) causes 769 problems for individuals, and the impact of the problematic data action should it occur. In 770 simple terms, privacy risk can be expressed as:

771

772

Privacy Risk =

**Likelihood of a**

**x Impact of a problematic data**

773

problematic data action action

774

775 Using this new equation, agencies can calculate the privacy risk of a data action by

776 assessing likelihood and impact of the data action becoming problematic. It is important

777 to consider both of these factors, because neither one alone can aid an agency in

778 prioritizing controls and allocating resources.

779

780 Likelihood is assessed as the probability that a data action will become problematic for a 781 representative or typical individual whose personal information is being processed by the 782 system. The PRAM demonstrates a step by step analysis of likelihood. Agencies can

45 *See* NIST 800-30R1, *supra* Note 21 at 8-13.

46 For an explanation of Information Technology risk assessments, *see* NIST Special Publication 800-100 “Information Security Handbook: A Guide for Managers,” at 88-89, *available at*

[http://csrc.nist.gov/publications/nistpubs/800‐100/SP800‐100‐Mar07‐2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf).

783 support the assessment of likelihood in a number of ways. They may use existing

784 information on customer demographics to estimate likelihood; they may extrapolate from

785 information available about privacy concerns in similar scenarios; alternatively, they 786 could conduct focus groups or surveys to glean more thorough and specific information 787 from users about privacy concerns.

788

789 Impact is assessed as the magnitude of the problematic data action on the organization if 790 it occurs. Impact is expressed through the organization for a few reasons. Although the 791 purpose of the PRAM is to make more visible the problems that individuals can

792 experience from the processing of their personal data in information systems, such

793 problems may occur at some distance from the initial processing in the agency system. In

794 addition, the actual magnitude for individuals may depend on their subjective

795 experiences, such that an agency has to make a risk-based determination based on the 796 composition of all individuals that may be affected. Finally, an important function of risk 797 calculation is to produce a risk prioritization that can enable determinations about risk 798 mitigation. Therefore, agencies must be able to reflect their best understanding of the 799 problems individuals may experience through the lens of their overall mission needs, 800 privacy-related goals and responsibilities, and resources. For this reason, the first two 801 stages of the PRMF are processes that enable agencies to frame their mission needs and 802 privacy goals and requirements. The PRAM reflects these framing processes with an

1. impact analysis focused on four organizational impact factors, listed below with
2. illustrative examples:
3. 1. Noncompliance costs: how will the agency be impacted by not complying with
4. applicable laws, policies, contracts, etc.?
5. 2. Direct costs: will the agency face a decrease in use of the system or face other
6. impediments to achieving its mission?
7. 3. Reputational costs: how will this potential problem affect public trust in the
8. agency?
9. 4. Internal culture costs: how will employee morale, retention, or other aspects of
10. agency culture be affected?

813

814 These four factors should not be considered an exhaustive list. Each agency should 815 consider any additional impact factors specific to its work, mission, structure, and 816 customer base.

817

818 Prioritization helps agencies to align mission priorities and resources. Addressing data 819 actions with low likelihood and low impact of being problematic may be of a lower 820 priority while addressing those with high likelihood and high impact is of the highest 821 priority. However, likelihood and impact do not always align. For example:

822  **Low likelihood/high impact:** While certain data actions may be less likely to 823 become problematic, they could have a severe impact; in these cases, an agency 824 may prioritize mitigation of these problems because any incidence of this severe 825 problem would have unacceptable consequences. For example, if researchers had 826 access to a data set of individuals’ health information, the likelihood that the

827 researchers would use the information improperly might be low, but the

828 consequences for individuals, and therefore, for the mission and reputation of the

829 organization, might be severe if misuse did occur, given the sensitive nature of

830 health information.

831  **High likelihood/low impact:** Alternatively, a problematic data action with a 832 small impact may have a very high likelihood, leading an agency to prioritize 833 controls for those problems in order to not negatively affect such a large portion 834 of their constituents, even if the impact is low. For instance, an agency might use

835 a web analytics tool that raised concerns among users of the website. In this case, 836 the impact may be limited to some customer questions or complaints, but given 837 that the tool affects all users, the agency might prioritize the application of a

838 control that anticipates and addresses the concerns.

839

840 These prioritization decisions will vary by agency and data action, but are much better 841 informed if both likelihood and impact are systematically assessed for each data action. 842 In many cases, a determination of likelihood and impact may not be a simple process; just 843 as implementing controls requires investment, properly assessing risk requires

844 investment. In some cases conducting research may be necessary to better understand the 845 likelihood of a privacy problem occurring. In others, it may be more appropriate to rely 846 on the knowledge of experts in the agency. Agencies must consider the benefits and costs 847 of different approaches.

848 *Inputs to the Privacy Risk Assessment Methodology*

849

850 This section describes the inputs set forth in the PRAM that are used in calculating 851 likelihood and impact. The principal inputs are the data actions of the system, the 852 personal information associated with a data action, and context, or the circumstances 853 surrounding the data actions. This section also describes the analytical functions that 854 agencies can apply to these inputs to enable risk prioritization so that they can make

855 determinations about risk acceptance or mitigation. In future iterations, the PRAM may 856 include the capability for agencies to compare controls for maximizing cost-effective 857 mitigations.

858

Identify Data Actions

Catalogue Personal Information and Contextual Factors

Document Summary Issues

Consider Problematic Data Actions

859

Figure 03: Inputs for the PRAM

860

861 Data Actions

862

863 Data actions are any information system operations that process personal information*.* As 864 noted, the privacy risk model hinges on whether a data action becomes problematic for 865 individuals. Thus, the PRAM is oriented around the analysis of specific data actions for 866 privacy risk. To better analyze the context applicable to each data action’s risk, agencies 867 should map and describe data actions at a sufficiently granular level. For example, rather

868 than using a high level label such as “collection” or “retention," agencies might include 869 more descriptive details, such as “collection from users at registration via mobile device” 870 or “storage in an internal database.”

871

872 Personal Information & Context

873

1. There are two critical inputs that modify the risk of any given data action: personal
2. information and context. For each data action, an organization should identify the
3. associated personal information at a granular level (e.g., doctor name, doctor address, and
4. medical diagnosis instead of simply “health information”). Agencies should consider
5. personal information broadly, and should include not only information that directly
6. identifies an individual, but also information about events or behavior that can be linked 880 to that individual.47 As with data actions, granular mapping of personal information is 881 important; it may be that specific pieces of personal information heighten the privacy

882 risk, such that applying targeted controls may enable the agency to better preserve system

883 functionality while mitigating risk to an acceptable level.

884

885 The risk of a data action is also a function of context – the circumstances surrounding the 886 system's processing of personal information. An agency may need to consider context 887 from various viewpoints (e.g., organizational, system, individual, data action) to

888 determine which circumstances influence the risk of a data action.48 Capturing contextual

889 factors will likely require coordination between privacy officers and information

890 technology personnel within an agency.

891

892 Summary Issues

893

894 Both context and associated personal information contribute to whether a data action has

895 the potential to cause privacy problems. Based on these pieces of information, it is

896 possible for an organization to draw initial observations about data actions - characterized

897 as summary issues. Summary issues can be expressed as statements that upon further 898 analysis heighten the assessment of risk or decrease it. They can also be expressed as 899 questions that function as flags. Depending on the stage of system design, agencies may 900 have open questions about certain aspects of the system operations. They should capture 901 these open questions because the eventual determinations may be dispositive to the risk 902 assessment. For example, whether a data action will be executed by the agency itself or a 903 third-party may be undecided at an early stage of design, but the eventual disposition 904 could be an important assessment factor. Therefore, the open question should be flagged 905 until the determination is made, and the final assessment can be completed.

47 For the purpose of risk assessment, personal information is considered broadly as any information that can uniquely identify an individual as well as any other information, events or behavior that can be associated with an individual. Where agencies are conducting activities subject to specific laws, regulation or policy, more precise definitions may apply.

48 *See infra* catalog of contextual factors in Appendix G.

906

#### 907 Problematic Data Actions

908

909 After cataloging the summary issues related to each data action, the next step of the 910 analysis is to identify the adverse effects, or problems for individuals that could arise 911 from these actions; these are termed problematic data actions. Each problematic data 912 action could result in one or more potential problems for individuals. Understanding 913 which problems are more likely to occur - and have the greatest impact - may help an 914 agency to pinpoint what type of control would be most effective to mitigate a data 915 action’s privacy risk. For the validation of the PRAM, NIST has developed a non-

916 exhaustive catalog of problematic data actions and problems set forth in Appendices E

917 and F, respectively.

918

919 Once these inputs and analyses have been captured in the worksheets, agencies can use 920 the PRAM to calculate the privacy risk of each data action. This process enables them to 921 compare risk points within the system, and prioritize them. Thus, the PRAM provides a 922 repeatable process that enables agencies to visualize where privacy risk may be occurring 923 in their systems, communicate these risks at appropriate organizational levels, and make 924 resource decisions with respect to addressing the risks.

925 4. Next Steps

926

1. It is NIST’s goal that this PRMF may inform agencies about privacy risk the same way
2. risk management frameworks for cybersecurity have informed the assessment and
3. mitigation of security risks. As the understanding of cybersecurity risks has become more
4. thorough, a baseline expectation for an understanding of this process has become
5. common. As a result, much of what is formalized in cybersecurity risk management
6. strategies like the NIST RMF has become second nature to many individuals contributing 933 to the security of agencies’ information systems. As NIST continues to research privacy 934 engineering, it is our goal to provide a complete set of tools that agencies can use to

935 understand potential privacy risks, prioritize them, and effectively address them.

936

937 To realize these goals, future areas of work in privacy risk management will focus on 938 improving the application of controls – policy, operational and technical – to mitigate 939 risks identified with the PRMF. It will require research to identify the breadth of controls 940 available, what kinds of privacy risks they can address, how they can be effectively

941 applied, and what kind of ancillary effects their application may create. To facilitate this

942 research, NIST will continue to request feedback to refine the privacy engineering

943 objectives and the privacy risk equation, and to develop additional guidance to assist 944 agencies in determining the likelihood and impact of privacy risks. The research process 945 will continue to be an open and transparent process that will solicit input from federal 946 agencies, academic institutions, private organizations, and civil society organizations in 947 order to develop guidance that reflects the best practices for addressing privacy risks.

948

949

# Appendices

##### 950 Appendix A: Glossary

951

952 **Context**: the circumstances surrounding the system's processing of personal information

953

954 **Data Actions**: Information system operations that process personal information.

955

956 **Manageability:** Providing the capability for granular administration of personal

957 information including alteration, deletion, and selective disclosure

958

959 **Disassociability:** Enabling the processing of personal information or events without 960 association to individuals or devices beyond the operational requirements of the system. 961

962 **Personal Information:** For the purpose of risk assessment, personal information is

963 considered broadly as any information that can uniquely identify an individual as well as

964 any other information, events or behavior that can be associated with an individual. 965 Where agencies are conducting activities subject to specific laws, regulation or policy, 966 more precise definitions may apply.

967

968 **Predictability:** Enabling of reliable assumptions by individuals, owners, and operators

969 about personal information and its processing by an information system.

970

971 **Privacy control:** The administrative, technical, and physical safeguards employed within 972 organizations to mitigate risks to individuals arising from the processing of their personal 973 information within information systems.

974

975 **Privacy engineering:** Privacy engineering is an emerging field, but currently there is no 976 widely-accepted definition of the discipline. For the purposes of this publication, privacy 977 engineering is a collection of methods to support the mitigation of risks to individuals 978 arising from the processing of their personal information within information systems.

979

980 **Problematic Data Actions:** A data action that causes an adverse effect, or problem, for

981 individuals.

982

983 **Processing:** Operation or set of operations performed upon personal information that can

984 include, but is not limited to, the collection, retention, logging, generation,

985 transformation, use, disclosure, transfer, and disposal of personal information. See

986 ISO/IEC 29100:2011(E) for a related definition.

987

988 **Risk:** A measure of the extent to which an entity or individual is threatened by a potential 989 circumstance or event, and typically is a function of: (i) the adverse impact that would 990 arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.49

991

992 **Summary Issues:** Initial contextual analyses about data actions that may heighten or

993 decrease the assessment of privacy risk.

994

49 *See* NIST 800-30R1, *supra* Note 21 at 8-13.

##### 995 Appendix B: Acronyms

996

|  |  |  |
| --- | --- | --- |
| 997 | CPS | Cyber‐physical systems |
| 998 | FIPPs | Fair Information Practice Principles |
| 999 | IDP | Identity service provider |
| 1000 | IoT | Internet of Things |
| 1001 | ITL | Information Technology Laboratory |
| 1002 | NIST | National Institute of Standards and Technology |
| 1003 | NITRD | Networking and Information Technology Research and Development |
| 1004 | NSTIC | National Strategy for Trusted Identities in Cyberspace |
| 1005 | OTP | One time password |
| 1006 | PIA | Privacy impact assessment |
| 1007 | PRAM | Privacy Risk Assessment Methodology |
| 1008 | PRMF | Privacy Risk Management Framework |
| 1009 | RMF | Risk Management Framework |
| 1010 |  |  |

##### 1011 Appendix C: Formal Mathematical Statement of the Privacy Risk Model

1012

1013 In this document, privacy risk is given by:

1014

1015

Privacy Risk =

**Likelihood of a**

**x Impact of problematic data**

1016

1017

1018

1019

1020

1021

problematic data action action

If this is true for each data action in an information system, then the unmitigated privacy risk for an entire system, ܴ௎, is given by

஽ ௉

ܴ௎ ൌ ෍ ෍ ܮௗ௣ܫௗ௣

ௗ ௣

1022 where

1023

1024

1025

1026

1027

ܮௗ௣ is the likelihood of privacy problem ݌ occurring in data action ݀

Iௗ௣ is the impact of privacy problem ݌ on the agency if it results from data action ݀

ܦ is the set of all possible data actions

ܲ is the set of all possible privacy problems.

1028

Mitigated, or residual, agency privacy risk for a system, ܴோ, is given by

஽ ௉

െ ܥ

ௗ௣

ௗ௣

1029

ܴோ ൌ ෍ ෍ሺܮௗ௣

ௗ ௣

௅

௅ ሻሺܫௗ௣

െ ܥூ ሻ

1030 where

1031

1032

1033

1034

ܥௗ௣ is the reduction in likelihood of privacy problem ݌ occurring in data

action ݀ by employing control ܥ

ܥூ is the reduction in impact of privacy problem ݌ on the agency if it results from data action ݀ by employing control ܥ

ௗ௣

1035 The residual risk calculation implies that, for any data action, a given control can reduce 1036 the likelihood of a privacy problem, the impact of that privacy problem should it occur, 1037 or both. While controls are not the focus of this document, this outcome is sufficiently 1038 important to address here. When determining controls, the agency may be able to

1039 dynamically reduce privacy risk through a single control that reduces both likelihood and

1040 impact and, potentially, does so in multiple data actions.

1041

##### 1042 Appendix D: Privacy Risk Assessment Methodology

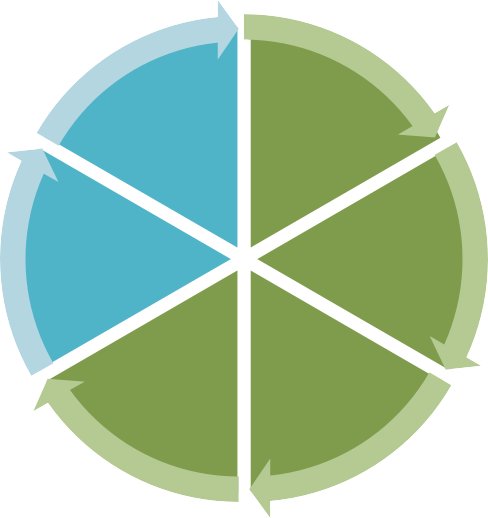
1043

1044 ***Introduction***

1045

1046 In order to better understand the practical implications of utilizing the privacy risk 1047 framework outlined in this document, NIST developed the PRAM. The PRAM consists 1048 of a series of worksheets that can be used to frame business objectives and privacy 1049 governance, and assess system design and privacy risk. These worksheets provide a 1050 practical method for implementing the framework. The current iteration only provides 1051 worksheets through the Assess Privacy Risk phase. As NIST develops the privacy risk 1052 framework further, it will explore how to best improve this tool, including developing 1053 worksheets to support the Design Privacy Controls phase.

1054



Monitor

Change

Frame

Business Objectives

Design

Privacy Controls

Frame Org

Privacy Governance

Assess

Privacy Risk

Assess

System Design

1055 A few of the funding recipients in the

1056 NSTIC pilot program have used this

1057 methodology while reviewing their systems 1058 for alignment with the NSTIC privacy 1059 guiding principle.50 These pilots provided 1060 valuable insight into the practical

1061 application of this risk assessment

1062 methodology. Their size ranged from start-

1063 ups to large information technology

1064 companies, and included systems designed 1065 for private use as well as public service 1066 deployment. The maturity of the systems 1067 assessed also varied, and allowed NIST to 1068 understand the value of privacy risk

1069 assessment at different stages of technical

1070 development.

1071

1072 The worksheets catalog data actions, context, and other inputs of risk. The worksheets 1073 provided a baseline, but a number of the pilots ultimately customized them to fit the 1074 needs of their specific information systems.

1075

1076 ***Guidance***

1077

1078 Instructions for the completion of the worksheets can be found in the sample worksheets 1079 below. Each page of instructions includes an example – this is a small use-case developed 1080 by NIST to illustrate how to include different inputs into the worksheets. The use case is 1081 illustrative only and does not reflect the design of any existing system, including those of 1082 the NSTIC pilots. The example purposefully includes many privacy flaws.

1083

1084

50 “Catalyzing the Marketplace: NSTIC Pilot Program,” *supra* Note 14.

1085 ***Common Issues for Consideration***

1086

1087 Over the course of working with the NSTIC pilots, some initial challenges became

1088 apparent. These are listed below with some guidance for each.

1089

1090 *Unmitigated Risk*

1091

1092 In the worksheets, the Summary Issues are the first consolidated assessment where

1093 observations that will provide the touch points for identifying problematic data actions 1094 are cataloged. This creates a critical juncture for the rest of the analysis – poor summation 1095 of the influence of contextual factors on data actions and personal information leads to 1096 poor downstream assessment of the potential problems for individuals. The goal of the 1097 risk assessment process is to provide a review of unmitigated risk in order to evaluate the 1098 comparative effectiveness of mitigating controls. However, pilots using this process

1099 sometimes had trouble analyzing existing or planned systems *without* including controls.

1100

1101 This created two challenges:

1102 1. Controls – either implemented or planned – can create an inaccurate assessment 1103 of existing or potential risks, and often created temptation for pilots to dismiss 1104 potential risks’ existence because they were already perceived as resolved. Just 1105 because a risk has been mitigated does not mean the risk does not exist at all – 1106 and understanding the sources of privacy risk in the system not only helps plan for 1107 mitigation strategies but will help agencies understand potential problems of

1108 perception, user discomfort, or misunderstanding that could create loss of trust in

1109 their system. Without analyzing unmitigated risk, agencies may leave an

1110 important output of privacy risk assessment on the table.

1111 2. Because an agency has implemented a control to mitigate privacy risk does not

1112 mean it is the most effective control. One benefit of risk assessment is the

1113 comparative evaluation of privacy controls. One control might be more costly, but 1114 may mitigate risk across a wider number of data actions. Another may be less 1115 effective, but affect risk in a way more aligned with the organization’s priorities. 1116 Some controls may be more appropriate to the current design roadmap for the 1117 system than other mechanisms. Effective privacy engineering is about making 1118 informed, consistent choices about privacy design that reflect the organization’s 1119 intentions and priorities, and without comparing the virtues of a variety of

1120 choices, that process is short-circuited.

1121

1122 *Personal Information*

1123

1124 It may be tempting for agencies to consider cataloging personal information only as what 1125 is familiar “PII” described in existing PIAs – Social Security Numbers, address, name, 1126 date of birth, etc. In order for these worksheets to be effective, agencies should consider 1127 personal information very broadly. Any information about an individual or that can be 1128 linked to an individual such as behavioral characteristics, should be cataloged in these 1129 worksheets. This includes information about session duration, login attempts, behavioral 1130 analysis – much of the information considered “metadata” or in system logs that are 1131 related to individual users can create privacy problems.

1132

*This page is intentionally blank.*

|  |  |  |
| --- | --- | --- |
| 1133 | *Appendix D: Worksheet 1* | page 1/3 |
| 1134 | | |
| 1135 | **Worksheet 1 has two tasks to complete:** |  |

|  |  |  |
| --- | --- | --- |
| 1136 |  | |
| 1137 | 1. | Frame business objectives. Frame the business objectives for the system(s), |
| 1138 |  | including the organizational needs served. |
| 1139 |  |  |
| 1140 | 2. | Frame organizational privacy governance. Frame the organizational privacy |
| 1141 |  | governance by identifying privacy‐related legal obligations, principles, |
| 1142 |  | organizational goals and other commitments. |
| 1143 |  |  |
| 1144 |  |  |
| 1145 |  |  |

### 1146 Task 1: Frame Business Objectives

1147

1. Describe the functionality of your system(s).

1148

1149

2. Describe the business needs that your system(s) serve.

1150

1151

1152

*Appendix D: Worksheet 1* page 2/3

1153

1154

3. Describe how your system will be marketed, with respect to any privacy‐ preserving functionality.

1155

1156

1157

### 1158 Task 2: Frame Organizational Privacy Governance

1159

1. Legal Environment: Identify any privacy‐related statutory, regulatory, contractual and/or other frameworks within which the system must operate. List any specific privacy requirements.

1160

1161

1162

*Appendix D: Worksheet 1* page 3/3

1163

1164

2. Identify any privacy‐related principles or other commitments to which the organization adheres (FIPPs, Privacy by Design, etc.).

1165

1166

3. Identify any privacy goals that are explicit or implicit in the organization’s vision and/or mission.

1167

1168

4. Identify any privacy‐related policies or statements within the organization, or business unit.

1169

1170

## This page is intentionally blank.

1171

*Appendix D: Use Case* page 1/1

1172

1173 The sample information filled out in worksheets 2 and 3 is based on the below use case (which describes a

1174 fictional company and situation).

1175

1176 Generic identity service provider (IDP) use case:

1177 ACME IdP service generates a high‐assurance identity credentialby combining:

1178  The individual’s (social site) online identity;

1179  An in‐person identity proofing event at a trusted third party office (e.g., UPS, FedEx location);

1180  A One Time Password (OTP) service to be usedas a second authentication factor.

1181 The high‐assurance credential will subsequently be used to verify the identity of the individual as they attempt to access

1182 governmentbenefits.

1183

1185

1186 Worksheet 2: Assessing System Design

1187 Purpose: Determining the risk for privacy of a particular data action in an information system requires determining the

1188 likelihood that a data action will be problematic (i.e. creates the potential for adverse effectson ind ividuals) and its impact (to 1189 be analyzed in worksheet 3). The purpose of this worksheet is to identify and catalog the inputs for this risk analysis. These 1190 inputs are the data actions being performed by the system, the personal information being processed by the data action, and 1191 relevant contextual factors.

1192

1193 Tasks:

1194 1. Map data processing within the system.

1195 2. Catalog general contextual factors.

1196 3. Catalog specific data actions, personal information being processed and unique contextual factors.

1197

1198

1199

1200

1201

1202

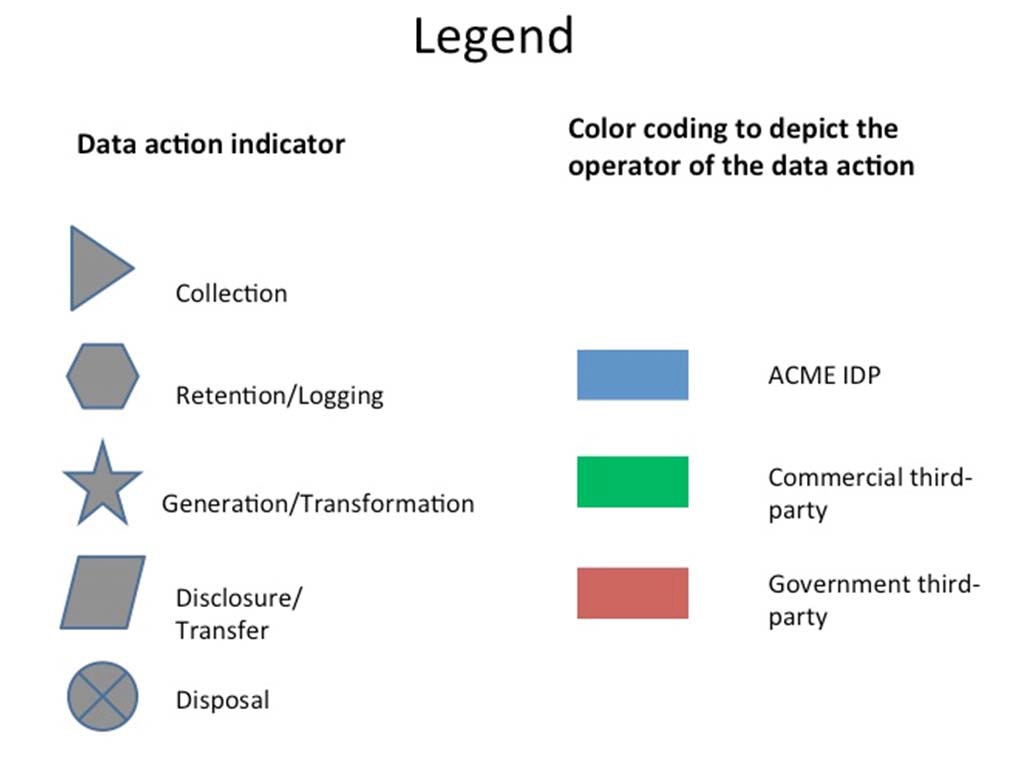
1203

1204

*Appendix D: Worksheet 2* page 2/7

1205

1206 Task 1: Map data processing within the system.

1207 

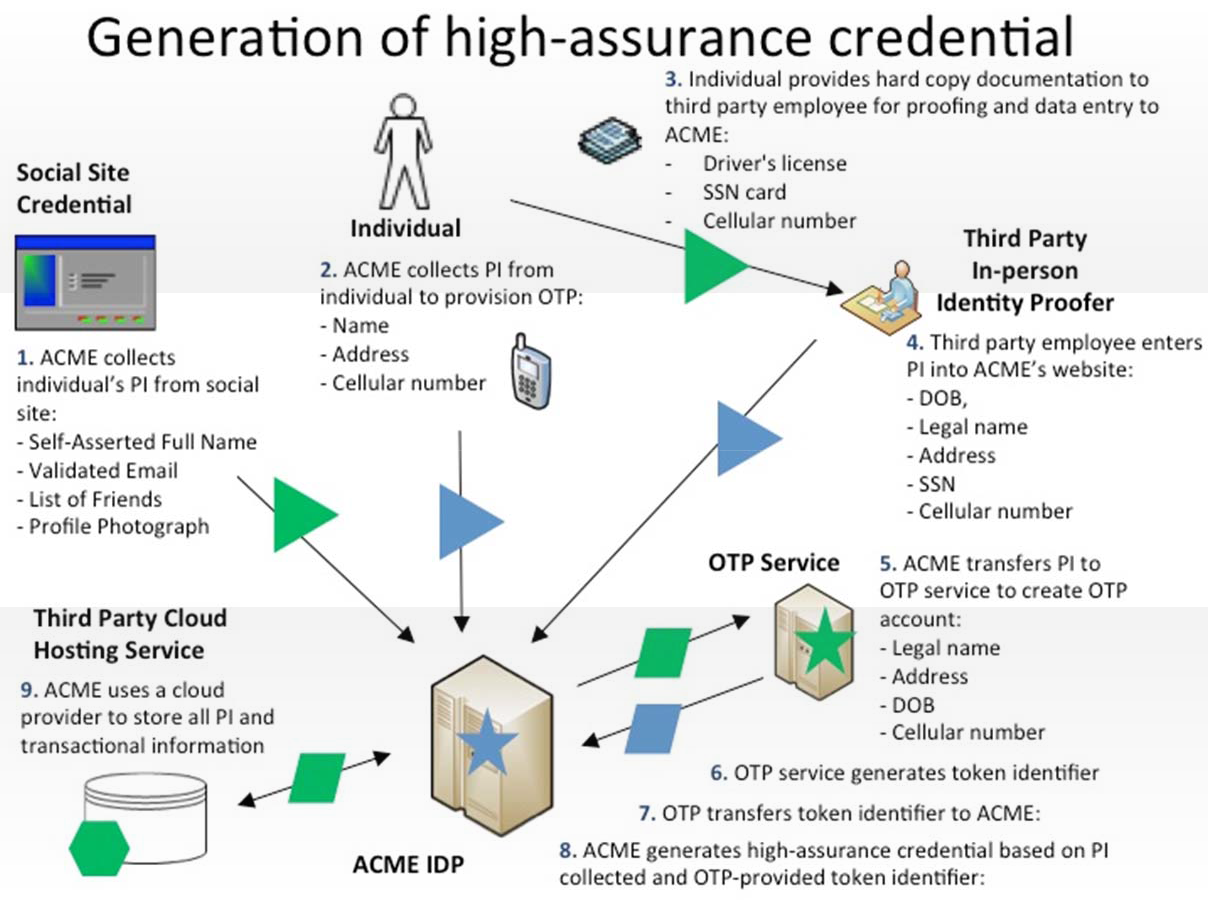
1208

1209

*Appendix D: Worksheet 2* page 3/7

1210

1211 Task 1: Map data processing within the system.

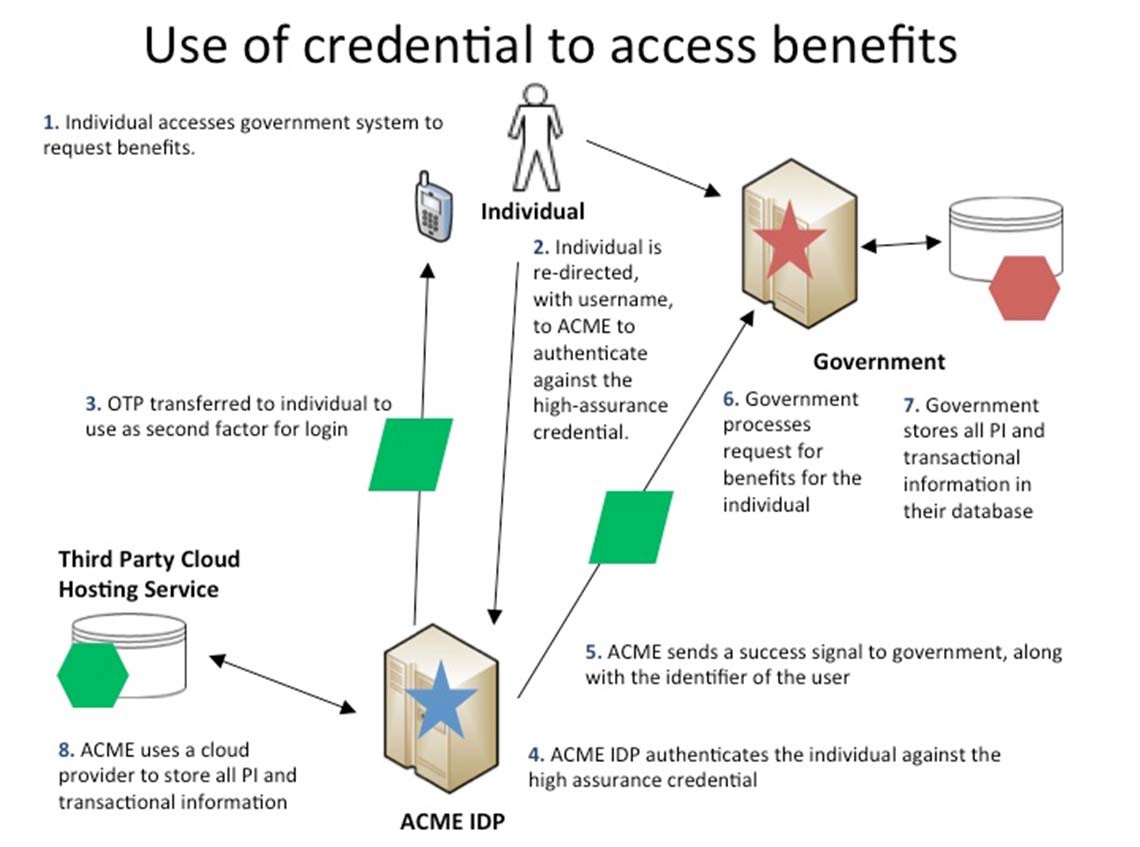
1212 

1213

1214 *Appendix D: Worksheet 2* page 4/7

1215

1216 Task 1: Map data processing within the system.

1217 

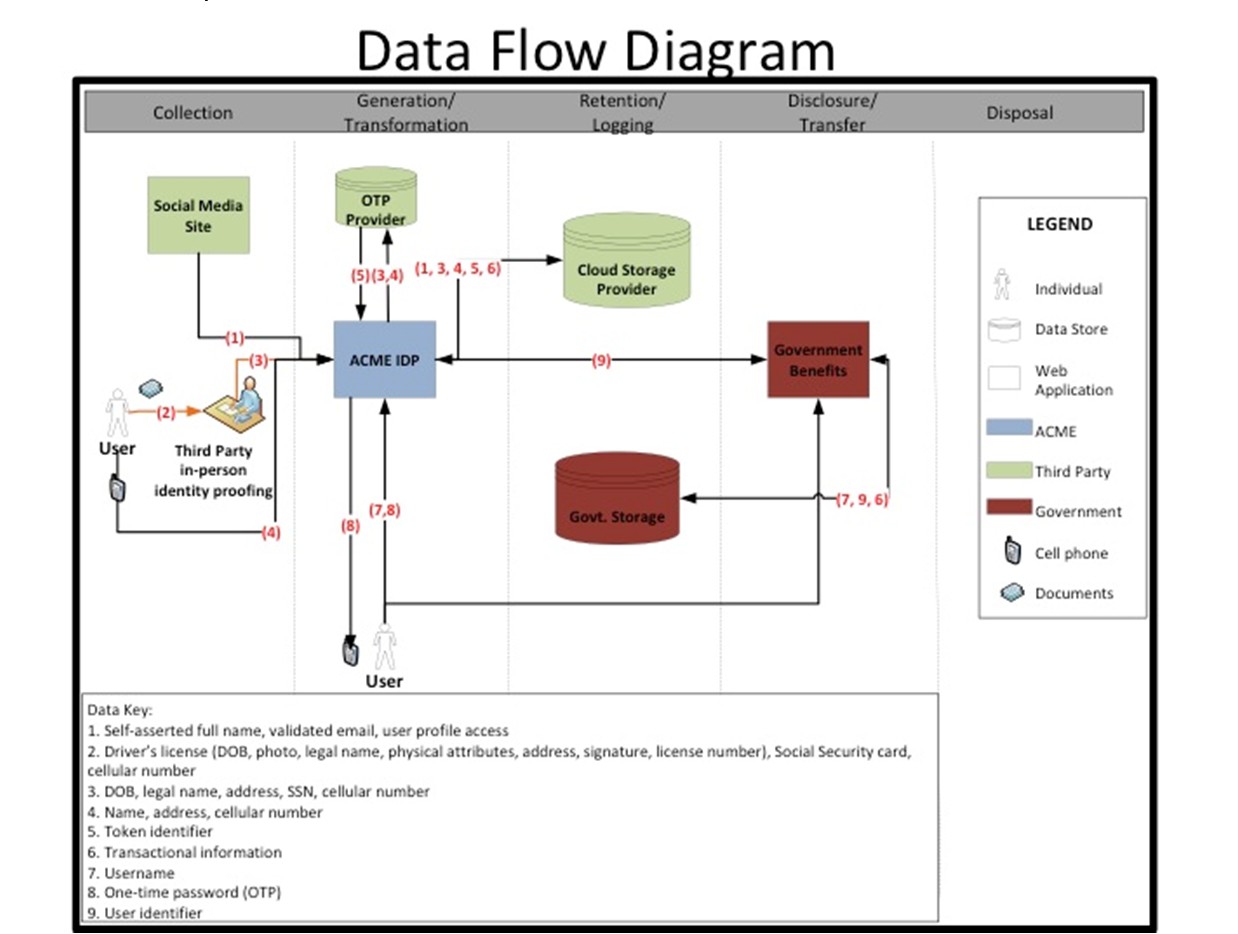
1218

1219

1220 *Appendix D: Worksheet 2* page 5/7

1221

1222 Task 1: Map data processing within the system.

1223 

1224

*Appendix D: Worksheet 2* page 6/7

1225

1226 Task 2: Catalog general contextualfactors.

1227

|  |  |  |  |
| --- | --- | --- | --- |
| Data Action | Personal Information | Specific Context | Summary Issues |
| Collection from the Social Media Site | ‐Self‐Asserted Full Name  ‐Validated Email  ‐List of Friends  ‐Profile Photograph | ‐One‐time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between user’s social media presence and ACME IDP  ‐Social credential linkingis vis ible touser  ‐Linking of social credential simplifies  access to government benefits system  ‐User profile may contain information the user considers sensitive  ‐User profile may contain information from other users not participating in the system  ‐User profile includes information unrelated to the purpose and operations of the system  ‐Access to PI is consented by user  ‐Nature of the API: full profile access is granted (by default: name, validated email, profile photograph, and list of friends) | ‐Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose.  ‐Will users understand the eventual high‐assurance credential is controlled by ACME and not by their social credential provider?  ‐How will perception of the social media organization’s privacy practices impact  users’ willingnessto consent to this data action?  ‐Will the user understand ACME will have ongoing access to information stored in their social profile?  ‐Will users’ social media privacy settings allow this data action? |

1228

1229

1230

1231

*Appendix D: Worksheet 2                       page 7/7*

1232

1233 Task 2: Catalog general contextualfactors.

|  |
| --- |
| **Example Contextual Factors** |
| Organizational |
| *System includes both government benefits agency and commercial service providers* |
| *Multiple privacy policies governing system* |
| *Public perception: high expectation of privacy with government benefits agency, low expectation with social credential provider* |
| *Relationships: No pre‐existing relationship with ACME IDP, regular interactions with government benefits agency, regular interactions with social credential provider* |
| System |
| *Personal information is not intended to be made public* |
| *New system, no history with affected individuals. Low similarity with existing systems/uses of social identity.* |
| *Four parties sharing personal information: one public institution, three private* |
| *ACME will use 3rd party cloud provider* |
| User |
| *High sensitivity about government benefits provided by system* |
| *Users exhibit various levels of technical sophistication* |
| *Potential user confusion regarding who "owns" the various segments of each system* |
| *20% of users use privacy settings at social provider* |

1234

## This page is intentionally blank.

1235

*Appendix D: Worksheet 3*

*page 1/6*

1236 Guidance

1237 **Likelihood:** Probability that a data action will become problematic for a representative or typical individual whose personal information is being

1238 processed by the system.

1239 **Calculation:** Determine on a scale from 1‐10 the estimated expected rate of occurrence for each potential problem for individuals whose

1240 personal information is being processed per data action.

1241 **Prior Worksheet Inputs:** Data actions and summary issues from worksheet 2.

1242 **Problematic Data Actions Catalog:** See *Appendix E.* The catalog may be used as a way to categorize the adverse effects that could arise from the

1243 issues or questions highlighted in the Summary Issues column. As noted in Worksheet 2, a summary issue may alleviate, rather than raise

1244 concerns about adverse effects. In that case, the summary issue should be scored as 0.

1245 **Potential Problems for Individuals Catalog:** See *Appendix F*. Problematic data actions may create the potential for more than one type of

1246 problem. However, some of the problems may have a higher likelihood of occurrence than others. If the data action ultimately is scored as risky,

1247 scoring the problems separately may help pinpoint what type of control would be most effective to mitigate the risk of the data action as a

1248 whole.

1249

**SAMPLE ‐ Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Actions** | **Summary Issues** | **Problematic Data Actions** | **Potential Problems for Individuals** | **Likelihood** |
| Collection fromthe social  media site | Full social credential profile access (including picture and list of friends)i s not necessary for fulfilling operational purpose. | ‐Appropriation  ‐Induced disclosure  ‐Surveillance  ‐Unanticipated revelation | Stigmatization: Information is revealed about the individual that they would prefer not to disclose. | 7 |
| Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage. | 2 |
| Will users understand the eventual high‐ assurance credentialis controlled by ACME and not by their social credential provider? | ‐The summaryissue will be associated with another data  action. |  | N/A |
| How will perception of the socialmedia organization’s privacy practices impact users’ willingness to consent to this data action? | ‐Induced disclosure  ‐Surveillance | Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information. | 6 |

1250

1251

1252

*Appendix D: Worksheet 3                       page 2/6*

1253 Guidance

1254 **Impact:** Cost to the organization of a data action if it became problematic for a representative or typical individual whose personal information is

1255 being processed by the system.

1256 **Calculation:** Determine on a scale of 1‐10 the estimated effect of each potential problem for individuals per data action on the business impact

1257 factors. The assigned values are added to calculate business impact per potential problem.

1258 **Prior Worksheet Inputs:** Relevant inputs from Worksheet 1. For example, in considering noncompliance costs, review the legal requirements or

1259 obligations identified in the legal environment box.

1260 Business Impact Factors

1261 **Noncompliance Costs:** Regulatory fines, litigation costs, remediation costs, etc.

1262 **Direct Business Costs:** Revenue loss from customer abandonment, etc.

1263 **Reputational Costs:** Brand, damage, loss of customer trust, etc.

1264 **Internal Culture Costs:** Impact on capability of organization/unit to achieve vision/mission. Consider impact on productivity/employee morale

1265 stemming from conflicts with internal cultural values.

1266 **Other:** Any other costs that an organization wants to consider.

1267 **SAMPLE ‐ Table**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Data**  **Actions** | **Summary Issues** | **Problematic**  **Data Actions** | **Potential**  **Problems for Individuals** | **Business Impact Factors** | | | | | **Total**  **Business Impact** |
|  |  |  |  | Noncompliance  Costs | Direct  Business Costs | Reputational  Costs | Internal  Culture Costs | Other |  |
| Collection  fromthe social media site | Full social credential profile access (including picture and  list of friends)i s not necessary for fulfilling operational purpose. | ‐Appropriation  ‐Induced disclosure  ‐Surveillance  ‐Unanticipated revelation | Stigmatization | 7 | 6 | 6 | 4 |  | 23 |
| Power Imbalance | 7 | 6 | 8 | 4 |  | 25 |
| How will perception of the socialmedia organization’s privacy  practices impact users’ willingness to consent to this data action? | ‐Induced disclosure  ‐Surveillance | Loss of Trust | 7 | 6 | 8 | 7 |  | 28 |

1268

*Appendix D: Worksheet 3 page 3/6*

1269 Guidance

1270 **Risk per Data Action**: Apply the risk equation to the outputs of the likelihood & impact tabs to determine the estimated risk per data action. The

1271 estimated likelihood per potential problem for individuals per data action is multiplied by its estimated business impact to yield the estimated

1272 risk per potential problem. The sum of the estimated risks for each potential problem for individuals is the estimated risk per data action.

1273 **SAMPLE ‐ Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data Actions** | **Potential Problems** | **Likelihood** | **Business Impact** | **Risk per Potential Problem** | **Risk per Data Action** |
| Collection from the social media site | Stigmatization | 7 | 23 | 161 | 379 |
| Power Imbalance | 2 | 25 | 50 |
| Loss of Trust | 6 | 28 | 168 |
| DA2 | Economic Loss | 6 | 32 | 192 | 317 |
| Loss of Autonomy | 5 | 19 | 95 |
| Exclusion | 2 | 15 | 30 |
| DA3 | Loss of Trust | 6 | 25 | 150 | 577 |
| Stigmatization | 7 | 36 | 252 |
| Loss of Liberty | 5 | 35 | 175 |
| DA4 | Loss of Trust | 5 | 48 | 240 | 240 |
| DA5 | Economic Loss | 6 | 37 | 222 | 821 |
| Loss of Autonomy | 5 | 20 | 100 |
| Power Imbalance | 3 | 25 | 75 |
| Exclusion | 8 | 33 | 264 |
| Stigmatization | 4 | 40 | 160 |
| DA6 | Loss of Trust | 5 | 22 | 110 | 438 |
| Loss of autonomy | 5 | 32 | 160 |
| Exclusion | 6 | 28 | 168 |
| DA7 | Loss of Autonomy | 8 | 43 | 344 | 659 |
| Stigmatization | 9 | 10 | 90 |
| Power Imbalance | 7 | 27 | 189 |
| Exclusion | 4 | 9 | 36 |
| DA8 | Loss of autonomy | 4 | 13 | 52 | 514 |
| Stigmatization | 9 | 32 | 288 |
| Power Imbalance | 8 | 15 | 120 |
| Exclusion | 6 | 9 | 54 |
| DA9 | Loss of Trust | 3 | 39 | 117 | 213 |
| Loss of Liberty | 2 | 48 | 96 |
| DA10 | Loss of Trust | 4 | 14 | 56 | 161 |
| Power Imbalance | 6 | 9 | 54 |
| Stigmatization | 3 | 17 | 51 |

1274

*Appendix D: Worksheet 3                       page 4/6*

1275 Guidance

1276 **System Risk Table:** Indicates the estimated risk presented by a data action, its estimated percentage of system risk, and its estimated ranking

1277 amongst other data actions. The risk column is the total estimated risk per data action and is colored to facilitate visual prioritization. The

1278 percent of system risk column is the estimated risk per data action relative to all other data actions. The rank among the data actions column

1279 assigns relative values to the data actions pursuant to their estimated system risk percentage.

1280 **SAMPLE – Data Action Risk Prioritization Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Actions** | **Risk** | **Percent of System Risk** | **Rank among Data Actions** |
| Collection from social media site | 379 | 9% | 6 |
| DA2 | 317 | 7% | 7 |
| DA3 | 577 | 13% | 3 |
| DA4 | 240 | 6% | 8 |
| DA5 | 821 | 19% | 1 |
| DA6 | 438 | 10% | 5 |
| DA7 | 659 | 15% | 2 |
| DA8 | 514 | 12% | 4 |
| DA9 | 213 | 5% | 9 |
| DA10 | 161 | 4% | 10 |
| Collection from social media site | 379 | 9% | 6 |

1281

1282

1283

*Appendix D: Worksheet 3                       page 5/6*

1284

1285 **SAMPLE – Two Dimensional Problem Prioritization Table (including 5 top highest likelihood & impact outliers)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Actions** | **Potential Problems** | **Point Label** | **Likelihood** | **Business Impact** |
| Collection from the social media site | Stigmatization | A | 7 | 23 |
| Power Imbalance | B | 2 | 25 |
| Loss ofTrust | C | 6 | 28 |
| DA2 | Economic Loss | D | 6 | 32 |
| Loss of Autonomy | E | 5 | 19 |
| Exclusion | F | 2 | 15 |
| DA3 | Loss ofTrust | G | 6 | 25 |
| Stigmatization | H | 7 | 36 |
| Loss ofL iberty | I | 5 | 35 |
| DA4 | Loss ofTrust | J | 5 | 48 |
| DA5 | Economic Loss | K | 6 | 37 |
| Loss of Autonomy | L | 5 | 20 |
| Power Imbalance | M | 3 | 25 |
| Exclusion | N | 8 | 33 |
| Stigmatization | O | 4 | 40 |
| DA6 | Loss ofTrust | P | 5 | 22 |
| Loss of autonomy | Q | 5 | 32 |
| Exclusion | R | 6 | 28 |
| DA7 | Loss of Autonomy | S | 8 | 43 |
| Stigmatization | T | 9 | 10 |
| Power Imbalance | U | 7 | 27 |
| Exclusion | V | 4 | 9 |
| DA8 | Loss of autonomy | W | 4 | 13 |
| Stigmatization | X | 9 | 32 |
| Power Imbalance | Y | 8 | 15 |
| Exclusion | Z | 6 | 9 |
| DA9 | Loss ofTrust Loss ofL iberty | AA BB | 3  2 | 39  48 |
| DA10 | Loss ofTrust | CC | 4 | 14 |
| Power Imbalance | DD | 6 | 9 |
| Stigmatization | EE | 3 | 17 |

1286

*Appendix D: Worksheet 3 page 6/6*

1287



**S**

**AA**

**O**

**K**

**H**

**I**

**Q**

**D**

**N**

**CR**

**U**

**B**

**M**

**P**

**G**

**A**

**EE**

**EL**

**F**

**CWC**

**Y**

**V**

**Z DD**

**Problem Prioritization Heat Map**

50

**BB**

**J**

45

40

35

30

**X**

25

20

15

10

**T**

5

0

0

1

2

3

4

5

**Likelihood**

6

7

8

9

10

**Impact**

1288

1289

1290 Appendix E: Catalog of Problematic Data Actions

1291

1292 **Appropriation:** Personal information is used in ways that exceed an individual’s expectation or authorization. Appropriation occurs 1293 when personal information is used in ways that an individual would object to or would have expected additional value for, absent an 1294 information asymmetry or other marketplace failure. Privacy harms that Appropriation can lead to include loss of trust, economic loss 1295 or power imbalance.

1296

1297 **Distortion**: The use or dissemination of inaccurate or misleadingly incomplete personal information. Distortion can present users in an

1298 inaccurate, unflattering or disparaging manner, opening the door for discrimination harms or loss of liberty.

1299

1300 **Induced Disclosure:** Pressure to divulge personal information. Induced disclosure can occur when users feel compelled to provide 1301 information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or 1302 privilege to an essential (or perceived essential) service. It can lead to harms such as power imbalance or loss of autonomy.

1303

1304 **Insecurity**: Lapses in data security. Lapses in data security can result in a loss of trust, as well as exposing individuals to economic

1305 loss, and stigmatization.

1306

1307 **Surveillance:** Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service. The 1308 difference between the data action of monitoring and the problematic data action of surveillance can be very narrow. Tracking user 1309 behavior, transactions or personal information may be conducted for operational purposes such as protection from cyber threats or to 1310 provide better services, but it becomes surveillance when it leads to harms such as power imbalance, loss of trust or loss of autonomy 1311 or liberty.

1312

1313 **Unanticipated Revelation:** Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways. 1314 Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give 1315 rise to stigmatization, power imbalance and loss of trust and autonomy.

1316

1317 **Unwarranted Restriction:** Unwarranted restriction to personal information includes not only blocking tangible access to personal 1318 information, but also limiting awareness of the existence of the information within the system or the uses of such information. Such 1319 restriction of access to systems or personal information stored within that system can result in harms such as exclusion, economic loss 1320 and loss of trust.

##### 1321 Appendix F: Catalog of Problems for Individuals

1322

1323 Loss of Self Determination

1324  Loss of autonomy: Loss of autonomy includes needless changes in behavior, including self-imposed restrictions on freedom of

1325 expression or assembly.

1326  Exclusion: Exclusion is the lack of knowledge about or access to personal information. When individuals do not know what 1327 information an entity collects or can make use of, or they do not have the opportunity to participate in such decision-making, it 1328 diminishes accountability as to whether the information is appropriate for the entity to possess or the information will be used 1329 in a fair or equitable manner.

1330  Loss of Liberty: Improper exposure to arrest or detainment. Even in democratic societies, incomplete or inaccurate information

1331 can lead to arrest, or improper exposure or use of information can contribute to instances of abuse of governmental power.

1332 More life-threatening situations can arise in non-democratic societies.

1333  Physical Harm: Actual physical harm to a person.

1334 **Discrimination**

1335  Stigmatization: Personal information is linked to an actual identity in such a way as to create a stigma that can cause

1336 embarrassment, emotional distress or discrimination. For example, sensitive information such as health data or criminal

1337 records or merely accessing certain services such as food stamps or unemployment benefits may attach to individuals creating

1338 inferences about them.

1339  Power Imbalance: Acquisition of personal information that creates an inappropriate power imbalance, or takes unfair

1340 advantage of or abuses a power imbalance between acquirer and the individual. For example, collection of attributes or

1341 analysis of behavior or transactions about individuals can lead to various forms of discrimination or disparate impact, including

1342 differential pricing or redlining.

1343 **Loss of Trust**

1344  Loss of trust is the breach of implicit or explicit expectations or agreements about the handling of personal information. For 1345 example, the disclosure of personal or other sensitive data to an entity is accompanied by a number of expectations for how 1346 that data is used, secured, transmitted, shared, etc. Breaches can leave individuals leave individuals reluctant to engage in 1347 further transactions.

1348 **Economic Loss**

1349  Economic loss can include direct financial losses as the result of identity theft to the failure to receive fair value in a

1350 transaction involving personal information.

##### 1351 Appendix G: Catalog of Contextual Factors

1352

|  |  |
| --- | --- |
| **Category** | **Contextual factors to consider** |
| **Organizational** | * The nature of the organizations engaged in the system such as public sector, private sector or regulated industry and how this factor might impact the data actions being taken by the system(s). * The public perception about participating organizations with respect to privacy. * The nature and history of user relationships with the organizations participatingin the system(s). |
| **System** | * The degree of connections to external systems and the nature of the data actions being conducted by those external systems such as retention, disclosure, or secondary use. * Any intended public exposure of personal information and the degree of granularity. * The nature and history of user interactions withthe system(s). * The degree of similarity between the operational purpose (e.g. goods or services being   offered) of this system and other systems that users have interacted with at participating organizations. |
| **Individuals** | * What is known about the privacy interests of the individuals whose information is being processed by the system. * The individuals' degree of information technology experience/understanding. * Any demographic factors that would influence the understanding or behavior of individuals with respect to the data actions being taken by thesystem (s). |
| **Data Action** | * The duration or frequency of the data actions being taken by the system(s). * How visible the data actions are to the individual. * The relationship between data actions being taken by the system(s) and the operational purpose. For example, in what manner or to what degree is the personal information being collected or generated contributing to the operational purpose? * The degree of sensitivity of the personal information, including particular piecesor the bundle as a whole. |

##### 1353 Appendix H: References

1354

1355 **LEGISLATION**

|  |  |  |
| --- | --- | --- |
| 1356 |  | |
| 1357 |  | 1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002. |
| 1358 |  |  |
| 1359 |  | 2. Privacy Act of 1974 (P.L. 107-56), December 1974. |
| 1360 |  |  |
| 1361 |  | **POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA** |
| 1362 |  |  |
| 1363 | 1. | Department of Health, Education, and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, |
| 1364 |  | *Records Computers and the Rights of Citizens*, June 1973. |
| 1365 |  |  |
| 1366 | 2. | Federal Trade Commission, Staff Report, *Internet of Things: Privacy and Security in a Connected World*, January 2015. |
| 1367 |  |  |
| 1368 | 3. | Government Accountability Office, Office of the Inspector General, *GAO’s Privacy Program: Opportunities Exist to Further* |
| 1369 |  | *Protect Personally Identifiable Information (PII)*, March 2015 |
| 1370 |  |  |
| 1371 | 4. | Government Accountability Office, Report to Congressional Requesters, *High-Risk Series: An Update*, February 2015. |
| 1372 |  |  |
| 1373 | 5. | Government Accountability Office, Report to Congressional Requesters, *Actions Needed to Address Weaknesses in* |
| 1374 |  | *Information Security and Privacy Controls*, September 2014. |
| 1375 |  |  |
| 1376 | 6. | National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February |
| 1377 |  | 2014. |
| 1378 |  |  |
| 1379 | 7. | The White House, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014. |
| 1380 |  |  |
| 1381 | 8. | The White House, Executive Office of the President, *National Strategy For Trusted Identities In Cyberspace: Enhancing* |
| 1382 |  | *Online Choice, Efficiency, Security, and Privacy*, April 2011. |

|  |  |  |
| --- | --- | --- |
| 1383 |  | |
| 1384 |  | **STANDARDS** |
| 1385 |  |  |
| 1386 | 1. | National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for* |
| 1387 |  | *Security Categorization of Federal Information and Information Systems*, February 2004. |
| 1388 |  |  |
| 1389 |  |  |
| 1390 |  | **GUIDELINES AND INTERAGENCY REPORTS** |
| 1391 |  |  |
| 1392 | 1. | National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for* |
| 1393 |  | *Securing Information Technology Systems,* September 1996. |
| 1394 |  |  |
| 1395 | 2. | National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing* |
| 1396 |  | *Cryptography in the Federal Government*, December 2005. |
| 1397 |  |  |
| 1398 | 3. | National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk* |
| 1399 |  | *Assessments*, September 2012. |
| 1400 |  |  |
| 1401 | 4. | National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk* |
| 1402 |  | *Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010. |
| 1403 |  |  |
| 1404 | 5. | National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk:* |
| 1405 |  | *Organization, Mission, and Information System View*, March 2011. |
| 1406 |  |  |
| 1407 | 6. | National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for* |
| 1408 |  | *Federal Information Systems and Organizations*, April 2013. |
| 1409 |  |  |
| 1410 | 7. | National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for* |
| 1411 |  | *Managers*, May 2007. |
| 1412 |  |  |

|  |  |  |
| --- | --- | --- |
| 1413 | 8. | National Institute of Standards and Technology Special Publication 1500-4, *Draft NIST Big Data Interoperability Framework:* |
| 1414 |  | *Volume 4, Security and Privacy*, April 2015. |
| 1415 |  |  |
| 1416 | 9. | National Institute of Standards and Technology Interagency Report 7628, Revision 1, *Guidelines for Smart Grid* |
| 1417 |  | *Cybersecurity: Volume 2 – Privacy and the Smart Grid*, September 2014. |
| 1418 |  |  |
| 1419 | 10. | National Institute of Standards and Technology Draft Interagency Report 8053, *De-Identification of Personally Identifiable* |
| 1420 |  | *Information*, April 2015. |
| 1421 |  |  |
| 1422 | 11. | National Institute of Standards and Technology Internal Report 8054, *NSTIC Pilots: Catalyzing the Identity Ecosystem*, April |
| 1423 |  | 2015. |
| 1424 |  |  |
| 1425 |  |  |