

Retired Draft

Warning Notice

The attached draft document has been RETIRED. NIST has discontinued additional development of this document, which is provided here in its entirety for historical purposes.

Retired Date October 05, 2022

Original Release Date April 02, 2015

Retired Document

Status Initial Public Draft (IPD)

Series/Number NIST IR 8050

Title Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy

Publication Date April 2015

Additional Information See <https://csrc.nist.gov> for information on NIST cybersecurity publications and programs.

EXECUTIVE TECHNICAL WORKSHOP ON IMPROVING CYBERSECURITY AND CONSUMER PRIVACY

Summary and Next Steps

Leah Kauffman
Nate Lesser
*National Cybersecurity Center of Excellence
Information Technology Lab*

Brian Abe
*The MITRE Corporation
McLean, VA*

DRAFT
April 2, 2015
consumer-nccoe@nist.gov

EXECUTIVE TECHNICAL WORKSHOP ON IMPROVING CYBERSECURITY AND CONSUMER PRIVACY

Summary and Next Steps

Leah Kauffman
Nate Lesser
*National Cybersecurity Center of Excellence
Information Technology Laboratory*

Brian Abe
*The MITRE Corporation
McLean, VA*

April 2015



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices. To learn more about the NCCoE, visit <http://nccoe.nist.gov>. To learn more about NIST, visit <http://www.nist.gov>.

ABSTRACT

Cybersecurity incidents have grown swiftly from conceivable to realized risks that regularly threaten national and economic security of the United States. These risks threaten the financial security of companies and the public, weaken consumer confidence, erode individual privacy protections, and damage the brand value and reputation of businesses. On February 12, 2015 the National Institute of Standards and Technology (NIST) and Stanford University hosted an executive technical workshop, held in coordination with the White House Summit on Cybersecurity and Consumer Protection, to discuss how to increase the use of advanced cybersecurity and privacy technologies in consumer-facing organizations. This document details the discussion and ideas presented at the workshop and serves as a platform to receive broader feedback on the relevance of projects and suggestions discussed at that event.

KEYWORDS

adaptive security; advanced detection; authentication; consumer protection; consumer-facing; cybersecurity; cybersecurity framework for critical infrastructure; cybersecurity standards; data integrity; decentralized systems; incident response; multi-factor authentication; privacy

DISCLAIMER

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 or NCCoE, nor is it intended to imply that the entities, materials or equipment are necessarily the best available for the purpose.

COMMENTS ON NCCoE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at <http://nccoe.nist.gov>.

Comments on this publication may be submitted to: consumer-nccoe@nist.gov

Public comment period: *April 2, 2015 – May 17, 2015*

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Amy Zegart and Dr. Herbert Lin of Stanford University, Ms. Kiersten Todt of Liberty Group Ventures, as well as the workshop participants who provided valuable input to this report.

1 INTRODUCTION

2 On February 12, 2015 the National Institute of Standards and Technology (NIST) and
3 Stanford University hosted a workshop with chief technology officers, chief information
4 officers, and security executives in consumer-facing organizations to discuss how to
5 increase the use of advanced cybersecurity and privacy technologies throughout their
6 sectors.

7 This document is a summary of the workshop, which was held in coordination with the
8 White House Summit on Cybersecurity and Consumer Protection. The National
9 Cybersecurity Center of Excellence (NCCoE) will initiate projects—described in the “Next
10 Steps” section—informed by the workshop. NIST is seeking broader feedback on the
11 relevance of these projects and suggestions about additional steps that can be taken to
12 foster improvements across these diverse organizations.

13 NIST would like feedback on the topics and ideas contained in this document. Respondents
14 should include the name of the person or organization filing the comment, although
15 anonymous comments will be accepted. All comments received are a part of the public
16 record and will generally be posted to <http://nccoe.nist.gov/consumer> without change.
17 Comments should be submitted at <http://nccoe.nist.gov/consumer> or by emailing them to
18 consumer-nccoe@nist.gov. All personal identifying information (for example, name and
19 address) voluntarily submitted by the commenter may be publicly accessible. Do not submit
20 confidential business information or otherwise sensitive or protected information.

21 NIST is planning another workshop in the summer of 2015 to follow up on many of these
22 same issues. For updates on future workshops and the most up-to-date status of the
23 projects resulting from these workshops, visit <http://nccoe.nist.gov/consumer>.

24 SUMMARY

25 A wide variety of consumer-facing organizations were represented at the workshop, from
26 banking and consumer products companies, to technology and health care providers, with
27 differences in geography, scale and available resources. Despite the range of businesses
28 represented, with different infrastructures and risk profiles, several key points emerged as
29 potential focus areas for future work. At the highest level, given their interactions with
30 consumers, participants quickly came to consensus that security, privacy, and usability
31 concerns are paramount as they consider protections for corporate and customer
32 information and assets.

33 Participants discussed the need for organizations to protect both consumer and corporate
34 data. While consumers might consider businesses to be responsible for the customer data
35 they hold, the workshop participants saw this as a shared responsibility. In addition to the
36 security programs they put in place, organizations can help strengthen cybersecurity
37 protections for their customers through education, training, transparent and clear privacy
38 policies, and cybersecurity measures that are easier for consumers to use.

39 Much of the focus of the day also looked at how to get cutting-edge cybersecurity
40 technology into the hands of those in industry that deploy it. There were discussions around
41 how software and application developers should be seen as consumers as well, and that
42 often the demand for additional features and better performance inhibits developers from
43 incorporating more sophisticated security features. The participants concluded that
44 developer tools, therefore, should make it easier to include security in software, without
45 compromising performance. Automated security that reduces the need for human
46 operators (e.g. tools that are able to dial up and down protection mechanisms based on a
47 changing threat landscape) was another common theme.

48 On the topic of implementation, workshop participants agreed that cybersecurity products
49 and services must be easier for security technologists to use. While a myriad of tools and
50 technologies are available today, there are serious challenges to adoption in consumer-
51 facing organizations.

52 Specifically, workshop participants articulated challenges in implementing a variety of
53 technologies, including:

- 54 • authentication and multi-factor authentication
- 55 • advanced detection
- 56 • recovery tools
- 57 • adaptive security in response to a changing threat environment
- 58 • data integrity, not just data confidentiality
- 59 • third-party access to key corporate systems
- 60 • decentralized systems
- 61 • network traffic analysis

62 Finally, in addition to the issues above, workshop participants invited the entire
63 cybersecurity community—people from government, industry, and academia—to
64 collaborate to address the larger issues of security usability, consumer training, regulatory
65 harmonization, third-party agreements and assessments, and transparency and clarity
66 regarding privacy. Participants expressed a commitment to continue to work together on
67 these issues and suggested that NIST could act as a convener for specific technical topics.

68 **KEY POINTS**

69 Workshop participants discussed in detail a variety of technical topics and challenges,
70 described below.

71 **Increase Education and Training**

72 Further education and training for five broad populations was highlighted.

73 For consumers, the flexibility of technology and ease of use has trumped security
74 historically. Consumers might see additional security controls as an annoyance. In general,

75 for this population, there are challenges in understanding the threat and steps individuals
76 can take to protect their data.

77 For businesses, employees, not technologies, tend to be the weakest link in a business's
78 security chain. Participants stated that security breaches, due to lost credentials, happen
79 more often than breaches caused by malware, with employees falling prey to increasingly
80 sophisticated phishing attempts. In addition, business owners and managers may not full
81 understand the need to implement cybersecurity capabilities.

82 For developers, common programming mistakes and the reuse of code found online help to
83 propagate unsecure applications. Additionally, participants stated that software release
84 dates are often driven by the need for increased functional requirements making it difficult
85 for developers to adequately account for security as part of the software development life
86 cycle.

87 For cybersecurity professionals, high demand in the marketplace creates significant career
88 mobility. While beneficial in elevating cybersecurity concerns, this also demonstrates the
89 need for more well trained cybersecurity professionals. Consistency across training
90 mechanisms (certifications, degree programs, vocational training) is necessary to ensure
91 this workforce remains up-to-date on the latest cybersecurity challenges and solutions as it
92 grows to meet demand.

93 **Protect Privacy**

94 Consumers interact with retailers and providers in a variety of ways enabled and enhanced
95 by networked technologies: joining shopper rewards program, paying bills from a digital
96 wallet, registering with online sellers to automate and track purchases, using mobile
97 applications for purchases on the go, completing health records and managing bank
98 accounts online. These capabilities have changed user experiences while allowing retailers
99 and providers to collect customer, client, and patient data with a greater level of veracity,
100 but they also pose privacy concerns to people who entrust businesses with their personal
101 information, payment card data, and purchase patterns. This trust can only be maintained if
102 the personal data of customers, clients, and patients is properly secured. Participants said
103 that the loss of corporate reputation among the people they serve is more damaging and
104 concerning than non-compliance with regulation and even potentially the loss of corporate
105 data. The stakes for organizations are extremely high in this arena and further enhance the
106 need for corporations to prioritize the implementation of technology to increase these
107 protections.

108 **Make Security Easier**

109 Organizations of all sizes, but particularly smaller organizations with proportionally-sized
110 resources, need technology that simplifies security instead of relying on individual
111 expertise. Technical solutions must be easily integrated and user friendly. Those that are
112 difficult to integrate, configure, and maintain essentially create their own barrier to entry
113 because they become expensive and require a higher level of subject matter expertise that

114 is not attainable for every business. Additionally, technical solutions must consider how
115 they integrate with users and business processes. Simplifying these integrations will reduce
116 cost and other barriers to implementation. Workshop participants also expressed a need for
117 tiered security measures, so that different kinds of employees with different levels of access
118 can be easily granted different levels of security.

119 **Detect and Act Early**

120 Businesses must have the ability to detect attacks – which are seen as inevitable – as soon
121 as possible. New technologies are needed to improve detection. This could include
122 assistance with sorting through large amounts of network and system data, reduction in
123 false positive alerts, and identification of useful intelligence about an attack. Once detected,
124 it is important to eliminate the threat, and quickly evaluate the extent of any compromised.

125 Independent of detection, proactive measures are also an important component of quick-
126 reaction solutions. Businesses must be able to reduce their attack surface and therefore
127 reduce the complexity, variability, and cost associated with security. Building agility into the
128 security solution will allow organizations to shift controls to new threat vectors
129 independent of an attack taking place.

130 **Make Authentication Stronger and More Useable**

131 Workshop participants agree that passwords alone no longer provide sufficient protection
132 for the assets they are meant to safeguard. The security infrastructure, therefore, must be
133 transitioned to rely on stronger authentication and authorization mechanisms, including
134 two-factor authentication. There are, however, challenges associated with this approach.
135 Any given organization is likely to have a different tolerance for balancing risk, security, and
136 usability for its employees and customers. For example, executives might mandate two-
137 factor authentication for employees, but hesitate to do so with customers due to the risk of
138 losing those customers to competitors.

139 While new technologies and approaches are emerging and consumer adoption is increasing,
140 consumer-facing organizations worry about backlash from moving to stronger
141 authentication technologies. If a security measure negatively impacts the user experience,
142 the consumer may choose a competitor's easier-to-use service. This makes it risky for a
143 company to force its consumers away from passwords. Companies that allow consumers to
144 opt for two-factor authentication find that they usually don't, perhaps due to limited
145 awareness of the security shortcomings associated with password authentication. Effective
146 education is need to help ease consumers' adoption of stronger authentication
147 mechanisms.

148 **Address New Payment Technologies**

149 Even as new credit card payment methods become mainstream, consumers still have a
150 traditional notion of the payment experience: they hand their card to a salesperson and it is
151 returned with a receipt needing a signature. Workshop participants speculated about how

152 new payment methods such as credit cards with chip-and-pin technology work amidst those
153 expectations, and suggested that more consumer education is required to increase use of
154 these more secure methods. Nevertheless, they agreed that traditional credit cards will not
155 go away quickly, and new risks will continue to emerge. Therefore, it remains vital to
156 identify mechanisms for securing existing magnetic swipe-based transactions.

157 To compound the issue surrounding payment in general, there are several distinct, yet
158 connected, components of the systems that must be considered. First, the payment type
159 itself can vary. Consumer-facing organizations contend with touchless payment options,
160 new cards with imbedded chips, and traditional credit cards. Then, there is diversity among
161 point-of-sale systems themselves. They can range from devices that plug into a smart phone
162 to standalone systems that do not do real-time processing, to integrated systems that feed
163 directly into an organization's network. The ecosystem that supports the transmission of
164 the data from the point-of-sale device to the financial institution introduces an additional
165 set of complexities as well. Each component and variation of the system comes with its own
166 security challenges and potentially the need for distinct technology solutions to provide
167 enhanced protection of consumer data.

168 **Increase Focus on Data Integrity**

169 As organizations assess their risks, they often focus on what can be stolen and used for
170 profit, like intellectual property or customer records. Workshop participants stated that
171 organizations also need to be concerned with data integrity. For example, instead of only
172 being stolen in a breach, data can also be altered to cause financial harm, compromise
173 safety of customers or workers, and disrupt a supply chain. Workshop participants indicated
174 that data integrity is often overlooked when focusing on confidentiality and availability.

175 **Account for Decentralized Environments**

176 Decentralized workforces increase the complexity of an organization's security profile in
177 two ways. First, a company must deal with varying laws and regulations; second, a
178 decentralized IT infrastructure makes it more difficult to ensure that updates and patches
179 are distributed and implemented. Companies that have branches run by franchisees find it
180 difficult to standardize security profiles because the national brand doesn't necessarily have
181 proper oversight mechanisms.

182 **Secure Third-Party Access**

183 For the purposes of conducting day-to-day business, organizations commonly allow third
184 parties (customers, vendors, contractors, service providers, and others) to access their
185 networks, systems, and data. This access needs to be evaluated, controlled, and accounted
186 for in organizations' risk management plans. Ascertaining how these relationships affect an
187 organization's risk posture is both non-trivial and critical. Participants discussed the need
188 for guidance on how to better structure these relationships and implement protections
189 around critical assets.

190 **Make Attacks More Costly and Demonstrate that Security Pays**

191 Most perpetrators of cybersecurity attacks do not experience consequences, and attacks
192 can be launched with little investment in personnel, equipment, or software. Technology is
193 key to making attacks harder to perpetrate, more costly to attackers, and easier to
194 investigate. To avoid indiscriminately spending limited resources, business must understand
195 what information is valuable so they can focus on what needs the most protection.
196 Additional steps like data encryption and intelligent data separation can make it harder for
197 attackers to gain valuable data.

198 Traditionally, when digital assets like customer and employee records were a byproduct of
199 traditional business models, security was a function of the IT department. Now that those
200 records can be businesses' most valuable assets, safeguarding them must be thought of as a
201 key business driver. Information technology security executives must think of security in
202 terms of business value. To get the attention of chief executives, chief information,
203 technology, and information security officers need to use metrics that resonate with their
204 business leaders, communicating clear outcomes that can be accomplished through
205 investments in security.

206 **Balance Between Regulation and Security**

207 While largely out of scope for this workshop, participants noted that when regulatory
208 compliance and security are in conflict, companies often prioritize regulatory compliance.
209 This issue is compounded in sectors where organizations are subject to regulations that
210 differ by jurisdiction or function.

211 **Apply the NIST Cybersecurity Framework to Consumer-Facing Organizations**

212 The NIST Framework for Improving Critical Infrastructure Cybersecurity was discussed
213 several times during the workshop as a tool to help consumer-facing organizations to
214 understand, communicate, and manage cybersecurity risk in the context of their enterprise
215 mission and business objectives. Participants expressed interest in understanding how NIST
216 and other cybersecurity standards, practices, and reference implementations relate to the
217 Framework, and how those resources can help consumer-facing organizations achieve their
218 cybersecurity priorities.

219 **EXISTING RESOURCES**

220 NIST is not the only organization addressing cybersecurity in consumer-facing organizations.
221 Many of the ideas expressed at the workshop dovetail with existing programs in
222 government, industry working groups and trade associations, academia, and public-private
223 partnerships. The Appendix to this document lists NIST programs dedicated to enhancing
224 cybersecurity.

225 **NEXT STEPS**

226 The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of
227 Standards and Technology (NIST) collaborates with technology vendors to demonstrate
228 standards-based example solutions to cybersecurity challenges using commercially available
229 products. Below is a list of potential projects under consideration that directly addresses
230 some of the issues raised during the technical workshop. Feedback will help determine
231 prioritization – with a goal of beginning with projects that would be most beneficial to
232 consumers and consumer-facing organizations.

We are seeking comments on the potential projects described below. Are these the most valuable projects? Are they scoped correctly? How should these efforts be prioritized? Are there higher priority projects on which we should focus?

233 **Data Integrity**

234 The NCCoE is considering a project that provides and verifies data integrity. For these
235 purposes, a violation of integrity can be viewed as any unauthorized change in data,
236 malicious or accidental, that is not immediately detected and remedied. The project might
237 explore database integrity, file integrity, system integrity, and the integrity of backups.
238 Technologies to examine might include auto-journaling file systems, cryptographic file
239 checksums, detailed auditing, virtual machine snapshots, and versioning software.

240 This project might explore specific questions, including:

- 241 • What was altered during a breach?
- 242 • What was the impact of the data alteration? This examination needs to include
243 traditional IT, mobile, cloud, and mainframe systems.
- 244 • From which backup version should an organization restore?
- 245 • After discovering and removing malicious code operating in an organization's
246 environment, from which backup version should the organization restore data,
247 applications, and services?

248 In addition to ensuring that the backup is of a known “good” image, this project should
249 examine questions of how to ascertain that vulnerabilities, weakness, and malware are not
250 reintroduced during the restoration.

What existing technologies enable organizations to maintain the integrity of systems, applications, files, databases, and backups?

251 *Relevant Cybersecurity Framework Functions and Categories: PR.DS, PR.IP, PR.PT, DE.AE,*
 252 *RS.RP, RS.AN, RS.MI, RC.RP, RC.IM.*

253 **Developer Tools**

254 Software systems have become increasingly complex, even while developers try to shorten
 255 development cycles. Complexity breeds flaws, which can be exploited to breach system
 256 security. As network security improves, attackers are targeting applications directly. To help
 257 address this growing software complexity problem, the NCCoE is considering a project to
 258 demonstrate the capabilities of software developer tools and environments that increase
 259 software assurance. This project might include static analysis, component architecture,
 260 dynamic analysis and other runtime analysis tools, and live vulnerability scanning and
 261 penetration analysis techniques.

262 This project might explore specific questions, including:

- 263 • What tools, development environments, and techniques enable secure code
 264 development?
- 265 • What tools can be put in the development environment to provide meaningful real-
 266 time feedback to improve developer knowledge on secure coding techniques, as
 267 well as integration-level feedback to catch vulnerabilities?
- 268 • Which existing and/or emerging languages provide inherent security benefits and
 269 what is needed to increase the use of these languages?
- 270 • What tools can be implemented to analyze external libraries and services as well as
 271 externally developed code components?

272 *Relevant Cybersecurity Framework Functions and Categories: ID.AM, ID.BE, ID.RA, ID.RM,*
 273 *PR.AC, PR.AT, PR.DS, PR.IP, PR.MA, PR.AT PR.PT.*

What existing technologies enable automated code reviews including static analysis, runtime analysis including dynamic analysis, live vulnerability scanning, and penetration analysis?

274 **Automated Information Sharing and Incident Response**

275 Organizations engaged in the sharing of information related to cybersecurity risks and
 276 incidents play an invaluable role in the collective cybersecurity of the nation. Barriers to
 277 participation in information sharing initiatives include cost, liability concerns, lack of
 278 standards, lack of a mutual taxonomy, and technology gaps related to automated
 279 anonymization, ingestion, filtering, and incident response. To help reduce these barriers,
 280 the NCCoE is considering a project that demonstrates technical tools and methods for the
 281 automated sharing and use of cybersecurity information.

282 This project might address a number of specific questions, including:

- 283 • How can trusted and unknown partners securely share sensitive data, such as the
284 actual attack vector detected or vulnerability identified?
- 285 • Can data be anonymized to address sensitivity, privacy concerns, and legally
286 protected information?
- 287 • Can protection tools and measures be readily updated through the exchange of
288 standards-based threat indicators?
- 289 • What technologies can automate the response to (and recovery from) a security
290 breach once detected.
- 291 • What current technology blends the need for human-in-the-loop responses to new
292 and sophisticated cyber-attacks with tools that learn from those responses?
- 293 *Relevant Cybersecurity Framework Functions and Categories: ID.RA, ID.RM, PR.DS, PR.MA,*
294 *PR.PT, DE.AE, DE.CM, DE.DP, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM.*

What existing technologies enable and automate sharing of sensitive information, anonymization, machine learning, and incident response resolution?

295 **Point of Sale/Payment Cards**

296 To address concerns surrounding the use and implementation of point-of-sale systems and
297 payment options such as traditional swipe cards, chip and pin cards, and touchless
298 payments, the NCCoE is considering a project to demonstrate security mechanisms that can
299 better protect information related to a consumer transaction.

300 This project might address a number of specific scenarios, including:

301 Technologies that can help secure different payment options

- 302 • How can an organization deploy technology to better secure consumer information
303 for customers who use touchless payment options?
- 304 • How can the organization enhance the security around the wireless connection
305 portion of the transaction?
- 306 • What other attack vectors might circumvent the security features of new payment
307 technologies?

308 Enhanced security for point-of-sale systems

- 309 • Are new point-of-sale devices providing enhanced protection to avoid the loss of
310 consumer data from traditional cards?
- 311 • Are new point-of-sale devices providing enhanced protection to avoid the loss of
312 consumer data from new payment options?

- 313 • If not, what are other technologies that can be implemented to provide enhanced
314 security for customers who continue to use traditional credit cards?

315 *Relevant Cybersecurity Framework Functions and Categories: ID.AM, PR.AC, PR.DS, PR.MA,*
316 *PR.PT, DE.AE*

What existing technologies enable increased security for different payment options and point-of-sale devices?

317 **External Entity Access**

318 Allowing an external entity to access internal IT infrastructure, resources, and data creates a
319 multitude of security issues. Whether the external entity is a different organization or a
320 different operating unit within the same organization, mechanisms are needed to protect
321 critical business and organizational functions. To address these concerns, the NCCoE is
322 considering a project to explore technologies that can be integrated to create secure
323 connections between and among entities, as well as allow for the monitoring of data access
324 and movement (inbound and outbound) as a result of these connections.

325 This project might explore specific questions, including:

- 326 • When connecting directly with external entities, what technologies can be employed
327 to provide logical separation of data and ensure that the outside organization has
328 access only to the resources necessary to conduct business?
- 329 • How can those technologies be configured to reduce or eliminate performance
330 degradation of an organization’s network, but still be secure?
- 331 • How can an organization monitor what is coming in through (and going out of the
332 connection) to an outside entity? Can these technologies detect structured and
333 unstructured data such as social security and credit card numbers or geolocation
334 data passed through the connection?
- 335 • If the data shared with the outside entity is encrypted, what tools exist to still ensure
336 that it contains only the appropriate information before leaving the security
337 boundary?
- 338 • What can we do to provide protection for an organization’s information that is
339 outside its boundary?

340 *Relevant Cybersecurity Framework Functions and Categories: PR.AC, PR.DS, PR.MA, PR.PT,*
341 *DE.AE, DE.CM, DE.DP, RS.CO, RS.AN, RS.MI, RC.RP, RC.CO*

What existing technologies can assess connections to external entities, monitor activity and the type of data transmitted, and can prevent access to off-limits resources?

342

343 **COMMENTS**

344 **Feedback**

345 NIST would like feedback on the topics and ideas contained in this document. Respondents
346 should include the name of the person or organization filing the comment, although
347 anonymous comments will be accepted. All comments received are a part of the public
348 record and will generally be posted to <http://nccoe.nist.gov/consumer> without change.
349 Comments should be submitted at <http://nccoe.nist.gov/consumer> or by emailing them to
350 consumer-nccoe@nist.gov. All personal identifying information (for example, name and
351 address) voluntarily submitted by the commenter may be publicly accessible. Do not submit
352 confidential business information or otherwise sensitive or protected information.

353 NIST is planning another workshop in the summer of 2015 to follow up on many of these
354 same issues. For updates on future workshops and the most up-to-date status of the
355 projects resulting from these workshops, visit <http://nccoe.nist.gov/consumer>.

356 **Join the Community**

357 To develop a project, the NCCoE forms a community of interest made up of companies who
358 are facing similar challenges. The community will help to ensure that any NCCoE work
359 addresses the most pressing concerns of the community, and that the supporting
360 architectures created accurately depict representative architectures from the community.
361 Once a technical description of the problem is finalized, including a map of the necessary
362 security characteristics to applicable standards and best practices, the NCCoE works with
363 technology providers to bring products into a laboratory environment where they are
364 joined together to create a potential solution. The NCCoE then publishes a practice guide to
365 assist companies in adopting technologies with similar characteristics.

366 You can join the community formed around issues in your sector at any time. You'll get
367 news about projects underway, requests to contribute comments, and alerts about newly-
368 launched projects. Visit <http://nccoe.nist.gov> to explore our work and sign up for alerts
369 from NCCoE.

370 APPENDIX: NIST RESOURCES

371 The NIST mission is to promote U.S. innovation and industrial competitiveness by advancing
372 measurement science, standards, and technology in ways that enhance economic security
373 and improve our quality of life.

374 Computer Security Division

375 Conducts research and develops standard, guidelines, tests, and metrics for protecting non-
376 national security federal information and communications infrastructure.

377 <http://csrc.nist.gov/>

378 Framework for Improving Critical Infrastructure Cybersecurity

379 Voluntary guidance, based on existing standards, guidelines, and practices, for critical
380 infrastructure to better manage and reduce cybersecurity risk, and foster cybersecurity risk
381 management communications among internal and external organizational stakeholders.

382 <http://www.nist.gov/cyberframework/>

383 National Cybersecurity Center of Excellence

384 Develops example solutions that show how standards and best practices can be
385 implemented in the real world. <http://nccoe.nist.gov/> and <http://nccoe.nist.gov/projects>

386

387 National Initiative for Cybersecurity Education

388 Promotes development of a cybersecurity workforce. <http://csrc.nist.gov/nice/>

389 National Strategy for Trusted Identities in Cyberspace

390 Dedicated to more secure alternatives to passwords. NSTIC seeks to improve the privacy,
391 security, and convenience of online transactions. <http://www.nist.gov/nstic/>

392 NIST Privacy Engineering Initiative

393 Developing a risk management approach for privacy within the federal government to
394 facilitate better identification of privacy risk in information systems and support the
395 development and implementation of more effective technical standards to mitigate privacy
396 risk. http://csrc.nist.gov/projects/privacy_engineering/