
CRITICAL CYBERSECURITY HYGIENE: PATCHING THE ENTERPRISE

Murugiah Souppaya

Kevin Stine

National Institute of Standards and Technology

Mark Simos

Sean Sweeney

Microsoft

Karen Scarfone

Scarfone Cybersecurity

DRAFT

August 31, 2018

cyberhygiene@nist.gov



1 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of
2 Standards and Technology (NIST), is a collaborative hub where industry organizations,
3 government agencies, and academic institutions work together to address businesses' most
4 pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular,
5 easily adaptable example cybersecurity solutions demonstrating how to apply standards and
6 best practices using commercially available technology. To learn more about the NCCoE, visit
7 <https://www.nccoe.nist.gov>. To learn more about NIST, visit <https://www.nist.gov>.

8 This document describes a problem that is relevant to many industry sectors. NCCoE
9 cybersecurity experts will address this challenge through collaboration with a community of
10 interest, including vendors of cybersecurity solutions. The resulting reference design will detail
11 an approach that can be incorporated across multiple sectors.

12 **ABSTRACT**

13 Cyber hygiene describes recommended mitigations for the small number of root causes
14 responsible for many cybersecurity incidents. Implementing a few simple practices can address
15 these common root causes. Patching is a particularly important component of cyber hygiene,
16 but existing tools and processes are frequently insufficient to rapidly mitigate this risk in many
17 environments and situations. The objective of this project is to demonstrate a proposed
18 approach for improving enterprise patching practices for general IT systems. Commercial and
19 open source tools will be used to aid with the most challenging aspects of patching, including
20 system characterization and prioritization, patch testing, and patch implementation tracking and
21 verification. These tools will be accompanied by actionable, prescriptive guidance on
22 establishing policies and processes for the entire patching life cycle, in the form of a freely
23 available NIST Cybersecurity Practice Guide.

24 **KEYWORDS**

25 *cyber hygiene; incidents; patching; security hygiene; software updates; vulnerabilities*

26 **DISCLAIMER**

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

32 **COMMENTS ON NCCoE DOCUMENTS**

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

36 Comments on this publication may be submitted to: cyberhygiene@nist.gov

37 Public comment period: August 31, 2018 to October 1, 2018

38 **TABLE OF CONTENTS**

39 **1 Executive Summary.....4**

40 Purpose 4

41 Scope..... 4

42 Assumptions/Challenges..... 5

43 Background 5

44 **2 Scenarios6**

45 Scenario 0: Asset identification and assessment..... 6

46 Scenario 1: Routine patching 6

47 Scenario 2: Routine patching with cloud delivery model 6

48 Scenario 3: Emergency patching..... 7

49 Scenario 4: Emergency workaround (and backout if needed) 7

50 Scenario 5: Isolation of unpatchable assets..... 7

51 Scenario 6: Patch management system security (or other system with administrative

52 privileges)..... 7

53 **3 High-Level Architecture.....8**

54 Component List 10

55 Desired Requirements 11

56 **4 Relevant Standards and Guidance12**

57 Secure Update Guidelines..... 12

58 Microsoft Software Update Guides 12

59 **5 Security Control Map12**

60 **Appendix A References.....14**

61 **Appendix B Acronyms and Abbreviations.....15**

62 1 EXECUTIVE SUMMARY

63 Purpose

64 This document defines a National Cybersecurity Center of Excellence (NCCoE) project focused on
65 helping organizations rapidly and effectively improve their security hygiene. The project's
66 objective is to increase cybersecurity ecosystem resiliency by helping organizations to overcome
67 the resource-intensive and often thankless nature of security hygiene. The project aims to
68 increase awareness of the importance of security hygiene issues, recommend specific prioritized
69 actions to overcome common obstacles, and establish a natural glide path for organizations to
70 continue on to achieve a comprehensive security hygiene program based on existing standards,
71 guidance, and publications.

72 The driver behind security hygiene is that there are a relatively small number of root causes for
73 many data breaches, malware infections, and other security incidents. Implementing a few
74 relatively simple practices can address those root causes to prevent many incidents from
75 occurring and to lower the potential impact of incidents that still occur. In other words, security
76 hygiene practices make it harder for attackers to succeed and reduce the damage they can
77 cause.

78 Unfortunately, security hygiene is easier said than done. For example, information technology
79 (IT) professionals have known for decades that patching software—operating systems,
80 applications, and the like—eliminates known vulnerabilities. Even though there is widespread
81 recognition that patching can be incredibly effective at mitigating security risk, patching is often
82 resource-intensive, and the act of patching itself can reduce system and service availability.
83 Attempts to reduce resource utilization and expedite patch distribution, such as not testing
84 patches before production deployment, can inadvertently break system functionality and
85 disrupt operations, in some cases causing a significant negative impact to the organization. On
86 the other hand, delays in patch deployment create a larger window of opportunity for attackers.

87 Patching is a particularly important component of cyber hygiene, but existing tools are
88 insufficient for many environments and situations. For example, many organizations lack tools
89 to help them measure and assess the effectiveness and timeliness of their patching efforts.
90 Many organizations also struggle to prioritize patching efforts, test patches before deployment,
91 and adhere to policies for how quickly patches need to be applied in different situations.

92 How, when, and what to patch can be difficult decisions for any organization. Each organization
93 must balance security with mission impact and business objectives, and figure out their risk
94 tolerance for each. Recent cybersecurity attacks have highlighted the dangers of having
95 equipment that has not been patched. Even with recent events and the historical attacks that
96 have been successfully carried out due to unpatched systems, patching remains a problem.

97 This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed
98 implementation guide of the practical steps needed to implement a cybersecurity reference
99 design that addresses this challenge.

100 Scope

101 The objective of this building block project is to demonstrate a proposed approach for improving
102 enterprise patching practices for general IT systems. In this project, commercial and open source
103 tools will be used to aid with the most challenging aspects of patching, including system
104 characterization and prioritization, patch testing, and patch implementation tracking and

105 verification. These tools will be accompanied by actionable, prescriptive guidance on
106 establishing policies and processes for the entire patching life cycle, to include defining roles and
107 responsibilities for all affected personnel, and establishing a playbook with rapid mitigation
108 actions for destructive malware outbreaks that organizations can execute tactically in the first
109 30 days, and recommendations that can be implemented strategically beyond 30 days.

110 The scope of this building block is general IT systems. There are additional challenges with
111 patching for legacy IT systems and virtual systems, as well as industrial control systems (ICS),
112 Internet of Things (IoT) devices, and other technologies stemming from operational technology
113 (OT). Future work could add some or all of these system types to the building block.

114 All aspects of security hygiene other than those related to patching are out of the scope of this
115 building block. The NCCoE is considering adding other security hygiene elements to this building
116 block in the future. Examples include disabling unneeded legacy protocols, only using current
117 (supported) versions of operating systems and applications, and protecting privileged access.

118 Assumptions/Challenges

119 The primary technical elements of this project are as follows:

- 120 • IT endpoints (desktops/laptops and servers running commonly used modern operating
121 systems and applications, including virtual machines and containers)
- 122 • Networking devices (such as routers and switches)
- 123 • Network firewalls
- 124 • Patch management systems
- 125 • Intrusion detection and prevention systems

126 An IT endpoint for an enterprise would have firmware, operating system(s), and application(s) to
127 be patched. The endpoint may be in a fixed location within the organization's own facilities or in
128 a fixed location at a third-party facility (e.g., a data center), or it may be intended for use in
129 multiple locations, such as a laptop used at the office and for telework. The proposed approach
130 for improving enterprise patching practices would have to account for all of these possibilities.

131 Problems sometimes occur with patches, such as a failure during installation, a patch that
132 cannot take effect until the endpoint is rebooted, or a patch that is uninstalled because of
133 operational concerns or because an attacker wants to maintain a vulnerability in a compromised
134 system. This project follows a "trust but verify" philosophy that does not assume installing a
135 patch automatically means the patch is successfully and permanently applied.

136 There are no standard protocols, formats, etc. for patch management, including patch
137 distribution, integrity verification, installation, and installation verification. It is also highly
138 unlikely for a single patch management system to be able to handle all patch management
139 responsibilities for all software on IT endpoints. For example, some applications may handle
140 patching themselves and not be capable of integrating with a patch management system for
141 patch acquisition and installation.

142 Background

143 Patching is not a new challenge for organizations. Many patching guidelines have been
144 published over the years. NIST released Special Publication (SP) 800-40, *Procedures for Handling
145 Security Patches*, in 2002 [1]. Since then, two revisions of SP 800-40 have been published. SP
146 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*, includes discussion
147 of creating and managing such a program, and testing its effectiveness [2]. The latest revision,

148 SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, was released in
149 2013 [3]. It is focused on assisting organizations in understanding the basics of enterprise patch
150 management technologies and increasing the automation of mature patch management
151 programs.

152 Another noteworthy publication is SP 800-184, *Guide for Cybersecurity Event Recovery*, which
153 provides recommendations for rapid recovery from incidents when they occur and helps to
154 minimize the impact on the organization and its constituents [4]. NIST SPs 800-40v2, 800-40r3,
155 and 800-184 can be leveraged to develop a playbook around patching as a recovery step in the
156 event of a fast destructive malware outbreak like Petya or WannaCrypt.

157 In addition to having practices in place for patching, organizations also need inventory
158 capabilities so that at any time, the organization knows what IT systems it has, what
159 dependencies each system has on other systems, what the criticality of each system is, and what
160 the impact would be of a system compromise or operational failure. Without this information,
161 patching efforts may be significantly hampered. Gathering and maintaining this information in a
162 timely manner necessitates relying on tools.

163 **2 SCENARIOS**

164 **Scenario 0: Asset identification and assessment**

165 *This scenario identifies the assets and classifies them based on different impact levels to*
166 *prioritize the order of remediation. It leverages free and commercial tools that can be used to*
167 *discover assets across the enterprise and the cloud to enumerate firmware, operating systems*
168 *(OSs), and applications.*

169 *Knowing which software and software versions are in use and predetermining remediation*
170 *priorities are critically important to all other patching processes. Without accurate, up-to-date,*
171 *and comprehensive information, an organization will have difficulties effectively and efficiently*
172 *performing patching processes, thus increasing risk. While many enterprises have constant asset*
173 *attrition, it is important to have full and accurate inventory of critical assets and the best*
174 *possible inventory for the full enterprise.*

175 **Scenario 1: Routine patching**

176 *This is the standard procedure for patches that are on a regular release cycle and haven't been*
177 *elevated to an active emergency status (because of active exploit in the wild or extreme*
178 *vulnerability severity). This includes endpoint firmware, OS, and applications, server OS and*
179 *applications hosted on-premises or in the cloud (e.g., Infrastructure as a Service), as well as*
180 *"network devices" like firewalls, Storage Area Network (SAN) devices, routers, network switches,*
181 *and other network appliances.*

182 *Most patching falls under this scenario or Scenario 2. However, because routine patching does*
183 *not have the urgency of emergency patching, and routine patch installation can interrupt*
184 *operations (e.g., device reboots), it is often postponed and otherwise neglected. This provides*
185 *many additional windows of opportunity for attackers.*

186 **Scenario 2: Routine patching with cloud delivery model**

187 *This is the standard procedure for patches that are delivered through a cloud delivery model,*
188 *such as a mobile device or a "Windows as a Service (WaaS)" model with Windows operating*

189 systems, Apple Software Update, and mobile device software updates for Android and iOS
190 devices provided by device manufacturers or mobile operators.

191 This scenario is similar in importance to Scenario 1, Routine Patching. However, organizations
192 may not be as accustomed to cloud-delivered patches (which are frequently cumulative for the
193 whole system vs. discrete patches), so this scenario is somewhat more likely to be overlooked by
194 organizations, which increases risk.

195 **Scenario 3: Emergency patching**

196 This is the emergency procedure to address active patching emergencies in a crisis situation,
197 such as extreme severity vulnerabilities like MS17-010, as well as vulnerabilities that are being
198 actively exploited in the wild. The scope of targets is the same as scenario 1.

199 Emergency patching needs to be handled as efficiently as possible to prevent imminent
200 exploitation of vulnerable devices. Key characteristics include identifying vulnerable assets,
201 triaging and applying patches based on a priority list, and tracking and monitoring the state of
202 those assets.

203 **Scenario 4: Emergency workaround (and backout if needed)**

204 This is the emergency procedure in a crisis situation to temporarily mitigate risk for
205 vulnerabilities prior to a vendor releasing a patch. It is typically required when the vulnerability is
206 being actively exploited in the wild. The workaround can vary and may or may not need to be
207 rolled back afterward. The scope of targets is the same as scenario 1.

208 Organizations need to be prepared to quickly implement a wide variety of emergency
209 workarounds to protect vulnerable devices. Without processes, procedures, and tools in place to
210 implement workarounds, too much time may be lost and vulnerable devices may be
211 compromised before workarounds are in place. This may require disabling system functionality,
212 having automated mechanisms to apply these changes, and having capabilities to revert back
213 these changes when a permanent and approved patch is released.

214 **Scenario 5: Isolation of unpatchable assets**

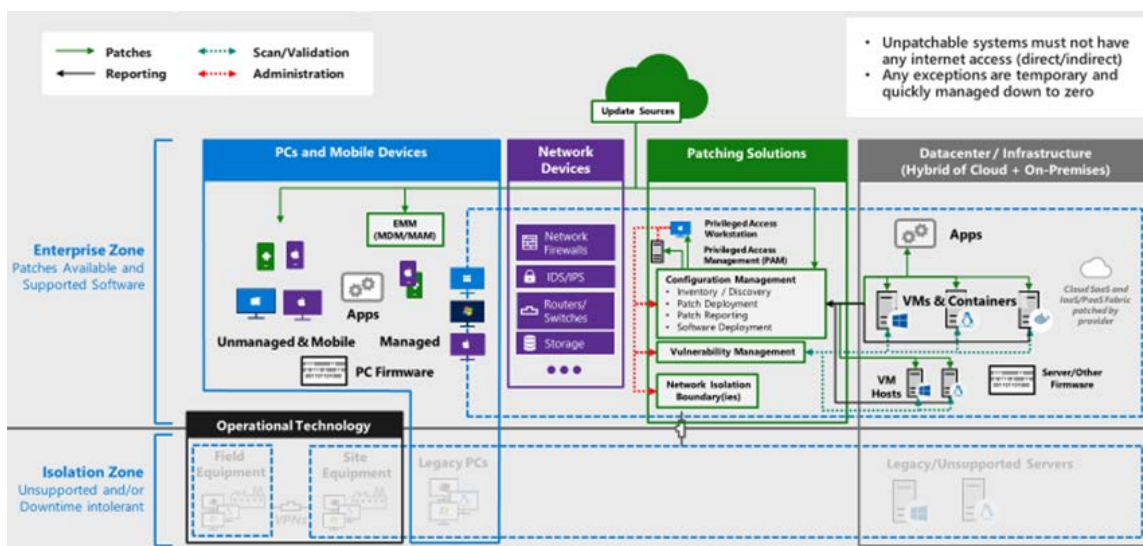
215 This is the reference architecture and implementation of isolation methods to mitigate the risk of
216 systems which cannot be easily patched. This is typically required if routine patching is not able
217 to accommodate these systems within a reasonable timeframe (usually X days or less). Most
218 systems in this scope are legacy unsupported systems or systems with very high operational
219 uptime requirements.

220 Isolation is a form of workaround that can be highly effective at stopping threats against
221 vulnerable devices. Organizations need to be prepared to implement isolation methods when
222 needed and to undo the isolation at the appropriate time to restore regular device access and
223 functionality.

224 **Scenario 6: Patch management system security (or other system with administrative 225 privileges)**

226 This is a reference architecture and implementation of recommended security practices for
227 systems like patch management systems which have administrative privileges over many
228 systems. This will include practices like least privilege, privileged access workstations, and
229 software updates.

230 **3 HIGH-LEVEL ARCHITECTURE**



231
232 **Figure 1: Security Patching Reference Architecture**

233 Patching is a relatively simple operation of updating existing software, but the implementation
234 of the systems has a small amount of complexity. Core assumptions of the architecture depicted
235 in Figure 1 include:

- 236
- 237 • Unpatchable systems must not have any internet access (direct/indirect).
 - 238 • Any exceptions are temporary and quickly managed down to zero.

239 You must patch all the software on the network, including operating systems across devices and
240 servers, applications across devices and servers, and firmware in the devices/hardware. It is
241 critical not to overlook that network, storage, and other enterprise devices also run operating
242 systems and firmware and must be patched regularly. Figure 1 depicts the common enterprise
243 components that need to be regularly updated and maintained.

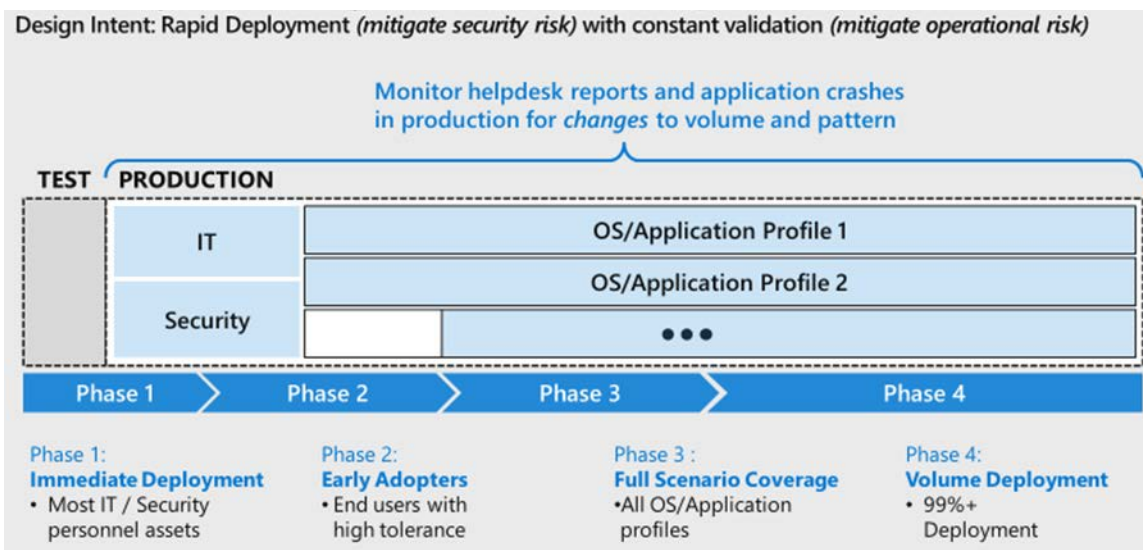
244 The critical cyber hygiene initiative is focused first on common enterprise services in the IT
245 environment. Operational technology and IoT devices are out of scope for the first phase not
246 because of lack of importance, but to ensure rapid delivery of the most common components.

247 The patching system components include:

- 248 • Configuration management tools (where patching is usually managed, though
249 sometimes standalone services like Windows Server Update Services [WSUS] are also
250 available)
- 251 • Vulnerability assessment to provide independent assessment of whether updates are
252 applied correctly (plus detect other non-update vulnerabilities)
- 253 • Security components for the patching and configuration management infrastructure
(elevated security required, given the potential enterprise-wide impact of compromise)
- 254 • Network isolation boundaries that protect systems from attacks on eternally unpatched
255 vulnerabilities (unsupported, sensitive to operational downtime, etc.)

256 Note that the patching by a cloud provider is a “trust but verify” situation where the cloud
 257 provider has to take care of the day-to-day responsibility, but you as a customer should have the
 258 ability to check on this. The mechanisms for how to do this can vary (during acquisition,
 259 informal/formal processes, etc.,) but many compliance regimes require service providers to
 260 provide access to audit reports.

261 The reference security patching process shown in Figure 2 allows you to maximize deployment
 262 speed while limiting the risk of application incompatibility. Note that measuring patch impact
 263 should focus on the changes to volume and pattern of likely issues (helpdesk calls and
 264 application crash/error reports). This process should be consistent regardless of the speed of the
 265 deployment (measured in the ideal of hours/days or starting out measuring in weeks).



266

267 **Figure 2: Security Patching Process**

268 The following describe each of the phases depicted in Figure 2.

269 **Phase 1: Immediate Deployment**

270 The goal of this is to immediately test the updates against real-world scenarios with
 271 technologically savvy users (who are also stakeholders in patching) in the IT and security
 272 organizations.

273 Target: Most IT/security personnel assets

274 **Phase 2: Early Adopters**

275 The goal of this is to rapidly include as many scenarios and technical profiles to flush out
 276 application compatibility issues. To mitigate the potential of operational downtime or
 277 interruption, we recommend recruiting early adopter users across the business with a high
 278 tolerance for interruption (and possibly including ‘dummy’ versions of production systems like
 279 process control network PCs, etc.) While it is desirable to cover all OS/application profiles, it is
 280 acceptable not to do so in this stage.

281 Targets: End users with high tolerance; “dummy” systems with production applications installed
 282 but no operational dependency

283 Phase 3: **Full Scenario Coverage**

284 The goal of this is to cover all OS/application profiles to create high confidence for enterprise
285 rollout. This group may need to evolve as business needs and application profiles change, so
286 including the update of this group in change release processes is highly recommended.

287 Target: All OS/application profiles

288 Phase 4: **Volume Deployment**

289 The goal of this phase is to achieve as close to 100% coverage of the update as feasible so the
290 organization's security attack surface does not include known vulnerabilities that an attacker
291 could exploit at extremely low cost to them.

292 Target: 99%+ deployment

293

294 **Component List**

295 The high-level architecture will include the following components:

- 296 • **PCs and Mobile Devices** – The architecture will include the following components used
297 on the client side:
 - 298 ○ **Managed:** There will be numerous enterprise PCs (desktops and laptops) in use
299 that are managed by the organization and need their operating systems
300 patched.
 - 301 ○ **Unmanaged & Mobile:** There will be numerous unmanaged PCs (desktops and
302 laptops) and mobile devices in use within the organization that need their
303 operating systems patched.
 - 304 ○ **Apps:** The apps on the managed PCs, unmanaged PCs, and mobile devices will
305 need to be patched or updated.
 - 306 ○ **PC Firmware:** The firmware on the managed and unmanaged PCs will need to
307 be patched or updated.
 - 308 ○ **EMM (MDM/MAM):** There will be an Enterprise Mobility Management (EMM)
309 solution deployed to help manage the mobile devices, including identifying
310 vulnerabilities and applying patches and updates. The EMM will be paired with
311 Mobile Device Management (MDM) and Mobile Application Management
312 (MAM) solutions for the mobile device platforms in use.
- 313 • **Network Devices** – The architecture will include the following components providing
314 network-based services for other parts of the architecture:
 - 315 ○ **Firewalls:** Firewalls will restrict network traffic between networks and network
316 segments.
 - 317 ○ **IDS/IPS:** Intrusion detection systems (IDS) and intrusion prevention systems
318 (IPS) will monitor network traffic for malicious packets and behaviors, and may
319 block or alert on the traffic.
 - 320 ○ **Routers/Switches:** Routers and switches will help direct network traffic from
321 source to destination and may impose some basic restrictions on the traffic.
 - 322 ○ **Storage:** Network-based storage systems will provide data storage for other
323 components on the architecture.

- 324 • **Update Sources** – Components of the architecture will interact with external update
325 sources controlled and managed by third parties.
 - 326 • **Patching Solutions** – The architecture will include the following components used to
327 perform patching responsibilities:
 - 328 ○ **Privileged Access Management (PAM) System:** The PAM system will be used to
329 help manage and monitor privileged access to other systems, most notably the
330 configuration management and vulnerability management systems.
 - 331 ○ **Privileged Access Workstation:** The privileged access workstation is a PC
332 (desktop or laptop) that will be authorized to administrate the configuration and
333 vulnerability management systems via the PAM system.
 - 334 ○ **Configuration Management System:** The configuration management system
335 will be used for several purposes, including inventory/discovery, patch
336 deployment, patch reporting, and software deployment.
 - 337 ○ **Vulnerability Management System:** The vulnerability management systems
338 scan for software vulnerabilities and assist with managing these.
 - 339 ○ **Network Isolation Boundaries:** The network controls isolate systems to mitigate
340 the risk of exploitation from another networked system.
 - 341 • **Datacenter/Infrastructure (Hybrid of Cloud + On-Premises)** – The architecture will
342 include the following components used to provide servers and server infrastructure:
 - 343 ○ **Apps:** There will be numerous applications running on both cloud and on-
344 premises servers, and these applications will need to be patched.
 - 345 ○ **VMs & Containers:** There will be virtual machines (VMs) and container
346 technologies running on both cloud and on-premises VM hosts. The VMs and
347 container technologies will need to be patched.
 - 348 ○ **VM Hosts:** There will be numerous VM hosts, which are the physical servers the
349 VMs and containers run on top of. The hosts will need their firmware patched.
 - 350 ○ **Server/Other Firmware:** The VM hosts and other physical servers (e.g., on-
351 premises) will need their firmware patched or updated.
 - 352 ○ **Cloud Software as a Service (SaaS) and Infrastructure as a Service
353 (IaaS)/Platform as a Service (PaaS) Fabric:** The resources provided by cloud
354 providers will be patched by the providers.
- 355 A more detailed architecture and design will be developed once the project is approved and the
356 project team has been assembled.

357 **Desired Requirements**

358 An NCCoE build for this project will require the following components:

- 359 • PCs and mobile devices, including operating systems, firmware, and apps
- 360 • EMM, MDM, and MAM solutions
- 361 • Firewalls and intrusion detection and prevention systems
- 362 • Routers/switches
- 363 • Network-based storage
- 364 • Update sources
- 365 • PAM system and privileged access workstation

- 366 • Configuration management system
- 367 • Vulnerability management system
- 368 • On-premises datacenter and cloud infrastructure, including servers, VM hosts, VMs,
- 369 containers, apps, and firmware

370 **4 RELEVANT STANDARDS AND GUIDANCE**

371 The resources and references required to develop this solution are generally stable, well
372 understood, and available in the commercial off-the-shelf market.

373 **Secure Update Guidelines**

- 374 • NIST Special Publication (SP) 800-40 Version 2, *Creating a Patch and Vulnerability*
375 *Management Program*. See <https://doi.org/10.6028/NIST.SP.800-40ver2>
- 376 • NIST Special Publication (SP) 800-40 Revision 3, *Guide to Enterprise Patch Management*
377 *Technologies*. See <https://doi.org/10.6028/NIST.SP.800-40r3>
- 378 • NIST Special Publication (SP) 800-184, *Guide for Cybersecurity Event Recovery*. See
379 <https://doi.org/10.6028/NIST.SP.800-184>
- 380 • Department of Homeland Security (DHS), Binding Operational Directive 15-01, *Critical*
381 *Vulnerability Mitigation*. See <https://cyber.dhs.gov/bod/15-01/>
- 382 • DHS, Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*. See
383 <https://cyber.dhs.gov/bod/16-02/>

384 **Microsoft Software Update Guides**

- 385 • Microsoft, *Security Update Guide*. See <https://portal.msrc.microsoft.com/en-us/>
- 386 • Microsoft, *Microsoft Lifecycle Policy*. See <https://support.microsoft.com/en-us/lifecycle>
- 387 • Microsoft, *Quick Guide to Windows as a Service*. See [https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/windows/deployment/update/waas-quick-start)
388 [us/windows/deployment/update/waas-quick-start](https://docs.microsoft.com/en-us/windows/deployment/update/waas-quick-start)

389 **5 SECURITY CONTROL MAP**

390 This table maps the characteristics of the commercial products that the NCCoE will apply to this
391 cybersecurity challenge to the applicable standards and best practices described in the
392 Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [5],
393 and other NIST activities. This exercise is meant to demonstrate the real-world applicability of
394 standards and best practices, but does not imply that products with these characteristics will
395 meet your industry's requirements for regulatory approval or accreditation.

Cybersecurity Framework Category	Cybersecurity Framework Subcategory	Draft SP 800-53 Revision 5 Controls [6]
<p>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.</p>	<p>ID.AM-1: Physical devices and systems within the organization are inventoried</p>	<p>CM-8, System Component Inventory</p>
	<p>ID.AM-2: Software platforms and applications within the organization are inventoried</p>	<p>CM-8, System Component Inventory</p>
	<p>ID.AM-4: External information systems are catalogued</p>	<p>SA-9, External System Services</p>
<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-1: Asset vulnerabilities are identified and documented</p>	<p>CA-7, Continuous Monitoring RA-3, Risk Assessment RA-5, Vulnerability Scanning SI-2, Flaw Remediation</p>
<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>PR.DS-2: Data-in-transit is protected</p>	<p>SC-8, Transmission Confidentiality and Integrity</p>
	<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity</p>	<p>SI-7, Software, Firmware, and Information Integrity</p>
<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>PR.IP-12: A vulnerability management plan is developed and implemented</p>	<p>RA-3, Risk Assessment RA-5, Vulnerability Scanning SI-2, Flaw Remediation</p>

APPENDIX A REFERENCES

- [1] NIST, Special Publication (SP) 800-40, *Procedures for Handling Security Patches*, 2002.
- [2] NIST, Special Publication (SP) 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*, 2005. <https://doi.org/10.6028/NIST.SP.800-40ver2>
- [3] NIST, Special Publication (SP) 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, 2013. <https://doi.org/10.6028/NIST.SP.800-40r3>
- [4] NIST, Special Publication (SP) 800-184, *Guide for Cybersecurity Event Recovery*, 2016. <https://doi.org/10.6028/NIST.SP.800-184>
- [5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018. <https://doi.org/10.6028/NIST.CSWP.04162018>
- [6] Joint Task Force, NIST Draft Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, 2017. <https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>

397
398

APPENDIX B ACRONYMS AND ABBREVIATIONS

DHS	Department of Homeland Security
EMM	Enterprise Mobility Management
IaaS	Infrastructure as a Service
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
MAM	Mobile Application Management
MDM	Mobile Device Management
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
OT	Operational Technology
PaaS	Platform as a Service
PAM	Privileged Access Management
PC	Personal Computer
SaaS	Software as a Service
SAN	Storage Area Network
SP	Special Publication
VM	Virtual Machine
WaaS	Windows as a Service
WSUS	Windows Server Update Services