Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Document issued on: January 21, 2016

You should submit comments and suggestions regarding this draft document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments to http://www.regulations.gov. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5418, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

Preface

Additional Copies

CDRH

Additional copies are available from the Internet. You may also send an e-mail request to CDRH-Guidance@fda.hhs.gov to receive an electronic copy of the guidance. Please use the document number (1400044) to identify the guidance you are requesting.

CBER

Additional copies are available from the Center for Biologics Evaluation and Research (CBER), by written request, Office of Communication, Outreach, and Development (OCOD), 10903 New Hampshire Ave., Bldg. 71, Room 3128, Silver Spring, MD 20993-0002, or by calling 1-800-835-4709 or 240-402-8010, by email, ocod@fda.hhs.gov or from the Internet at http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm.

Table of Contents

Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

> *This draft guidance, when finalized, will represent the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.*

I.   Introduction

FDA is issuing this guidance to inform industry and FDA staff of the Agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed medical devices. In addition to the specific recommendations contained in this guidance, manufacturers are encouraged to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to the safety and effectiveness of medical devices and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the patient safety impact and the overall risk to public health.

This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. For the majority of cases, actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered "cybersecurity routine updates or patches," for which the FDA does not require advance notification or reporting under 21 CFR part 806. For a small subset of cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death, the FDA would require medical device manufacturers to notify the Agency.[1]

---

[1] *See* 21 CFR 806.10.

37   For the current edition of the FDA-recognized standard(s) referenced in this document, see the
38   FDA Recognized Consensus Standards Database Web site at
39   http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.
40
41   FDA's guidance documents, including this draft guidance, do not establish legally enforceable
42   responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should
43   be viewed only as recommendations, unless specific regulatory or statutory requirements are
44   cited. The use of the word *should* in Agency guidance means that something is suggested or
45   recommended, but not required.
46

II.   Background

47
48
49   On February 19, 2013, the President issued Executive Order 13636 – *Improving Critical*
50   *Infrastructure Cybersecurity* (EO 13636), which recognized that resilient infrastructure is
51   essential to preserving national security, economic stability, and public health and safety in the
52   United States. EO 13636 states that cyber threats to national security are among the most serious,
53   and that stakeholders must enhance the cybersecurity and resilience of critical infrastructure. This
54   includes the Healthcare and Public Health Critical Infrastructure Sector (HPH Sector).
55   Furthermore, Presidential Policy Directive 21 – *Critical Infrastructure Security and Resilience*
56   (PPD-21) issued on February 12, 2013 tasks Federal Government entities to strengthen the
57   security and resilience of critical infrastructure against physical and cyber threats such that these
58   efforts reduce vulnerabilities, minimize consequences, and identify and disrupt threats. PPD-21
59   encourages all public and private stakeholders to share responsibility in achieving these outcomes.
60
61   In recognition of the shared responsibility for cybersecurity, the security industry has established
62   resources including standards, guidelines, best practices and frameworks for stakeholders to adopt
63   a culture of cybersecurity risk management. Best practices include collaboratively assessing
64   cybersecurity intelligence information for risks to device functionality and clinical risk. FDA
65   believes that, in alignment with EO 13636 and PPD-21, public and private stakeholders should
66   collaborate to leverage available resources and tools to establish a common understanding that
67   assesses risks for identified vulnerabilities in medical devices among the information technology
68   community, healthcare delivery organizations (HDOs), the clinical user community, and the
69   medical device community. These collaborations can lead to the consistent assessment and
70   mitigation of cybersecurity threats, and their impact on medical device safety and effectiveness.
71
72   Cybersecurity risk management is a shared responsibility among stakeholders including, the
73   medical device manufacturer, the user, the Information Technology (IT) system integrator, Health
74   IT developers, and an array of IT vendors that provide products that are not regulated by the FDA.
75   FDA seeks to encourage collaboration among stakeholders by clarifying, for those stakeholders it
76   regulates, recommendations associated with mitigating cybersecurity threats to device
77   functionality and device users.
78
79   As stated in the FDA guidance document titled "Content of Premarket Submissions for
80   Management of Cybersecurity in Medical Devices," when manufacturers consider cybersecurity
81   during the design phases of the medical device lifecycle, the resulting impact is a more proactive

82 and robust mitigation of cybersecurity risks. Similarly, a proactive and risk based approach to the
83 postmarket phase for medical devices, through engaging in cybersecurity information sharing and
84 monitoring, promoting "good cyber hygiene" through routine device cyber maintenance,
85 assessing postmarket information, employing a risk-based approach to characterizing
86 vulnerabilities, and timely implementation of necessary actions can further mitigate emerging
87 cybersecurity risks and reduce the impact to patients.

89 To further aid manufacturers in managing their cybersecurity risk, the Agency encourages the use
90 and adoption of the voluntary "Framework for Improving Critical Infrastructure Cybersecurity"
91 that has been developed by the National Institute of Standards and Technology (NIST) with
92 collective input from other government agencies and the private sector.

94 Critical to the adoption of a proactive, rather than reactive, postmarket cybersecurity approach, is
95 the sharing of cyber risk information and intelligence within the medical device community. This
96 information sharing can enhance management of individual cybersecurity vulnerabilities and
97 provide advance cyber threat information to additional relevant stakeholders to manage and
98 enhance cybersecurity in the medical device community and HPH Sector.

99 Executive Order 13691 – *Promoting Private Sector Cybersecurity Information Sharing* (EO
100 13691), released on February 13, 2015, encourages the development of Information Sharing
101 Analysis Organizations (ISAOs), to serve as focal points for cybersecurity information sharing
102 and collaboration within the private sector as well as between the private sector and government.
103 EO 13691 also mandates that the ISAO "…protects the privacy and civil liberties of individuals,
104 that preserves business confidentiality, [and] that safeguards the information being shared…."
105 ISAOs gather and analyze critical infrastructure information in order to better understand
106 cybersecurity problems and interdependencies, communicate or disclose critical infrastructure
107 information to help prevent, detect, mitigate, or recover from the effects of cyber threats, or
108 voluntarily disseminate critical infrastructure information to its members or others involved in the
109 detection and response to cybersecurity issues.[2]

110 The ISAOs are intended to be: Inclusive (groups from any and all sectors, both non-profit and for-
111 profit, expert or novice, should be able to participate in an ISAO); Actionable (groups will receive
112 useful and practical cybersecurity risk, threat indicator, and incident information via automated,
113 real-time mechanisms if they choose to participate in an ISAO); Transparent (groups interested in
114 an ISAO model will have adequate understanding of how that model operates and if it meets their
115 needs); and Trusted (participants in an ISAO can request that their information be treated as
116 Protected Critical Infrastructure Information. Such information is shielded from any release
117 otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt
118 from regulatory use and civil litigation if the information satisfies the requirements of the Critical
119 Infrastructure Information Act of 2002 (6 U.S.C. §§ 131 et seq.)).

120 The FDA Center for Devices and Radiological Health has entered into a Memorandum of
121 Understanding with one such ISAO, the National Health Information Sharing & Analysis Center,

---

[2] *See* Homeland Security Act, 6 U.S.C. § 212 (2002).

122 (NH-ISAC)[3] in order to assist in the creation of an environment that fosters stakeholder
123 collaboration and communication, and encourages the sharing of information about cybersecurity
124 threats and vulnerabilities that may affect the safety, effectiveness, integrity, and security of the
125 medical devices and the surrounding Health IT infrastructure.
126
127 The Agency wishes to promote collaboration among the medical device and Health IT community
128 to develop a shared understanding of the risks posed by cybersecurity vulnerabilities to medical
129 devices and foster the development of a shared understanding of risk assessment to enable
130 stakeholders to consistently and efficiently assess patient safety and public health risks associated
131 with identified cybersecurity vulnerabilities and take timely, appropriate action to mitigate the
132 risks. This approach will also enable stakeholders to provide timely situational awareness to the
133 HPH community and take efforts to preemptively address the cybersecurity vulnerability through
134 appropriate mitigation and/or remediation before it impacts the safety, effectiveness, integrity or
135 security of medical devices and the Health IT infrastructure.
136
137 The Agency considers voluntary participation in an ISAO a critical component of a medical
138 device manufacturer's comprehensive proactive approach to management of postmarket
139 cybersecurity threats and vulnerabilities and a significant step towards assuring the ongoing safety
140 and effectiveness of marketed medical devices. For companies that voluntarily participate in such
141 a program, and follow other recommendations in this guidance, the Agency does not intend to
142 enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act)
143 (see Section VIII).
144

145 # III. Scope

146
147 This guidance applies to: 1) medical devices that contain software (including firmware) or
148 programmable logic, and 2) software that is a medical device. This guidance supplements the
149 information addressed in the FDA guidance document titled "Cybersecurity for Networked
150 Medical Devices Containing Off-the-Shelf (OTS) Software." This guidance does not apply to
151 experimental or investigational medical devices.

152

153 # IV. Definitions

154
155 For the purposes of this guidance, the following definitions are used:
156

157 ## A.   Compensating Controls

158
159 A cybersecurity compensating control is a safeguard or countermeasure, external to the device,
160 employed by a user in lieu of, or in the absence of sufficient controls that were designed in by a
161 device manufacturer, and that provides supplementary or comparable cyber protection for a

---

[3] *See* Memorandum of Understanding between the National Health Information Sharing & Analysis Center, Inc. (NH-ISAC) and the U.S. Food and Drug Administration Center for Devices and Radiological Health.

162 medical device.[4] For example, a manufacturer's assessment of a cybersecurity vulnerability
163 determines that unauthorized access to a networked medical device will most likely impact the
164 device's essential clinical performance. However, the manufacturer determines that the device
165 can safely and effectively operate without access to the host network, in this case the hospital
166 network. The manufacturer instructs users to configure the network to remove the ability of
167 unauthorized/unintended access to the device from the hospital network. This type of counter
168 measure is an example of a compensating control.
169

B.   Controlled Risk

170
171
172 Controlled risk is present when there is sufficiently low (acceptable) residual risk that the device's
173 essential clinical performance could be compromised by a cybersecurity vulnerability.
174

C.   Cybersecurity Routine Updates and Patches

175
176
177 Cybersecurity "routine updates and patches" are updates or patches to a device to increase device
178 security and/or remediate vulnerabilities associated with controlled risk and not to reduce a risk to
179 health or correct a violation of the FD&C Act. They include any regularly scheduled security
180 updates or patches to a device, including upgrades to the software, firmware, programmable logic,
181 hardware, or security of a device to increase device security as well as updates or patches to
182 address vulnerabilities associated with controlled risk performed earlier than their regularly
183 scheduled deployment cycle even if they are distributed to multiple units. Cybersecurity routine
184 updates and patches are generally considered to be a type of device enhancement that may be
185 applied to vulnerabilities associated with controlled risk and is not considered a repair.
186 Cybersecurity routine updates and patches may also include changes to product labeling,
187 including the instructions for use, to strengthen cybersecurity through increased end-user
188 education and use of best practices. The concept "cybersecurity routine updates and patches" has
189 been developed for the purpose of this guidance and are generally not required to be reported
190 under 21 CFR part 806. See Section VII for more details on reporting requirements for
191 vulnerabilities with controlled risk. Security updates made to remediate vulnerabilities associated
192 with a reasonable probability that use of, or exposure to, the product will cause serious adverse
193 health consequences or death are not considered to be cybersecurity routine updates or patches.
194

D.   Cybersecurity Signal

195
196
197 A cybersecurity signal is any information which indicates the potential for, or confirmation of, a
198 cybersecurity vulnerability or exploit that affects, or could affect a medical device. A
199 cybersecurity signal could originate from traditional information sources such as internal
200 investigations, postmarket surveillance, or complaints, and/or security-centric sources such as
201 CERTS (Computer/Cyber, Emergency Response/Readiness Teams), ISAOs[5] and security

---

[4] This definition is adapted from NIST Special Publication "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST SP 800-53A Rev. 4.
[5] *See* Department of Homeland Security, "Frequently Asked Questions about Information Sharing and Analysis Organizations (ISAOs)."

202 researchers. Signals may be identified within the HPH Sector. They may also originate in
203 another critical infrastructure sector (e.g., defense, financial) but have the potential to impact
204 medical device cybersecurity.
205

E.   Essential Clinical Performance

207
208 Essential clinical performance means performance that is necessary to achieve freedom from
209 unacceptable clinical risk[6], as defined by the manufacturer. Compromise of the essential clinical
210 performance can produce a hazardous situation that results in harm and/or may require
211 intervention to prevent harm. The concept "essential clinical performance" has been developed
212 for the purpose of this guidance.
213

F.   Exploit

215
216 An exploit is an instance where a vulnerability or vulnerabilities have been exercised (accidently
217 or intentionally) and could impact the essential clinical performance of a medical device or use a
218 medical device as a vector to compromise the performance of a connected device or system.
219

G.   Remediation

221
222 Remediation is any action(s) taken to reduce the risk to the medical device's essential clinical
223 performance to an acceptable level. Remediation actions may include complete solutions to
224 remove a cybersecurity vulnerability from a medical device (sometimes known as official fix[7]) or
225 compensating controls that adequately mitigate the risk (e.g., notification to customer base and
226 user community identifying a temporary fix, or work-around). An example of remediation is a
227 notification to the customer base and user community that discloses the vulnerability and potential
228 impact to essential clinical performance and provides a strategy to reduce the risk to the marketed
229 device's essential clinical performance to an acceptable level. If the customer notification does
230 not provide a strategy to reduce the risk to the marketed device's essential clinical performance to
231 an acceptable level, then the remediation is considered *incomplete*.
232

H.   Threat

234
235 Threat is any circumstance or event with the potential to adversely impact the essential clinical
236 performance of the device, organizational operations (including mission, functions, image, or
237 reputation), organizational assets, individuals, or other organizations through an information
238 system via unauthorized access, destruction, disclosure, modification of information, and/or

---

[6] IEC 60601-1:2005, *Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance*, Section 3.27 defines "Essential Performance" as "performance necessary to achieve freedom from unacceptable risk." This draft guidance adapts this definition to explain "Essential Clinical Performance."
[7] "Common Vulnerability Scoring System," Version 3.0, defines "Official Fix" as "A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available."

239 denial of service.[8] Threats exercise vulnerabilities, which may impact the essential clinical
240 performance of the device.
241

I.   Threat modeling

244 Threat modeling is a methodology for optimizing Network/Application/Internet Security by
245 identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or
246 mitigate the effects of, threats to the system.[9] For medical devices, threat modeling can be used to
247 optimize mitigations by identifying vulnerabilities and threats to a particular product, products in
248 a product line, or from the organization's supply chain that can adversely affect patient safety.
249

J.   Uncontrolled Risk

252 Uncontrolled risk is present when there is unacceptable residual risk that the device's essential
253 clinical performance could be compromised due to insufficient compensating controls and risk
254 mitigations.
255

K.   Vulnerability

258 A vulnerability is a weakness in an information system, system security procedures, internal
259 controls, or implementation that could be exploited by a threat.[10]
260

V.   General Principles

262

263 FDA recognizes that medical device cybersecurity is a shared responsibility between stakeholders
264 including health care facilities, patients, providers, and manufacturers of medical devices. Failure
265 to maintain cybersecurity can result in compromised device functionality, loss of data (medical or
266 personal) availability or integrity, or exposure of other connected devices or networks to security
267 threats. This in turn may have the potential to result in patient illness, injury or death.
268

269 Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing
270 the likelihood that device functionality is intentionally or unintentionally compromised by
271 inadequate cybersecurity. An effective cybersecurity risk management program should
272 incorporate both premarket and postmarket lifecycle phases and address cybersecurity from
273 medical device conception to obsolescence. It is recommended that manufacturers apply the
274 NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., Identify, Protect,
275 Detect, Respond and Recover) in the development and implementation of their comprehensive
276 cybersecurity programs. Alignment of the NIST Framework for Improving Critical Infrastructure

---

[8] NIST SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009. Note: Adapted from NIST definition (SP 800-53).
[9] *See* "Threat Modeling" as defined in the Open Web Application Security Project (OWASP).
[10] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1.

277 Cybersecurity five core functions to management of cybersecurity in medical devices is discussed
278 in the Appendix in greater detail.
279

A.   Premarket Considerations

281
282 The FDA guidance document titled "Content of Premarket Submissions for Management of
283 Cybersecurity in Medical Devices" clarifies recommendations for manufacturers to address
284 cybersecurity during the design and development of the medical device, as this can result in more
285 robust and efficient mitigation of patient risks. Manufacturers should establish design inputs for
286 their device related to cybersecurity, and establish a cybersecurity vulnerability and management
287 approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g).
288 The approach should appropriately address the following elements:
289
290 • Identification of assets, threats, and vulnerabilities;
291 • Assessment of the impact of threats and vulnerabilities on device functionality and end
292   users/patients;
293 • Assessment of the likelihood of a threat and of a vulnerability being exploited;
294 • Determination of risk levels and suitable mitigation strategies;
295 • Assessment of residual risk and risk acceptance criteria.
296
297 For additional information see FDA guidance titled "Content of Premarket Submissions for
298 Management of Cybersecurity in Medical Devices."
299

B.   Postmarket Considerations

301
302 Because cybersecurity risks to medical devices are continually evolving, it is not possible to
303 completely mitigate risks through premarket controls alone. Therefore, it is essential that
304 manufacturers implement comprehensive cybersecurity risk management programs and
305 documentation consistent with the Quality System Regulation (21 CFR part 820), including but
306 not limited to complaint handling (21 CFR 820.198), quality audit (21 CFR 820.22), corrective
307 and preventive action (21 CFR 820.100), software validation and risk analysis (21 CFR
308 820.30(g)) and servicing (21 CFR 820.200).
309
310 These programs should emphasize addressing vulnerabilities which may permit the unauthorized
311 access, modification, misuse or denial of use, or the unauthorized use of information that is
312 stored, accessed, or transferred from a medical device to an external recipient, and may impact
313 patient safety. Manufacturers should respond in a timely fashion to address identified
314 vulnerabilities. Critical components of such a program include:
315
316 • Monitoring cybersecurity information sources for identification and detection of
317   cybersecurity vulnerabilities and risk;
318 • Understanding, assessing and detecting presence and impact of a vulnerability;
319 • Establishing and communicating processes for vulnerability intake and handling;
320 • Clearly defining essential clinical performance to develop mitigations that protect, respond
321   and recover from the cybersecurity risk;

322   • Adopting a coordinated vulnerability disclosure policy and practice; and
323   • Deploying mitigations that address cybersecurity risk early and prior to exploitation.
324 Postmarket cybersecurity information may originate from an array of sources including
325 independent security researchers, in-house testing, suppliers of software or hardware technology,
326 health care facilities, and information sharing and analysis organizations. It is strongly
327 recommended that manufacturers participate in a cybersecurity ISAO as sharing and
328 dissemination of cybersecurity information and intelligence pertaining to vulnerabilities and
329 threats across multiple sectors is integral to a successful postmarket cybersecurity surveillance
330 program.
331
332 To manage postmarket cybersecurity risks for medical devices, a company should have a
333 structured and systematic approach to risk management and quality management systems
334 consistent with 21 CFR part 820. For example, such a program should include:
335
336   • Methods to identify, characterize, and assess a cybersecurity vulnerability.
337   • Methods to analyze, detect, and assess threat sources. For example:
338   o A cybersecurity vulnerability might impact all of the medical devices in a
339   manufacturer's portfolio based on how their products are developed; or
340   o A cybersecurity vulnerability could exist vertically (i.e., within the
341   components of a device) which can be introduced at any point in the supply
342   chain for a medical device manufacturing process.
343
344 It is recommended as part of a manufacturer's cybersecurity risk management program
345 that the manufacturer incorporates elements consistent with the <u>NIST Framework for</u>
346 <u>Improving Critical Infrastructure Cybersecurity</u> (i.e., Identify, Protect, Detect, Respond,
347 and Recover).
348
349 FDA recognizes that medical devices and the surrounding network infrastructure cannot be
350 completely secured. Design, architecture, technology, and software development environment
351 choices may result in the inadvertent incorporation of vulnerabilities. The presence of a
352 vulnerability does not necessarily trigger patient safety concerns. Rather it is the impact of the
353 vulnerability on the essential clinical performance of the device which may trigger patient safety
354 concerns. Vulnerabilities that do not appear to currently impact essential clinical performance
355 should be assessed by the manufacturer for future impact.
356

357 ## C.   Defining Essential Clinical Performance
358
359 Essential clinical performance means performance that is necessary to achieve freedom from
360 unacceptable clinical risk, as defined by the manufacturer. Compromise of the essential clinical
361 performance can produce a hazardous situation that results in harm and/or may require
362 intervention to prevent harm.
363
364 Manufacturers should define, as part of risk management, the essential clinical performance of
365 their device, the resulting severity outcomes if compromised, and the risk acceptance criteria.
366 Defining essential clinical performance requirements, severity outcomes, and mapping

367 requirements allows manufacturers to triage vulnerabilities for remediation (see Section VI for
368 additional information on risk assessments).
369
370 When defining essential clinical performance, manufacturers should consider the requirements
371 necessary to achieve device safety and effectiveness. Understanding and defining essential
372 clinical performance is of importance in assessing a vulnerability's impact on device
373 performance, and in determining whether proposed or implemented remediation can provide
374 assurance that the cybersecurity risk to the essential clinical performance is reasonably controlled.
375 Importantly, acceptable mitigations will vary according to the device's essential clinical
376 performance. For example, a cybersecurity vulnerability affecting the essential clinical
377 performance of a thermometer may be quite different than a cybersecurity vulnerability affecting
378 the essential clinical performance of an insulin infusion pump.
379

VI. Medical Device Cybersecurity Risk Management

380
381
382 As part of their risk management process consistent with 21 CFR part 820, a manufacturer should
383 establish, document, and maintain throughout the medical device lifecycle an ongoing process for
384 identifying hazards associated with the cybersecurity of a medical device, estimating and
385 evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the
386 controls. This process should include risk analysis, risk evaluation, risk control, and
387 incorporation of production and post-production information. Elements identified in the Appendix
388 of this guidance should be included as part of the manufacturer's cybersecurity risk management
389 program to support an effective risk management process. Manufacturers should have a defined
390 process to systematically conduct a risk evaluation and determine whether a cybersecurity
391 vulnerability affecting a medical device presents an acceptable or unacceptable risk. It is not
392 possible to describe all hazards, associated risks, and/or controls associated with medical device
393 cybersecurity vulnerabilities in this guidance. It is also not possible to describe all scenarios
394 where risk is controlled or uncontrolled. Rather, FDA recommends manufacturers to define and
395 document their process for objectively assessing the cybersecurity risk for their device(s).
396
397 As outlined below, it is recommended that such a process focus on assessing the *risk to the*
398 *device's essential clinical performance* by considering:
399
400   1) The exploitability of the cybersecurity vulnerability, and
401   2) The severity of the health impact to patients if the vulnerability were to be exploited.
402
403 Such analysis should also incorporate consideration of compensating controls and risk
404 mitigations.
405

A. Assessing Exploitability of the Cybersecurity Vulnerability

408
409 Manufacturers should have a process for assessing the exploitability of a cybersecurity
410 vulnerability. In many cases, estimating the probability of a cybersecurity exploit is very difficult

411 and in the absence of data on the probability of the occurrence of harm, conventional medical
412 device risk management approaches suggest using a "reasonable worst-case estimate" or setting
413 the default value of the probability to one. While these approaches are acceptable, FDA suggests
414 that manufacturers instead consider using a cybersecurity vulnerability assessment tool or similar
415 scoring system for rating vulnerabilities and determining the need for and urgency of the
416 response.
417
418 One such tool, the "Common Vulnerability Scoring System," Version 3.0, for example, provides
419 numerical ratings corresponding to high, medium and low by incorporating a number of factors in
420 assessing exploitability including[11]:

421 • Attack Vector (physical, local, adjacent, network)
422 • Attack Complexity (high, low)
423 • Privileges Required (none, low, high)
424 • User Interaction (none, required)
425 • Scope (changed, unchanged)
426 • Confidentiality Impact (high, low, none)
427 • Integrity Impact (none, low, high)
428 • Availability Impact (high, low, none)
429 • Exploit Code Maturity (high, functional, proof-of-concept, unproven)
430 • Remediation Level (unavailable, work-around, temporary fix, official fix, not defined)
431 • Report Confidence (confirmed, reasonable, unknown, not defined)
432
433 Other vulnerability scoring systems may also be adapted for assessing the exploitability of
434 medical device cybersecurity vulnerabilities.
435

B. Assessing Severity Impact to Health

437
438 Manufacturers should also have a process for assessing the severity impact to health, if the
439 cybersecurity vulnerability were to be exploited. While there are many potentially acceptable
440 approaches for conducting this type of analysis, one such approach may be based on qualitative
441 severity levels as described in ANSI/AAMI/ISO 14971: 2007/(R)2010: *Medical Devices –*
442 *Application of Risk Management to Medical Devices*:
443
444 Common Term   Possible Description
445
446 Negligible: Inconvenience or temporary discomfort
447 Minor: Results in temporary injury or impairment not requiring professional
448   medical intervention
449 Serious: Results in injury or impairment requiring professional medical intervention
450 Critical: Results in permanent impairment or life-threatening injury
451 Catastrophic: Results in patient death

---

[11] For a full description of each factor, see "Common Vulnerability Scoring System," Version 3.0: Specification Document.
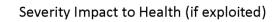
452 ## C.   Evaluation of Risk to Essential Clinical Performance
453
454 A key purpose of conducting the cyber-vulnerability risk assessment is to evaluate whether the
455 risk to essential clinical performance of the device is controlled (acceptable) or uncontrolled
456 (unacceptable). One method of assessing the acceptability of risk to essential clinical
457 performance is by indicating in a matrix in which combinations of "exploitability" and "severity
458 impact to health" represent risks that are controlled or uncontrolled. A manufacturer can then
459 conduct assessments of the exploitability and severity impact to health and then use such a matrix
460 to assess the risk to essential clinical performance for the identified cybersecurity vulnerabilities.
461
462 For risks that remain uncontrolled, additional remediation should be implemented.
463
464 The following figure shows a possible evaluation approach and the relationship between
465 exploitability and impact to health. It can be used to assess the risk to the device's essential
466 clinical performance from a cybersecurity vulnerability as controlled or uncontrolled. While in
467 some cases the evaluation will yield a definite determination that the situation is controlled or
468 uncontrolled, it is possible that in other situations this determination may not be as distinct.
469 Nevertheless, in all cases, FDA recommends that manufacturers make a binary determination that
470 a vulnerability is either controlled or uncontrolled using an established process that is tailored to
471 the product, its essential clinical performance, and the situation. Risk mitigations, including
472 compensating controls, should be implemented when necessary to bring the residual risk to an
473 acceptable level.
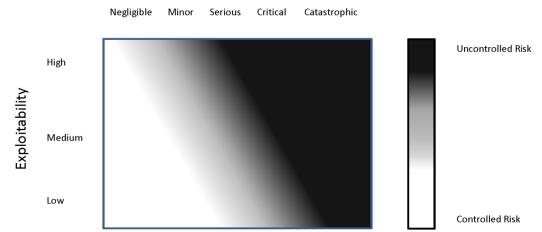

474
475 Figure – Evaluation of Risk to Essential Clinical Performance. The figure shows the relationship
476 between exploitability and risk to health, and can be used to assess the risk to the device's
477 essential clinical performance from a cybersecurity vulnerability. The figure can be used to
478 categorize the risk to essential clinical performance as controlled or uncontrolled.
479

VII. Remediating and Reporting Cybersecurity Vulnerabilities

Based on the vulnerability assessment described in the previous section, the exploitability of an identified vulnerability and its severity impact to health can help determine the extent of the compromise to the essential clinical performance of a device and can be categorized as either "controlled" (acceptable residual risk) or "uncontrolled" (unacceptable residual risk). When determining how to manage a cybersecurity vulnerability, manufacturers should incorporate already implemented compensating controls and risk mitigations into their risk assessment.

FDA encourages efficient, timely and ongoing cybersecurity risk management for marketed devices by manufacturers. For cybersecurity routine updates and patches, the FDA will, typically, not need to conduct premarket review to clear or approve the medical device software changes. In addition, manufacturers should:

- Proactively practice good cyber hygiene, and reduce cybersecurity risks even when residual risk is acceptable;
- Remediate cybersecurity vulnerabilities to reduce the risk of compromise to essential clinical performance to an acceptable level;
- Conduct appropriate software validation under 21 CFR 820.30(g) to assure that any implemented remediation effectively mitigates the target vulnerability without unintentionally creating exposure to other risks;
- Properly document the methods and controls used in the design, manufacture, packaging, labeling, storage, installation and servicing of all finished devices as required by 21 CFR part 820.
- Identify and implement compensating controls, such as a work-around or temporary fix, to adequately mitigate the cybersecurity vulnerability risk, especially when an "official fix" may not be feasible or immediately practicable. In addition, manufacturers should consider the level of knowledge and expertise needed to properly implement the recommended fix;
- Provide users with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use.

In addition to the general recommendations described above, Sections VII.A. and VII.B. below clarify specific recommendations for managing controlled and uncontrolled risks to essential clinical performance.[12]

---

[12] Please note that manufacturers and user facilities may have additional reporting requirements from sources other than FDA.

519 ## A.   Controlled Risk to Essential Clinical Performance
520
521 Controlled risk is present when there is sufficiently low (acceptable) residual risk that the device's
522 essential clinical performance could be compromised by the vulnerability.
523
524
525 Manufacturers are encouraged to promote good cyber hygiene and reduce cybersecurity risks
526 even when residual risk is acceptable. The following are recommendations for changes or
527 compensating control actions taken to address vulnerabilities associated with controlled risk:
528
529 - Changes to a device that are made solely to strengthen cybersecurity are typically
530 considered device enhancements[13], which may include cybersecurity routine updates and
531 patches, and are generally not required to be reported, under 21 CFR 806.10;
532 - For premarket approval (PMA) devices with periodic reporting requirements under 21
533 CFR 814.84, newly acquired information concerning cybersecurity vulnerabilities and
534 device changes made as part of cybersecurity routine updates and patches should be
535 reported to FDA in a periodic (annual) report. See Section VIII for recommended content
536 to include in the periodic report.
537
538 *Examples of Vulnerabilities Associated with Controlled Risk and their Management:*
539
540 - A device manufacturer is notified of an open, unused communication port by the U.S.
541 Department of Homeland Security Industrial Control Systems-Cyber Emergency
542 Response Team (ICS-CERT). Subsequent analyses show that a design feature of the
543 device prevents unauthorized remote firmware download onto the device. The threat is
544 mitigated substantially by the need for physical access due to this device feature and the
545 residual risk is considered "acceptable." The manufacturer takes steps to further enhance
546 the device's security by taking steps to close the unused communication port(s) and
547 provide adequate communication to device users (e.g., user facilities) to facilitate the
548 patch. If the manufacturer closes the open communication ports, the change would be
549 considered a cybersecurity routine update or patch, a type of device enhancement. The
550 change may not require reporting under 21 CFR part 806.
551
552 - A device manufacturer receives a user complaint that a recent security software scan of the
553 PC component of a Class III medical device has indicated that the PC is infected with
554 malware. The outcome of a manufacturer investigation and impact assessment confirms
555 the presence of malware and that the primary purpose of the malware is to collect internet
556 browsing information. The manufacturer also determined that the malware has actively
557 collected browsing information, but that the device's essential clinical performance is not
558 impacted by such collection. The manufacturer's risk assessment determines that the risk
559 due to the vulnerability is controlled. Since essential clinical performance was not
560 impacted, the manufacturer can update the product and it will be considered a

---

[13] *See* FDA guidance titled "Distinguishing Medical Device Recalls from Medical Device Enhancements."

561   cybersecurity routine update or patch. In this case, the manufacturer does not need to
562   report this software update to the FDA in accordance with 21 CFR 806.10. Because the
563   device is a Class III device, the manufacturer should report the changes to the FDA in its
564   periodic (annual) report required for holders of an approved PMA under 21 CFR 814.84.
565

566 ## B.   Uncontrolled Risk to Essential Clinical Performance

567
568 Uncontrolled risk is present when there is unacceptable residual risk that the device's essential
569 clinical performance could be compromised due to insufficient risk mitigations and compensating
570 controls. If the risk to essential clinical performance is assessed as uncontrolled, additional risk
571 control measures should be applied.
572
573 The following are recommendations for changes or compensating control actions to address
574 vulnerabilities associated with uncontrolled risk:
575

576 • Manufacturers should remediate the vulnerabilities to reduce the risk of compromise to
577   essential clinical performance to an acceptable level;

578 • While an official fix may not be feasible or immediately practicable, manufacturers should
579   identify and implement risk mitigations and compensating controls, such as a work-around
580   or temporary fix, to adequately mitigate the risk;

581 • Manufacturers should report these vulnerabilities to the FDA according to 21 CFR part
582   806, unless reported under 21 CFR parts 803 or 1004. However, the FDA does not intend
583   to enforce reporting requirements under 21 CFR part 806 if all of the following
584   circumstances are met:

585   1) There are no known serious adverse events or deaths associated with the
586   vulnerability,

587   2) Within 30 days of learning of the vulnerability, the manufacturer identifies and
588   implements device changes and/or compensating controls to bring the residual risk
589   to an acceptable level and notifies users, and

590   3) The manufacturer is a participating member of an ISAO, such as NH-ISAC;

591 • Remediation of devices with annual reporting requirements (e.g., Class III devices) should
592   be included in the annual report;

593 • The manufacturer should evaluate the device changes to assess the need to submit a
594   premarket submission (e.g., PMA supplement, 510(k), etc.) to the FDA;

595 • The customer base and user community should be provided with relevant information on
596   recommended work-arounds, temporary fixes and residual cybersecurity risks so that they
597   can take appropriate steps to mitigate the risk and make informed decisions regarding
598   device use;

599 • For PMA devices with periodic reporting requirements under 21 CFR 814.84, information
600   concerning cybersecurity vulnerabilities, and the device changes and compensating
601   controls implemented in response to this information should be reported to FDA in a

602 periodic (annual) report. See Section VIII for recommended content to include in the
603 periodic report.

604 In the absence of remediation, a device with uncontrolled risk to its essential clinical performance
605 may be considered to have a reasonable probability that use of, or exposure to, the product will
606 cause serious adverse health consequences or death. The product may be considered in violation
607 of the FD&C Act and subject to enforcement or other action.
608
609 *Examples of Vulnerabilities Associated with Uncontrolled Risk That Must Be Remediated and*
610 *Response Actions:*
611

612 • A manufacturer is made aware of open, unused communication ports. Subsequent
613   analysis determines that the device's designed-in features do not prevent a threat from
614   downloading unauthorized firmware onto the device, which could be used to compromise
615   the device's essential clinical performance. Although there are no reported serious
616   adverse events or deaths associated with the vulnerability, the risk assessment concludes
617   the risk to the device's essential clinical performance is uncontrolled. The manufacturer
618   develops and implements a software update to close the unused communication port(s)
619   and notifies device users (e.g., Healthcare Delivery Organizations (HDOs)) to facilitate the
620   remediation. The manufacturer identifies and implements compensating controls to bring
621   the residual risk to an acceptable level and notifies users within 30 days of becoming
622   aware of the vulnerability. The manufacturer is also a participating member of an ISAO
623   and the manufacturer did not submit an 806 report to the Agency. For Class III devices,
624   the manufacturer does submit a summary of the remediation as part of their periodic
625   (annual) report to FDA. Under these circumstances, FDA does not intend to enforce the
626   reporting requirements under 21 CFR part 806.
627

628 • A manufacturer becomes aware of a vulnerability via a researcher that its Class III medical
629   device (e.g., implantable defibrillator, pacemaker, etc.) can be reprogrammed by an
630   unauthorized user. If exploited, this vulnerability could result in permanent impairment, a
631   life-threatening injury, or death. The manufacturer is not aware that the vulnerability has
632   been exploited and determines that the vulnerability is related to a hardcoded password,
633   and cannot be mitigated by the device's design controls. The risk assessment concludes
634   that the exploitability of the vulnerability is moderate and the risk to the device's essential
635   clinical performance is uncontrolled. The manufacturer notifies appropriate stakeholders,
636   and distributes a validated emergency patch. The manufacturer is not a participating
637   member of an ISAO and reports this action to the FDA under 21 CFR 806.10.
638

639 • A vulnerability known to the security community, yet unknown to a medical device
640   manufacturer, is incorporated into a Class II device during development. Following
641   clearance, the manufacturer becomes aware of the vulnerability and determines that the
642   device continues to meet its specifications, and that no device failures or patient injuries
643   have been reported. There is no evidence that the identified vulnerability has been
644   exploited. However, it was determined that the vulnerability introduced a new failure
645   mode to the device that impacts essential clinical performance, and the device's design
646   controls do not mitigate the risk. The manufacturer conducts a risk assessment and

647 determines that without additional mitigations, the risk to essential clinical performance is
648 uncontrolled. Although the manufacturer does not currently have a software update to
649 mitigate the impact of this vulnerability on the device's essential clinical performance, the
650 manufacturer notifies the customer base and user community of the cybersecurity risk and
651 instructs them to disconnect the device from the hospital network to prevent unauthorized
652 access to the device. The company's risk assessment concludes that the risk to essential
653 clinical performance is controlled with this additional mitigation. If the company took this
654 action to mitigate the risk within 30 days of learning of the vulnerability and is a
655 participating member of an ISAO, FDA does not intend to enforce compliance with the
656 reporting requirement under 21 CFR part 806.
657

658 • A hospital reports that a patient was harmed after a medical device failed to perform as
659 intended. A manufacturer investigation determines that the medical device malfunctioned
660 as a result of exploitation of a previously unknown vulnerability in its proprietary
661 software. The outcome of the manufacturer's investigation and impact assessment
662 determines that the exploit indirectly impacts the device's essential clinical performance
663 and may have contributed to a patient death. The manufacturer notifies the customer base
664 and user community, and develops a validated emergency patch within 30 days of learning
665 of the vulnerability. The manufacturer is a participating member of an ISAO. Because
666 there has been a serious adverse event or death associated with the vulnerability, the
667 manufacturer files a report in accordance with 21 CFR 806.10 to notify FDA and complies
668 with reporting requirements under 21 CFR part 803.
669

VIII. Recommended Content to Include in PMA Periodic Reports

672
673 For PMA devices with periodic reporting requirements under 21 CFR 814.84, information
674 concerning cybersecurity vulnerabilities, and device changes and compensating controls
675 implemented in response to this information should be reported to FDA in a periodic (annual)
676 report.
677
678 It is recommended that the following information be provided for changes and compensating
679 controls implemented for the device:
680
681 • A brief description of the vulnerability prompting the change including how the
682 firm became aware of the vulnerability;
683 • A summary of the conclusions of the firm's risk assessment including whether the
684 risk to essential clinical performance was controlled or uncontrolled;
685 • A description of the change(s) made, including a comparison to the previously
686 approved version of the device;
687 • The rationale for making the change;
688 • Reference to other submissions/devices that were modified in response to this
689 same vulnerability;

690
691
- Identification of event(s) related to the rationale/reason for the change (e.g., MDR number(s), recall number);

692
- Unique Device Identification (UDI) should be included, if available;

693
- A link to an ICS-CERT advisory, if applicable;

694
695
- The date and name of the ISAO to which the vulnerability was reported, if any; and

696
697
698
- Reference to other relevant submission (PMA Supplement[14], 30-Day Notice, 806 report, etc.), if any, or the scientific and/or regulatory basis for concluding that the change did not require a submission/report.

699
700

---

[14] *See* 21 CFR 814.39.

IX. Appendix: Elements of an Effective Postmarket Cybersecurity Program

It is recommended that the following elements, consistent with the <u>NIST Framework for Improving Critical Infrastructure Cybersecurity</u> (i.e., Identify, Protect, Detect, Respond, and Recover), be included as part of a manufacturer's cybersecurity risk management program.

A. Identify

(1) Defining Essential Clinical Performance

Essential clinical performance means performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer. Compromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm.

Manufacturers should define the essential clinical performance of their device, the resulting severity outcomes if compromised, and the risk acceptance criteria. Defining essential clinical performance requirements, severity outcomes, and mapping requirements allows manufacturers to triage vulnerabilities for remediation (see Section VI for additional information on risk assessments).

When defining essential clinical performance, manufacturers should consider the requirements necessary to achieve device safety and effectiveness. Understanding and defining essential clinical performance is of importance in assessing vulnerability impact on device performance, and in determining whether proposed or implemented remediations can provide assurance that the cybersecurity risk to the essential clinical performance is reasonably controlled. Importantly, acceptable mitigations will vary according to the device's essential clinical performance. For example, mitigation for a cybersecurity vulnerability affecting the essential clinical performance of a thermometer may be quite different than a mitigation considered for an insulin infusion pump.

(2) Identification of Cybersecurity Signals

Manufacturers are required to analyze complaints, returned product, service records, and other sources of quality data to identify existing and potential causes of nonconforming product or other quality problems (21 CFR 820.100). Manufacturers are encouraged to actively identify cybersecurity signals that might affect their product, and engage with the sources that report them. It is important to recognize that signals can originate from sources familiar to the medical device workspace such as internal investigations, post market surveillance and or/complaints. It is also important to recognize that cybersecurity signals may originate from cybersecurity-centric sources such as Cyber Emergency Response Teams (CERTS), ISAOs, security researchers, or from other critical

745   infrastructure sectors such as the Defense or Financial Sectors. Irrespective of the
746   originating source, a clear, consistent and reproducible process for intake and handling of
747   vulnerability information should be established and implemented by the manufacturer.
748   FDA has recognized ISO/IEC 30111:2013: *Information Technology – Security Techniques*
749   *– Vulnerability Handling Processes* that may be a useful resource for manufacturers.
750   Manufacturers should develop strategies to enhance their ability to detect signals (e.g.,
751   participating in an ISAO). Manufacturers can also enhance their postmarket detection of
752   cybersecurity risks by incorporating detection mechanisms into their device design and
753   device features to increase the detectability of attacks and permit forensically sound
754   evidence capture.
755

756 ## B.   Protect/Detect
757

758 ### (1)   Vulnerability Characterization and Assessment
759

760   FDA recommends that manufacturers characterize and assess identified vulnerabilities
761   because it will provide information that will aid manufacturers to triage remediation
762   activities. When characterizing the exploitability of a vulnerability, the manufacturer
763   should consider factors such as remote exploitability, attack complexity, threat privileges,
764   actions required by the user, exploit code maturity, and report confidence. Scoring
765   systems such as the "Common Vulnerability Scoring System" (CVSS)[15] provide a
766   consistent framework for assessing exploitability by quantifying the impact of the factors
767   that influence exploitability. See Section VI for additional guidance on vulnerability risk
768   assessment.
769

770 ### (2)   Risk Analysis and Threat Modeling
771

772   FDA recommends that manufacturers conduct cybersecurity risk analyses that include
773   threat modeling for each of their devices and to update those analyses over time. Risk
774   analyses and threat modeling should aim to triage vulnerabilities for timely remediation.
775   Threat modeling is a procedure for optimizing Network/Application/Internet Security by
776   identifying objectives and vulnerabilities, and then defining countermeasures to prevent,
777   or mitigate the effects of, threats to the system.[16] Threat modeling provides traditional
778   risk management and failure mode analysis paradigms, and a framework to assess threats
779   from active adversaries/malicious use. For each vulnerability, a summary report should be
780   produced that concisely summarizes the risk analysis and threat modeling information.
781   Due to the cyclical nature of the analyses, the information should be traceable to related
782   documentation.
783

---

[15] "Common Vulnerability Scoring System," Version 3.0, Scoring Calculator.
[16] *See* "Threat Modeling" as defined in the Open Web Application Security Project.

(3)   Analysis of Threat Sources[17]

FDA recommends manufacturers to analyze possible threat sources. A threat source is defined as the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability[18]. Analysis of threat sources, as part of risk analysis and threat modeling provides a framework for risk introduced by an active adversary. Therefore, characterization of threat sources will be advantageous to manufacturers in accessing risks not covered by traditional failure mode analysis methods.

(4)   Incorporation of Threat Detection Capabilities

Medical devices may not be capable of detecting threat activity and may be reliant on network monitoring. Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound postmarket evidence capture in the event of an attack. This information may assist the manufacturer in assessing and remediating identified risks.

(5)   Impact Assessment on All Devices

FDA recommends manufacturers to have a process to assess the impact of a cybersecurity signal horizontally (i.e., across all medical devices within the manufacturer's product portfolio and sometimes referred to as variant analyses) and vertically (i.e., determine if there is an impact on specific components within the device). A signal may identify a vulnerability in one device, and that same vulnerability may impact other devices including those in development, or those not yet cleared, approved or marketed. Therefore, it will be advantageous to manufacturers to conduct analyses for cybersecurity signals such that expended detection resources have the widest impact.

C.   Protect/Respond/Recover

(1)   Compensating Controls Assessment (Detect/Respond)

FDA recommends manufacturers to implement device-based features as a primary mechanism to mitigate the impact of a vulnerability to essential clinical performance. Manufacturers should assess and prescribe to users, compensating controls such that the risk to essential clinical performance is further mitigated by a defense-in-depth strategy. Section VII describes recommendations for remediating and reporting identified cybersecurity vulnerabilities, including the development, implementation and user notification concerning official fixes, temporary fixes, and work-arounds. Manufacturers

---

[17] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Revision 1.

[18] National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4, Appendix B.

824   should also adopt a coordinated vulnerability disclosure policy. FDA has recognized
825   ISO/IEC 29147:2014: *Information Technology – Security Techniques – Vulnerability*
826   *Disclosure* that may be a useful resource for manufacturers.
827

(2)   Risk Mitigation of Essential Clinical Performance

829

830   Once the preceding information has been assessed and characterized, manufacturers
831   should determine if the risk levels presented by the vulnerability to the essential clinical
832   performance are adequately controlled by existing device features and/or manufacturer
833   defined compensating controls (i.e., residual risk levels are acceptable). Actions taken
834   should reflect the magnitude of the problem and align with the risks encountered.
835   Manufacturers should also include an evaluation of residual risk, benefit/risk, and risk
836   introduced by the remediation. Manufacturers should design their devices to ensure that
837   risks inherent in remediation are properly mitigated including ensuring that the
838   remediation is adequate and validated, that the device designs incorporate mechanisms for
839   secure and timely updates.
840

841   Changes made to improve the performance or quality of a device that do not impact the
842   essential clinical performance of the device are considered device enhancements, not
843   recalls. Cybersecurity routine updates and patches are generally considered a type of
844   device enhancement. For further information on distinguishing between device
845   enhancements and recalls, see FDA guidance titled Distinguishing Medical Device Recalls
846   from Medical Device Enhancements."
847