

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

D-LINK SYSTEMS, INC.,

Defendant.

CIVIL ACTION NO.
3:17-CV-39-JD

~~[PROPOSED]~~ **STIPULATED ORDER
FOR INJUNCTION AND JUDGMENT**

Plaintiff, the Federal Trade Commission (“Commission”), filed its Complaint for Permanent Injunction and Other Equitable Relief pursuant to Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 53(b). The Commission and Defendant stipulate, for the purpose of settlement, to the entry of this Stipulated Order for Injunction (“Order”) to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint charges that Defendant participated in deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, related to the security of the software in its IP cameras and Routers.
3. This Order does not constitute an admission by Defendant that the law has been violated as alleged in the Complaint, or that the facts as alleged in the complaint, other than the jurisdictional facts, are true. Defendant waives and releases any claims that it may have against

1 the Commission, its employees, and its agents that relate to this action. Only for purposes of this
2 action, Defendant admits the facts necessary to establish jurisdiction.

3
4 4. Defendant waives any claim that it may have under the Equal Access to Justice
5 Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order,
6 and agrees to bear its own costs and attorney fees. The Commission also agrees to bear its own
7 costs and attorney fees.

8 5. Defendant and the Commission waive all rights to appeal or otherwise challenge
9 or contest the validity of this Order.

10 **DEFINITIONS**

11 For the purpose of this Order, the following definitions apply:

12
13 1. **“Approved Standard”** shall mean the “Security for industrial automation and
14 control systems – Part 4-1: Secure product development lifecycle requirements”, attached hereto
15 as Exhibit A, or, in the event that such standard no longer exists, any successor standard
16 established or approved by the International Electrotechnical Commission, or any successor
17 entity thereto. In the event no such successor standard or successor entity exists, or at the
18 election of Defendant, Approved Standard shall mean a standard of comparable scope and
19 thoroughness approved, at his or her sole discretion, by the Associate Director for Enforcement,
20 Bureau of Consumer Protection, Federal Trade Commission. Any decision not to approve a
21 standard must be accompanied by a writing setting forth in detail the reasons for denying such
22 approval.
23

24 2. **“Defendant”** means D-Link Systems, Inc. and its successors and assigns.

25 3. **“Covered Device”** shall mean any IP Camera or Router that Defendant sells on or
26 after January 5, 2017, directly or through authorized re-sellers to consumers in the United States;
27

1 provided that “Covered Device” does not include IP Cameras or Routers that Defendant can
2 establish that Defendant offers primarily for enterprises and other commercial entities, including
3 products identified in Exhibit B.
4

5 4. “**IP Camera**” shall mean any Internet Protocol (“IP”) camera, cloud camera, or
6 other Internet-accessible camera that transmits, or allows for the transmission of, video, audio, or
7 audiovisual data over the Internet.

8 5. “**Router**” shall mean any network device that forwards IP data packets from one
9 network to another or from a network to the Internet.

10 **ORDER**

11 **I. COMPREHENSIVE SOFTWARE SECURITY PROGRAM**

12 **IT IS ORDERED** that Defendant shall, for a period of twenty (20) years after entry of
13 this Order, continue with or establish and implement, and maintain, a comprehensive software
14 security program (“Software Security Program”) that is designed to provide protection for the
15 security of its Covered Devices, unless Defendant ceases to market, distribute, or sell any
16 Covered Devices. Subject to Section II.I of this Order, to satisfy this requirement, Defendant
17 must, at a minimum:
18

19 A. Document in writing the content, implementation, and maintenance of the
20 Software Security Program;
21

22 B. Provide the written program and any evaluations thereof or updates thereto to
23 Defendant’s board of directors or governing body or, if no such board or equivalent governing
24 body exists, to a senior officer of Defendant responsible for Defendant’s Software Security
25 Program at least once every twelve (12) months;
26

1 C. Designate a qualified employee or employees to coordinate and be responsible for
2 the Software Security Program;

3
4 D. Assess and document, at least once every twelve (12) months, internal and
5 external risks to the security of Covered Devices that could result in the unauthorized disclosure,
6 misuse, loss, theft, alteration, destruction, or other compromise of such information input into,
7 stored on or captured with, accessed, or transmitted by a Covered Device;

8 E. Design, implement, maintain, and document safeguards, as a part of a secure
9 software development process, that control for the internal and external risks Defendant
10 identifies to the security of Covered Devices. Such safeguards shall also include:

11 1. Engaging in security planning by enumerating in writing how
12 functionality and features will affect the security of Covered Devices;

13 2. Performing threat modeling to identify internal and external risks to the
14 security of data transmitted using Covered Devices;

15 3. Engaging in pre-release code review of every release of software for
16 Covered Devices through the use of automated static analysis tools;

17 4. Conducting pre-release vulnerability testing of every release of software
18 for Covered Devices;

19 5. Performing ongoing code maintenance by maintaining a database of
20 shared code to be used to help find other instances of a vulnerability when a vulnerability is
21 reported or otherwise discovered;

22 6. Remediation processes designed to address security flaws, or analogous
23 instances of security flaws, identified at any stage of software development process;

1 I. Evaluate and adjust the Software Security Program in light of any changes to
2 Defendant's operations or business arrangements, or any other circumstances that Defendant
3 knows or has reason to know may have an impact on the effectiveness of the Software Security
4 Program. At a minimum, Defendant must evaluate the Software Security Program at least once
5 every twelve (12) months and modify the Software Security Program based on the results.
6

7 Except for Sections I.B and I.C, Defendant may select, appoint, and work with third
8 parties that are contractually required to comply with the requirements of this Section I, provided
9 that Defendant discloses all material facts and does not misrepresent any material facts to said
10 third party. Defendant shall obtain from said third party all materials and documentation
11 necessary to evaluate the effectiveness of the compliance with any provisions that the third party
12 is contracted to comply with. However, Defendant shall be solely responsible for compliance
13 with this Order.
14

15 **II. SOFTWARE SECURITY ASSESSMENTS BY A THIRD PARTY**

16 **IT IS FURTHER ORDERED** that, in connection with compliance with Defendant's
17 Software Security Program, Defendant must obtain initial and biennial assessments
18 ("Assessments"):
19

20 A. The Assessments must be obtained from a qualified, objective, independent third-
21 party professional ("Assessor"), who: (1) is qualified as a Certified Secure Software Lifecycle
22 Professional (CSSLP) with professional experience with secure Internet-accessible devices;
23 (2) uses procedures and standards generally accepted in the profession; (3) conducts an
24 independent review of the Software Security Program, or, at the election of Defendant, an
25 assessment of the Approved Standard; and (4) retains all documents considered for each
26 Assessment for five (5) years after completion of such Assessment and will provide such
27

1 documents to the Commission within fourteen (14) days of receipt of a written request from a
2 representative of the Commission. No documents considered for an Assessment may be
3 withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product or
4 attorney client privilege.
5

6 B. For each Assessment, Respondent shall provide the Associate Director for
7 Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the
8 name and affiliation of the person selected to conduct the Assessment, which the Associate
9 Director shall have the authority to approve in his sole discretion. Any decision not to approve
10 an individual selected to conduct such Assessment must be accompanied by a writing setting
11 forth in detail the reasons for denying such approval.
12

13 C. The reporting period for the Assessments to FTC must cover: (1) from the entry
14 of this Order to January 31, 2020, for the initial Assessment; and (2) each 2-year period
15 thereafter for ten (10) years after entry of this Order for the biennial Assessments.

16 D. If Defendant elects to assess Defendant's compliance with the Software Security
17 Program, the Assessment must: (1) determine whether Defendant has implemented and
18 maintained the Software Security Program; (2) assess the effectiveness of Defendant's
19 implementation and maintenance of sub-Sections I.A-I; (3) identify any gaps or weaknesses in
20 the Software Security Program; (4) identify specific evidence (such as documents reviewed,
21 sampling and testing performed, and interviews conducted) examined to make such
22 determinations, assessments, and identifications, and explain why the evidence that the Assessor
23 examined is sufficient to justify the Assessor's findings; or,
24

25 E. If Defendant elects to assess Defendant's compliance with the Approved
26 Standard, the Assessment must certify compliance with the Approved Standard, including, but
27

1 not limited to, the following provisions: (1) Part 6.4 (“SR-3: Product Security Requirements”);
2 (2) Part 6.5 (“SR-4: Product security requirements content”); (3) Part 6.3 (“SR-2: Threat
3 model”); (4) Part 8.3.1(c) (“Static Code Analysis”); (5) Part 9.4 (“SVV-3: Vulnerability
4 Testing”); (6) Part 9.5 (“Penetration Testing”); (7) Part 10.4 (“DM-3: Assessing security-related
5 issues”); (8) Part 10.5 (“DM-4: Addressing security-related issues”); (9) Part 10.2 (“DM-1:
6 Receiving notifications of security-related issues”); (10) Part 11.6 (“SUM-5: Timely delivery of
7 security patches”); (11) Part 10.6 (“DM-5: Disclosing security-related issues”); (12) Part 5.6
8 (“SM-4: Security expertise”).
9

10 F. No finding of any Assessment shall rely solely on assertions or attestations by
11 Defendant’s management. The Assessment shall be signed by the Assessor and shall state that
12 the Assessor conducted an independent review of the Software Security Program or the
13 Approved Standard, and did not rely solely on assertions or attestations by Defendant’s
14 management.
15

16 G. To the extent that Defendant has selected, appointed, or worked with a third party
17 to implement any of the criteria of the Software Security Program or any criteria of the Approved
18 Standard, Defendant shall provide to the Assessor, or cause to be provided to the Assessor, in
19 connection with the Assessment, all materials and documentation necessary for the Assessor to
20 conduct the Assessment of the effectiveness of the Comprehensive Software Security Program or
21 Approved Standard. All such materials and documentation shall be maintained and produced
22 upon request pursuant to the provisions of this Order.
23

24 H. Each Assessment must be completed within sixty (60) days after the end of the
25 reporting period to which the Assessment applies. Unless otherwise directed by a Commission
26 representative in writing, Defendant must submit the initial Assessment to the Commission
27

1 within twenty (20) days after the Assessment has been completed via email to DEbrief@ftc.gov
2 or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement,
3 Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,
4 Washington, DC 20580. The subject line must begin, “In re D-Link Systems, FTC File No.
5 X170030.” All subsequent biennial Assessments shall be retained by Defendant until the order
6 is terminated and provided to the Associate Director for Enforcement within twenty (20) days of
7 request.
8

9 I. If Defendant obtains an Assessment (i) certifying that the Software Security
10 Program for the Covered Devices is in compliance with the Approved Standard and
11 (ii) certifying that Defendant is in compliance with Section I.E.10, Defendant shall be deemed in
12 compliance with Section I of this Order for two (2) years from the date of that Assessment or
13 until the next January 31 Assessment deadline, whichever is earlier. *Provided, however:*

14 1. Defendant shall not be deemed in compliance with Section I of this Order
15 based on a Section II Assessment if Defendant made a representation, express or implied, that
16 either misrepresented or omitted a material fact and such misrepresentation or omission would
17 likely affect a reasonable Assessor’s decision about whether Defendant complied with the
18 Approved Standard. Further, in the event that such a misrepresentation or omission was made
19 for the purpose of deceiving the Assessor, Defendant shall not be deemed in compliance with
20 any portion of Section I or Section II of this Order based on that Assessment.
21

22 2. Defendant shall not be deemed in compliance with Section I of this Order
23 based upon a Section II Assessment if Defendant materially changed its practices after the
24 Assessment in question, unless, at the time of the material change, an Assessor qualified under
25
26

1 this Section certifies that the material change does not cause Defendant to fall out of compliance
2 with the Approved Standard on which the Assessment in question was based.

3
4 **III. COOPERATION WITH THIRD-PARTY SOFTWARE SECURITY ASSESSOR**

5 **IT IS FURTHER ORDERED** that Defendant, whether acting directly or indirectly, in
6 connection with any Assessment required by Section II of this Order titled Software Security
7 Assessments by a Third Party, must:

8 A. Disclose all material facts to the Assessor, and must not misrepresent in any
9 manner, expressly or by implication, any fact material to the Assessor's Assessment; and

10 B. Provide or otherwise make available to the Assessor all information and material
11 in its possession, custody, or control that is necessary to the Assessment for which there is no
12 reasonable claim of privilege.

13
14 **IV. ANNUAL CERTIFICATION**

15 **IT IS FURTHER ORDERED** that, in connection with compliance with Defendant's
16 Software Security Program, Defendant shall:

17 A. One year after the entry of this Order, and each year thereafter, provide the
18 Commission with a certification from a senior corporate manager, or, if no such senior corporate
19 manager exists, a senior officer of Defendant responsible for Defendant's Software Security
20 Program that: (1) the requirements of this Order have been established, implemented, and
21 maintained; and (2) Defendant is not aware of any material noncompliance that has not been (a)
22 corrected or (b) disclosed to the Commission. The certification must be based on the personal
23 knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom
24 the senior corporate manager or senior officer reasonably relies in making the certification.
25
26

1 B. Unless otherwise directed by a Commission representative in writing, submit all
2 annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or
3 by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau
4 of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,
5 Washington, DC 20580. The subject line must begin, "In re D-Link Systems, Inc., FTC File No.
6 X170030."
7

8 **V. SPECIFIC CONDUCT PROVISIONS**

9 **IT IS FURTHER ORDERED** that

10 A. Defendant shall no longer sell, distribute, or host on its website the IP Camera set-
11 up wizard software containing the representations shown in Exhibit C attached hereto for any
12 Covered Devices.
13

14 B. Within 60 days of the effective date of this Order, provide clear and conspicuous
15 notice to all consumers who registered their Covered Devices, through the communication
16 channel(s) the consumer chose at the time of registration, containing instructions for updating
17 said device with the latest firmware update.
18

19 **VI. ORDER ACKNOWLEDGMENTS**

20 **IT IS FURTHER ORDERED** that Defendant obtains acknowledgments of receipt of
21 this Order:

22 A. Defendant, within 7 days of entry of this Order, must submit to the Commission
23 an acknowledgment of receipt of this Order sworn under penalty of perjury.

24 B. For three years after entry of this Order, Defendant must deliver a copy of this
25 Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all
26 employees having managerial responsibilities for the security of Covered Devices and all agents
27

1 and representatives who participate in the security of Covered Devices; and (3) any business
2 entity resulting from any change in structure as set forth in the Section titled Compliance
3 Reporting. Delivery must occur within 7 days of entry of this Order for current personnel. For
4 all others, delivery must occur before they assume their responsibilities.
5

6 C. From each individual or entity to which a Defendant delivered a copy of this
7 Order, that Defendant must obtain, within 30 days, a signed and dated acknowledgment of
8 receipt of this Order.

9 **VII. COMPLIANCE REPORTING**

10 **IT IS FURTHER ORDERED** that Defendant makes timely submissions to the
11 Commission:

12 A. On January 31, 2020, Defendant must submit a compliance report, sworn under
13 penalty of perjury, which must: (1) identify the primary physical, postal, and email address and
14 telephone number, as designated points of contact, which representatives of the Commission may
15 use to communicate with Defendant; (2) identifies all of that Defendant's businesses by all of
16 their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes
17 the activities of each business, including the security and marketing practices; (4) describes in
18 detail whether and how Defendant is in compliance with each Section of this Order (either
19 directly or, at Defendant's election, Defendant may, for the purpose of satisfying this
20 requirement as to Sections I and II, incorporate a Section II initial Assessment); and (5) provides
21 a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously
22 submitted to the Commission.
23
24

25 B. For ten (10) years after entry of this Order, Defendant must submit a compliance
26 notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any
27

1 designated point of contact; or (b) the structure of Defendant or any entity that Defendant has
2 any ownership interest in or controls directly or indirectly that may affect compliance obligations
3 arising under this Order, including: creation, merger, sale, or dissolution of the Defendant or any
4 subsidiary, parent, or affiliate that Defendant has any ownership interest in or controls directly or
5 indirectly that engages in any acts or practices subject to this Order.
6

7 C. Defendant must submit to the Commission notice of the filing of any bankruptcy
8 petition, insolvency proceeding, or similar proceeding by or against such Defendant within 14
9 days of its filing.

10 D. Any submission to the Commission required by this Order to be sworn under
11 penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by
12 concluding: “I declare under penalty of perjury under the laws of the United States of America
13 that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s
14 full name, title (if applicable), and signature.
15

16 E. Unless otherwise directed by a Commission representative in writing, all
17 submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or
18 sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement,
19 Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,
20 Washington, DC 20580. The subject line must begin: *FTC v. D-Link Systems, Inc.*, X170030.
21

22 VIII. RECORDKEEPING

23 **IT IS FURTHER ORDERED** that Defendant must create certain records for ten (10)
24 years after entry of the Order, and retain each such record for 5 years. Specifically, Defendant
25 must create and retain the following records:

26 A. accounting records showing the revenues from all goods or services sold;

1 B. Defendant's personnel records showing, for each person providing services,
2 whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job
3 title or position; dates of service; and (if applicable) the reason for termination;
4

5 C. records of all consumer complaints and refund requests, whether received directly
6 or indirectly, such as through a third party, concerning the subject matter of the Order;

7 D. all records necessary to demonstrate full compliance with each provision of this
8 Order, including all submissions to the Commission; and

9 E. a copy of each unique advertisement or other marketing material by Defendant
10 making a representation subject to this Order.
11

12 IX. COMPLIANCE MONITORING

13 **IT IS FURTHER ORDERED** that, for the purpose of monitoring Defendant's
14 compliance with this Order:

15 A. Within 14 days of receipt of a written request from a representative of the
16 Commission, Defendant must: submit additional compliance reports or other requested
17 information, which must be sworn under penalty of perjury; appear for depositions; and produce
18 documents for inspection and copying. The Commission is also authorized to obtain discovery,
19 without further leave of court, using any of the procedures prescribed by Federal Rules of Civil
20 Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69. Provided,
21 however, that Defendant, after attempting to resolve a dispute without court action and for good
22 cause shown, may file a motion with this Court seeking an order for one or more of the
23 protections set forth in Rule 26(c).
24

25 B. For matters concerning this Order, the Commission is authorized to communicate
26 directly with Defendant, Defendant must permit representatives of the Commission to interview
27

1 any employee or other person affiliated with Defendant who has agreed to such an interview.

2 The person interviewed may have counsel present.

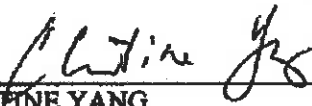
3
4 C. The Commission may use all other lawful means, including posing, through its
5 representatives, as consumers, suppliers, or other individuals or entities, to Defendant or any
6 individual or entity affiliated with Defendant, without the necessity of identification or prior
7 notice. Nothing in this Order limits the Commission's lawful use of compulsory process,
8 pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1, nor does it limit
9 Defendant's ability to assert any and all objections, defenses, rights, or privileges available to it,
10 as to any such process.


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28


X. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.


Dated: _____ By: 
WILLIAM C. BROWN, Chief Information Security Officer
D-Link Systems, Inc.

Dated: _____ By: 
CHRISTINE YANG
Law Offices of S.J. Christine Yang
Attorney for Defendant D-Link Systems, Inc.

Dated: 5/6/2019 By: 
JOHN A. VECCHIONE, President and CEO
Cause of Action Institute
Attorney for Defendant D-Link Systems, Inc.

Dated: 7/1/19 By: 
KEVIN H. MORIARTY
CATHLIN TULLY
JARAD A. BROWN
KATHERINE E. MCCARON
BRIAN C. BERGGREN
Counsel for the Federal Trade Commission

SO ORDERED this 6th day of August, 2019.



Honorable James Donato
United States District Judge
Northern District of California

**Stipulated Order for
Injunction and Judgment**

Exhibit A

(Placeholder Excerpted Public Version of
Document Filed Under Seal at ECF 271)



IEC 62443-4-1

Edition 1.0 2018-01

INTERNATIONAL STANDARD



Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.030

ISBN 978-2-8322-5239-0

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	11
2 Normative references	11
3 Terms, definitions, abbreviated terms, acronyms and conventions.....	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms and acronyms	16
3.3 Conventions.....	17
4 General principles	17
4.1 Concepts	17
4.2 Maturity model	19
5 Practice 1 – Security management	20
5.1 Purpose	20
5.2 SM-1: Development process	21
5.2.1 Requirement.....	21
5.3 Rationale and supplemental guidance.....	21
5.4 SM-2: Identification of responsibilities	21
5.4.1 Requirement.....	21
5.4.2 Rationale and supplemental guidance.....	21
5.5 SM-3: Identification of applicability.....	21
5.5.1 Requirement.....	21
5.5.2 Rationale and supplemental guidance.....	22
5.6 SM-4: Security expertise	22
5.6.1 Requirement.....	22
5.6.2 Rationale and supplemental guidance.....	22
5.7 SM-5: Process scoping	22
5.7.1 Requirement.....	22
5.7.2 Rationale and supplemental guidance.....	23
5.8 SM-6: File integrity.....	23
5.8.1 Requirement.....	23
5.8.2 Rationale and supplemental guidance.....	23
5.9 SM-7: Development environment security	23
5.9.1 Requirement.....	23
5.9.2 Rationale and supplemental guidance.....	23
5.10 SM-8: Controls for private keys	23
5.10.1 Requirement.....	23
5.10.2 Rationale and supplemental guidance.....	24
5.11 SM-9: Security requirements for externally provided components.....	24
5.11.1 Requirement.....	24
5.11.2 Rationale and supplemental guidance.....	24
5.12 SM-10: Custom developed components from third-party suppliers	24
5.12.1 Requirement.....	24
5.12.2 Rationale and supplemental guidance.....	25
5.13 SM-11: Assessing and addressing security-related issues	25
5.13.1 Requirement.....	25
5.13.2 Rationale and supplemental guidance.....	25

5.14	SM-12: Process verification	25
5.14.1	Requirement.....	25
5.14.2	Rationale and supplemental guidance.....	25
5.15	SM-13: Continuous improvement	25
5.15.1	Requirement.....	25
5.15.2	Rationale and supplemental guidance.....	26
6	Practice 2 – Specification of security requirements	26
6.1	Purpose	26
6.2	SR-1: Product security context.....	27
6.2.1	Requirement.....	27
6.2.2	Rationale and supplemental guidance.....	27
6.3	SR-2: Threat model.....	27
6.3.1	Requirement.....	27
6.3.2	Rationale and supplemental guidance.....	28
6.4	SR-3: Product security requirements.....	28
6.4.1	Requirement.....	28
6.4.2	Rationale and supplemental guidance.....	28
6.5	SR-4: Product security requirements content	29
6.5.1	Requirement.....	29
6.5.2	Rationale and supplemental guidance.....	29
6.6	SR-5: Security requirements review	29
6.6.1	Requirement.....	29
6.6.2	Rationale and supplemental guidance.....	29
7	Practice 3 – Secure by design	30
7.1	Purpose	30
7.2	SD-1: Secure design principles	30
7.2.1	Requirement.....	30
7.2.2	Rationale and supplemental guidance.....	30
7.3	SD-2: Defense in depth design.....	31
7.3.1	Requirement.....	31
7.3.2	Rationale and supplemental guidance.....	32
7.4	SD-3: Security design review	32
7.4.1	Requirement.....	32
7.4.2	Rationale and supplemental guidance.....	32
7.5	SD-4: Secure design best practices	32
7.5.1	Requirement.....	32
7.5.2	Rationale and supplemental guidance.....	33
8	Practice 4 – Secure implementation.....	33
8.1	Purpose	33
8.2	Applicability	33
8.3	SI-1: Security implementation review	33
8.3.1	Requirement.....	33
8.3.2	Rationale and supplemental guidance.....	34
8.4	SI-2: Secure coding standards	34
8.4.1	Requirement.....	34
8.4.2	Rationale and supplemental guidance.....	34
9	Practice 5 – Security verification and validation testing.....	34
9.1	Purpose	34

9.2	SVV-1: Security requirements testing	35
9.2.1	Requirement	35
9.2.2	Rationale and supplemental guidance	35
9.3	SVV-2: Threat mitigation testing	35
9.3.1	Requirement	35
9.3.2	Rationale and supplemental guidance	35
9.4	SVV-3: Vulnerability testing	36
9.4.1	Requirement	36
9.4.2	Rationale and supplemental guidance	36
9.5	SVV-4: Penetration testing	36
9.5.1	Requirement	36
9.5.2	Rationale and supplemental guidance	36
9.6	SVV-5: Independence of testers	37
9.6.1	Requirement	37
9.6.2	Rationale and supplemental guidance	37
10	Practice 6 – Management of security-related issues	38
10.1	Purpose	38
10.2	DM-1: Receiving notifications of security-related issues	38
10.2.1	Requirement	38
10.2.2	Rationale and supplemental guidance	38
10.3	DM-2: Reviewing security-related issues	38
10.3.1	Requirement	38
10.3.2	Rationale and supplemental guidance	39
10.4	DM-3: Assessing security-related issues	39
10.4.1	Requirement	39
10.4.2	Rationale and supplemental guidance	39
10.5	DM-4: Addressing security-related issues	40
10.5.1	Requirement	40
10.5.2	Rationale and supplemental guidance	40
10.6	DM-5: Disclosing security-related issues	41
10.6.1	Requirement	41
10.6.2	Rationale and supplemental guidance	41
10.7	DM-6: Periodic review of security defect management practice	42
10.7.1	Requirement	42
10.7.2	Rationale and supplemental guidance	42
11	Practice 7 – Security update management	42
11.1	Purpose	42
11.2	SUM-1: Security update qualification	42
11.2.1	Requirement	42
11.2.2	Rationale and supplemental guidance	42
11.3	SUM-2: Security update documentation	42
11.3.1	Requirement	42
11.3.2	Rationale and supplemental guidance	43
11.4	SUM-3: Dependent component or operating system security update documentation	43
11.4.1	Requirement	43
11.4.2	Rationale and supplemental guidance	43
11.5	SUM-4: Security update delivery	43
11.5.1	Requirement	43

11.5.2	Rationale and supplemental guidance.....	43
11.6	SUM-5: Timely delivery of security patches.....	44
11.6.1	Requirement.....	44
11.6.2	Rationale and supplemental guidance.....	44
12	Practice 8 – Security guidelines.....	44
12.1	Purpose.....	44
12.2	SG-1: Product defense in depth.....	44
12.2.1	Requirement.....	44
12.2.2	Rationale and supplemental guidance.....	45
12.3	SG-2: Defense in depth measures expected in the environment.....	45
12.3.1	Requirement.....	45
12.3.2	Rationale and supplemental guidance.....	45
12.4	SG-3: Security hardening guidelines.....	45
12.4.1	Requirement.....	45
12.4.2	Rationale and supplemental guidance.....	46
12.5	SG-4: Secure disposal guidelines.....	46
12.5.1	Requirement.....	46
12.5.2	Rationale and supplemental guidance.....	46
12.6	SG-5: Secure operation guidelines.....	46
12.6.1	Requirement.....	46
12.6.2	Rationale and supplemental guidance.....	47
12.7	SG-6: Account management guidelines.....	47
12.7.1	Requirement.....	47
12.7.2	Rationale and supplemental guidance.....	47
12.8	SG-7: Documentation review.....	47
12.8.1	Requirement.....	47
12.8.2	Rationale and supplemental guidance.....	47
Annex A (informative)	Possible metrics.....	48
Annex B (informative)	Table of requirements.....	50
Bibliography	52
Figure 1 – Parts of the IEC 62443 series.....		9
Figure 2 – Example scope of product life-cycle.....		10
Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle.....		18
Table 1 – Maturity levels.....		20
Table 2 – Example SDL continuous improvement activities.....		26
Table 3 – Required level of independence of testers from developers.....		37
Table B.1 – Summary of all requirements.....		50

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SECURITY FOR INDUSTRIAL AUTOMATION
AND CONTROL SYSTEMS –**
Part 4-1: Secure product development lifecycle requirements**FOREWORD**

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-4-1 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65/685/FDIS	65/688/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

IEC 62443-4-1:2018 © IEC 2018

– 7 –

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS). This document describes product development life-cycle requirements related to cyber security for products intended for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.

This document has been developed in large part from the Secure Development Life-cycle Assessment (SDLA) Certification Requirements [26]¹ from the ISA Security Compliance Institute (ISCI). Note that the SDLA procedure was based on the following sources:

- ISO/IEC 15408-3 (Common Criteria) [18];
- Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [36];
- The Security Development Life-cycle by Michael Howard and Steve Lipner [43];
- IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems [24], and
- RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [28].

Therefore, all these sources can be considered contributing sources to this document.

This document is the part of the IEC 62443 series that contains security requirements for developers of any automation and control products where security is a concern.

Figure 1 illustrates the relationship of the different parts of IEC 62443 that were in existence or planned as of the date of circulation of this document. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

¹ Figures in square brackets refer to the bibliography.

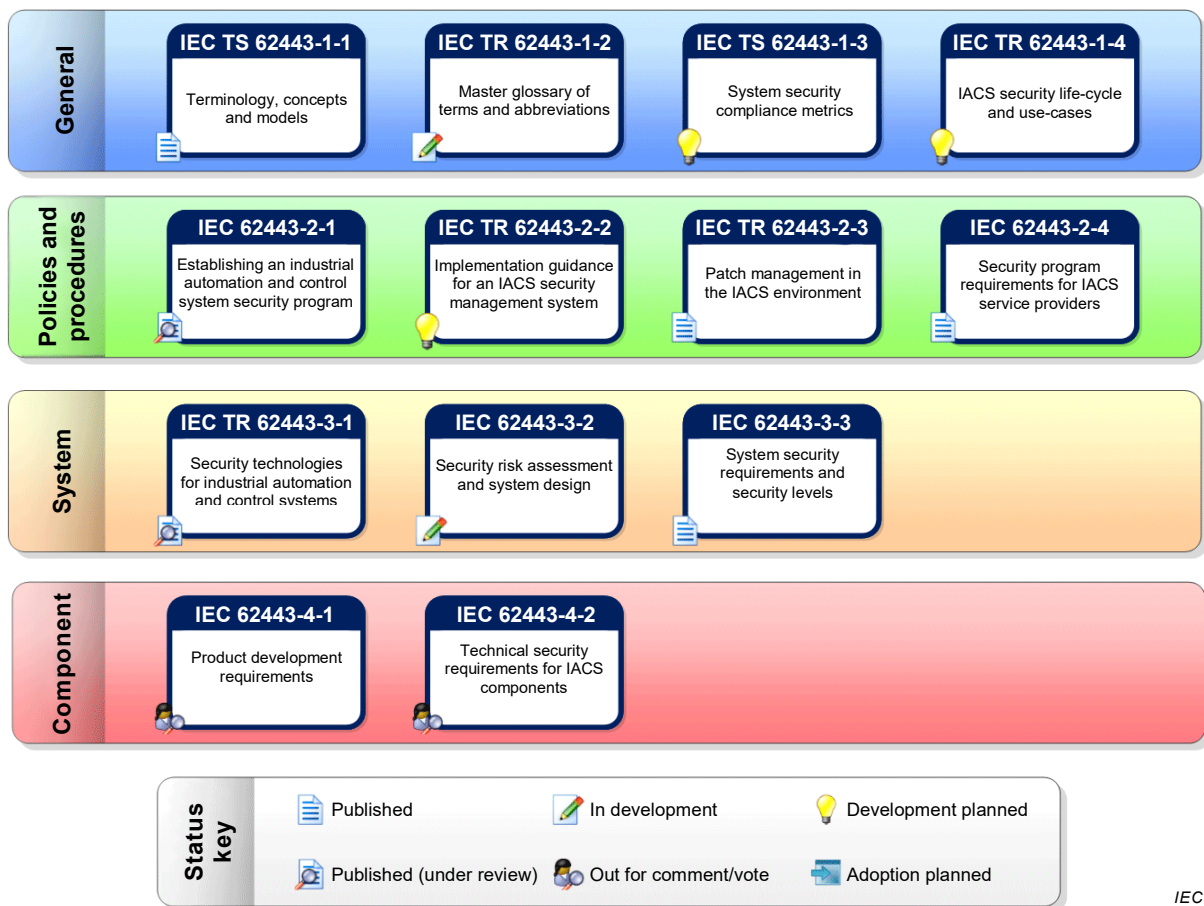


Figure 1 – Parts of the IEC 62443 series

Figure 2 illustrates how the developed product relates to maintenance and integration capabilities defined in IEC 62443-2-4 and to its operation by the asset owner. The product supplier develops products using a process compliant with this document. Those products may be a single component, such as an embedded controller, or a group of components working together as a system or subsystem. The products are then integrated together, usually by a system integrator, into an Automation Solution using a process compliant with IEC 62443-2-4. The Automation Solution is then installed at a particular site and becomes part of the industrial automation and control system (IACS). Some of these capabilities reference security measures defined in IEC 62443-3-3 [10] that the service provider ensures are supported in the Automation Solution (either as product features or compensating mechanisms). This document only addresses the process used for the development of the product; it does not address design, installation or operation of the Automation Solution or IACS.

In Figure 2, the Automation Solution is illustrated to contain one or more subsystems and optional supporting components such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 1 Automation Solutions typically have a single product, but they are not restricted to do so. In some industries, there may be a hierarchical product structure. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (for example, continuous or manufacturing) as defined by the asset owner.

NOTE 2 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

NOTE 3 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

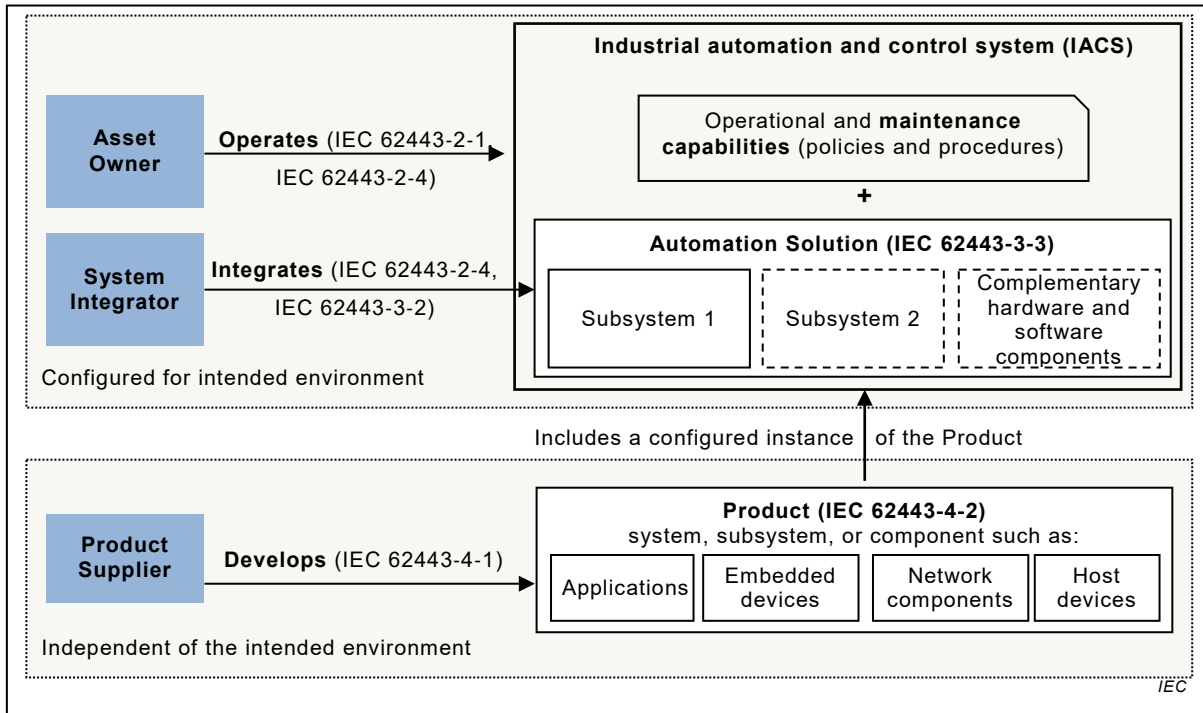


Figure 2 – Example scope of product life-cycle

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-1: Secure product development lifecycle requirements

1 Scope

This part of IEC 62443 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development life-cycle (SDL) for the purpose of developing and maintaining secure products. This life-cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product. A summary list of the requirements in this document can be found in Annex B.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62443-2-4:2015, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC 62443-2-4:2015/AMD1:2017

**Stipulated Order for
Injunction and Judgment
Exhibit B**

Exhibit B

DCS-1201
DCS-2230
DCS-3511
DCS-4602EV & -VB1
DCS-4603
DCS-4605EV
DCS-4622
DCS-4633EV
DCS-4701E & -VB1
DCS-4703E
DCS-4705E
DCS-4802E & -VB1
DCS-5615
DCS-6004L
DCS-6010L
DCS-6113
DCS-6210
DCS-6212L
DCS-6314
DCS-6315
DCS-6510
DCS-6511/MCD
DCS-6513
DCS-6517 & /MCD
DCS-6616
DCS-6818
DCS-6915
DCS-7010L
DCS-7110
DCS-7513
DCS-7517
DSR-1000AC
DSR-150 & 150/RE & 150N & 150N/RE
DSR-250 & 250/RE & 250N & 250N/RE
DSR-500 & 500/RE & 500N/RE
DSL-2750B-VZ
DWR-920V-UC
DWR-922-UC
DWR-961-SP & -UC & -VZ

**Stipulated Order for
Injunction and Judgment
Exhibit C**

