EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454

ANNEXES 1 to 6

ANNEXES

to the

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

{SEC(2022) 321} - {SWD(2022) 282} - {SWD(2022) 283}

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product (‘minimisation of data’);

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

ANNEX II

INFORMATION AND INSTRUCTIONS TO THE USER

As a minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;
2. the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;
3. the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;
4. the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;
5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;
6. if and, where applicable, where the software bill of materials can be accessed;
7. where applicable, the internet address at which the EU declaration of conformity can be accessed;
8. the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates;
9. detailed instructions or an internet address referring to such detailed instructions and information on:
   (a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;
   (b) how changes to the product can affect the security of data;
   (c) how security-relevant updates can be installed;
   (d) the secure decommissioning of the product, including information on how user data can be securely removed.

ANNEX III

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;
13. Remote access/sharing software;
14. Mobile device management software;
15. Physical network interfaces;
16. Operating systems not covered by class II;
17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
19. Microprocessors not covered by class II;
20. Microcontrollers;
21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
23. Industrial Internet of Things not covered by class II.

Class II

1. Operating systems for servers, desktops, and mobile devices;

2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
3. Public key infrastructure and digital certificate issuers;
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;
5. General purpose microprocessors;
6. Microprocessors intended for integration in programmable logic controllers and secure elements;
7. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;
8. Secure elements;
9. Hardware Security Modules (HSMs);
10. Secure cryptoprocessors;
11. Smartcards, smartcard readers and tokens;
12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
14. Robot sensing and actuator components and robot controllers;
15. Smart meters.

ANNEX IV

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 20, shall contain all of the following information:

1. Name and type and any additional information enabling the unique identification of the product with digital elements;
2. Name and address of the manufacturer or his authorised representative;
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;
4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);
5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;
6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;
8. Additional information:

Signed for and on behalf of: ……

(place and date of issue):

(name, function) (signature):

ANNEX V

CONTENTS OF THE TECHNICAL DOCUMENTATION

The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:

1. a general description of the product with digital elements, including:
   (a) its intended purpose;
   (b) versions of software affecting compliance with essential requirements;
   (c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;
   (d) user information and instructions as set out in Annex II;
2. a description of the design, development and production of the product and vulnerability handling processes, including:
   (a) complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;
   (b) complete information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;
   (c) complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.
3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation;
4. a list of the harmonised standards applied in full or in part the references of which have been published in the *Official Journal of the European Union*, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;
5. reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;
6. a copy of the EU declaration of conformity;

7. where applicable, the software bill of materials as defined in Article 3, point (36), further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I.

ANNEX VI

CONFORMITY ASSESSMENT PROCEDURES

Conformity Assessment procedure based on internal control (based on Module A)

1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I.

2. The manufacturer shall draw up the technical documentation described in Annex V.

3. Design, development, production and vulnerability handling of products with digital elements

   The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.

4. Conformity marking and declaration of conformity

4.1. The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this Regulation.

4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

5. Authorised representatives

   The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.

EU-type examination (based on Module B)

1. EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.

2. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the

technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).

3. The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice.

The application shall include:

– the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;

– a written declaration that the same application has not been lodged with any other notified body;

– the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V;

– the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility.

4. The notified body shall:

4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I;

4.2. verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;

4.3. carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly;

4.4. carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I have not been applied, the

solutions adopted by the manufacturer meet the corresponding essential requirements;

4.5. agree with the manufacturer on a location where the examinations and tests will be carried out.

5. The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.

6. Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached.

The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.

Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.

The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.

8. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued.

The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical

documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.

9. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market.

10. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate.

Conformity to type based on internal production control (based on Module C)

1. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3, and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I.

2. Production

2.1. The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with the approved type described in the EU-type examination certificate and with the essential requirements as set out in Section 1 of Annex I.

3. Conformity marking and declaration of conformity

3.1. The manufacturer shall affix the CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument.

3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

4. Authorised representative

The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.

Conformity based on full quality assurance (based on Module H)

1. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I.

2. Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4.

3. Quality system

3.1. The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned.

The application shall include:

– the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well;

– the technical documentation for one model of each category of products intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V;

– the documentation concerning the quality system; and

– a written declaration that the same application has not been lodged with any other notified body.

3.2. The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I.

All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.

It shall, in particular, contain an adequate description of:

– the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;

– the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met;

– the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met;

– the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used

when designing and developing the products pertaining to the product category covered;

– the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;

– the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;

– the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc;

– the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.

3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.

It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification.

In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements.

The manufacturer or his authorised representative shall be notified of the decision.

The notification shall contain the conclusions of the audit and the reasoned assessment decision.

3.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.

3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system.

The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

4. Surveillance under the responsibility of the notified body

4.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.

4.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:

– the quality system documentation;

– the quality records as provided for by the design part of the quality system, such as results of analyses, calculations, tests, etc.;

– the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.

4.3. The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.

5. Conformity marking and declaration of conformity

5.1. The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation.

5.2. The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up.

A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

6. The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market, keep at the disposal of the national authorities:

– the technical documentation referred to in point 3.1;

– the documentation concerning the quality system referred to in point 3.1;

– the change referred to in point 3.5, as approved;

– the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4.

7. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

8. Authorised representative

The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.