Label Data Entry Form Mockup

1. About:

Labeling recommendations have not yet been finalized. Both the contents and format of each field are active areas of research and therefore subject to change. This form is not currently being used for the production of any cybersecurity label or in association with an existing cyber labeling program. Rather, this mockup is intented to provide vendors and other stakeholders with a sample of data types that a cybersecurity label for smart meters and inverters may request, in order to gather feedback on the value and limitations of types of information presented in this example label generation form.

Research Assumptions:

1. Producing and receiving a label would be a voluntary (not regulatory) process.
2. Any information disclosed in this form may be displayed in a publicly available fact sheet associated with a label.
3. The label fact sheet would be hosted online and updated virtually by the vendor/author. Data fields may be updated at any time.
4. A small sticker would be printed and displayed on the product or product manual. This sticker would include a QR code or URL pointing to the virutally hosted fact sheet. Minimal immutable information (such as product name and model number) may be included on this printed sticker.
5. Receiving a label is not equivalent to a seal of approval for security. Rather, a label of this type promotes transparency and due diligence. Any further assumptions drawn about the security of the product based on information in the label data sheet are subject to the interpretation of the consumer.
6. Most questions in the generator form would be requested on a voluntary basis. This means that if a question is not applicable to the system, the author may enter N/A. If the author is unwilling to disclose certain information about the system, they may leave the field blank and it will show as unanswered in the data sheet output. Minimum required fields are marked with an asterisk (*). We are interested in feedback on the minimum required information necessary for a useful label output.

2. Label Author/Creator

Name of the entity responsible for the contents of this form

3. Device Manufacturer

Name of the manufacturer of the Finished Good

4. Product Name and Model Number

"Product" refers to a standalone device. Model number means a combination of letters, digits, or characters representing the manufacturer, brand, design, or performance of an appliance. If model number doesn't exist, this can be blank.

4a. Product Description

Description of product function and features

5. Is this product manufactured by one company, then packaged and sold by other companies under one or more brand names?

This question refers to the final product. Component source is addressed in a later question.

- ◯ Yes
- ◯ No *(skip to Q9)*

6. For resellers: Who is the original manufacturer of this product?

Skip to question 8 if you are the original manufacturer.

7. For resellers: What changes have you made to this product?

- [ ] No changes, this product is unaltered from the original manufacturer software/firmware/hardware configuration
- [ ] Software changes
- [ ] Firmware changes
- [ ] Hardware changes
- [ ] Other

INSTRUCTIONAL TEXT: Resellers should point to the original manufacturer's label. Please reach out to the original manufacturer to coordinate.

8. For original manufacturers: Please list all known brands or designations this product is distributed under:

9. Which software version(s) does the information listed in this form apply to?

Application layer software, not specifically tied to lower level hardware

9. Cryptographic Hash of Software

Cryptographically secure hash, using current NIST recommended algorithms. Hash type and value:

10a. Which firmware version(s) does the information listed in this form apply to?

Low level software (e.g., device drivers) tightly integrated into hardware

10b. Cryptographic Hash of Firmware

Cryptographically secure hash, using current NIST recommended algorithms. Hash type and value:

11a. Security Certifications or Standards Met

List any certifications the product has achieved and which version of that certification the product is attesting compliance with. Enter certification name, version (if applicable), and issuer/originating entity/country

11b. Privacy Certifications or Standards Met

List any certifications the product has achieved and which version of that certification the product is attesting compliance with. Enter certification name, version (if applicable), and issuer/originating entity/country

12. System Access Methods

Which methods can be used to read or write data to and from the system?

- [ ] Website - locally hosted
- [ ] Website - remotely hosted
- [ ] Physical access
- [ ] Mobile app

13. Does the security of this device depend upon security mechanisms enforced by systems external to this device?

(e.g. external firewall, gateway)

- ◯ Yes
- ◯ No

List system(s) here:

14. System Interfaces

Wireless protocols supported, physical connections

15a. Communications Ports and Protocols

Complete list of all network protocols used/supported

15b. Configurable network ports

15c. Required open network ports

16. Required Network Services

Which communication protocols are required for full functionality?

17. Protection of Data at Rest

Disclose what mechanisms are used to secure communications channels. This should include communications between devices within the system (if applicable) and between the system and external entities. Disclose where the credentials are stored (e.g. if you are using a key to protect information, are you storing it in a file or a hardware security module). Enter the mechanism of protection for each category:

17a. Confidentiality

17b. Integrity

17c. Authenticity

18. Protection of Data in Motion

Disclose what mechanisms are used to secure communications channels. Disclose where the keys are stored (e.g. if you are using a key to protect information, are you storing it in a file or a hardware security module). Enter the mechanism of protection for each category:

18a. Confidentiality

18b. Integrity

18c. Authenticity

19. Secure Boot Mechanisms

list any technologies or protocols used to ensure security (integrity, confidentiality, etc) of the boot process (e.g. certified IoT platform, hardware or root of trust utilized, secure boot process, secure boot protocols, standards met, supported, etc.)

20. Final Assembly Country: Software

Country device software was "finalized" in

Afghanistan
Albania
Algeria
Andorra

21. Final Assembly Country: Hardware

Country device hardware was "finalized" in

Afghanistan
Albania
Algeria
Andorra

22. In what country do final quality assurance checks for this device's software occur?

Afghanistan
Albania
Algeria
Andorra

23. In what country do final quality assurance checks for this device's hardware occur?

Afghanistan
Albania
Algeria
Andorra

24. Components Source Countries

List countries that logic-bearing, storage, and communication components came from

Afghanistan
Albania
Algeria
Andorra

25. Hardware Bill of Materials (HBOM)

Hardware Bill of Materials (HBOM) refers to a listing of the components (circuit boards, chips, etc.) within a hardware system.

	Yes	No
Do you maintain an HBOM for this system for the purposes of cyber-supply chain risk management?	☐	☐
Is it available upon request?	☐	☐

26. Software Bill of Materials (SBOM)

Software Bill of Materials (SBOM) refers to a listing of components (e.g. applications, libraries, files and folders) within a software package.

	Yes	No
Do you maintain an SBOM for this system for the purposes of cyber-supply chain risk management?	☐	☐
Is it available upon request?	☐	☐

27. Security Audits Performed

Has a third party entity performed security audits on the system ***as a whole?***

- ◯ Yes *(proceed to question 29)*
- ◯ No

28. Has a third party entity performed security audits on any components of the system?

This may include hardware, software, backend cloud infrastructure, mobile application, etc.

- ◯ Yes
- ◯ No *(Skip to question 30)*

List all components audited:

29. What type(s) of third party security audits have been performed on this device?

For "other" please list assessment type, entity, and date of most recent passed assessment.

- ☐ Third-party vulnerability assessment
- ☐ Risk assessment
- ☐ Other

For each type, list assessor name; date of most recent assessment; report availability (public, available upon request, or not available)

30. Offline Functionality

Can the system operate without network/internet communication, if so, what functionality remains? If network communication is lost, what functionality is lost and in what timeframe?

31. Authentication Method

Fill columns 1-3 for each authentication method this system uses. Methods that are not used should be left blank.

	Purpose (e.g. user identify authentication; firmware signatures)	Default credentials provided? (Y/N)	Can the end user install their own credentials? (Y/N)
Password (string of characters)			
Passcode (numeric code)			
PIN			
Access Badge			
Key			
Token			
Fingerprint			
Optical			
Face ID			
MFA			

32. Security Update Policy*

Link to security update policy (url)

33. Vulnerability Disclosure Policy*

Link to vulnerability disclosure policy (url)

34. Defined Support Period

*Indicate the date at which support for this device ends (EOL). *skip if no support period is defined*

Month Day Year

35. Security Updates: Are security updates provided?

- ◯ Yes
- ◯ No *(skip to question 38)*

36. Security Update Mechanism

How are firmware updates applied?

	Mechanism (e.g. over the air, USB, etc.)
Automatic Updates	
Manual Updates	

37. Update notification method

Identify the notification mechanism(s) by which the user is informed of security updates

- ☐ App push notification
- ☐ e-Mail
- ☐ SMS
- ☐ Mail delivery
- ☐ Phone call
- ☐ Other

38. Security Maintenance Requirements

Who is responsible for maintaining the security of the device?

- ☐ Consumer
- ☐ Vendor/Manufacturer
- ☐ Utility
- ☐ Integrator
- ☐ **Other**

39. Privacy Policy*

Link to privacy policy (url)

40. Data Policy*

Link to data policy (URL), covering data sharing, collection, and data types

41. Who has access to data generated by this system?

Select all that apply

	Anonymized Data	Device Data
Consumer	☐	☐
Utility	☐	☐
Integrator	☐	☐
Vendor/Manufacturer	☐	☐
VPP/Demand response program operator/Electricity market aggregator	☐	☐
Third-party support technicians	☐	☐
Third-party: Other (see below)	☐	☐

42. Which third-parties can access data generated by this system?

Skip if "Third-party is not selected in question 41)

☐ Advertisers

☐ Credit Reporting Agencies

- [ ] Government entities
- [ ] Data analytics providers
- [ ] Other

43. Third Party default data sharing consent

- ◯ Opt-In (action is required to opt into data sharing)
- ◯ Opt-Out (data is automatically shared, action required to opt-out)

44. Who has control of data generated by this system?

"Control" refers to who legally owns the data and has the authority to grant access to, modify, or destroy the data.

- [ ] Consumer
- [ ] Utility
- [ ] Integrator
- [ ] Vendor/Manufacturer
- [ ] Third-Party
- [ ] Other

45. Within what geopolitical boundaries to command and control servers for this system exist, if applicable?

46. Where is data generated by this system stored?

- [ ] Local
- [ ] Cloud
- [ ] Utility
- [ ] Other

Cloud Storage location (geopolitical boundaries); provider

47. Sensing Capabilities

List all sensors not directly related to the defined function of the device

- [ ] None
- [ ] Temperature
- [ ] Pressure
- [ ] Motion
- [ ] Level
- [ ] Image
- [ ] Proximity
- [ ] Chemical
- [ ] Gas
- [ ] Smoke
- [ ] Infrared
- [ ] Gyroscopic
- [ ] Humidity
- [ ] Optical
- [ ] Sound