PLAIN LANGUAGE STATEMENT AND CONSENT FORM

We cordially invite you to participate in this survey. The information collected in this survey is part of the research project “Development of Australian Cyber Criteria Assessment”. The project is peer-reviewed and funded by Cyber Security Cooperative Research Centre, with an amount of AUD $156,000. This research study is being conducted by researchers at Deakin University and Charles Sturt University (Australia) led by Professor Chang-Tsun Li. The purpose of this research study is to identify what challenges are hindering the adoption of Common Criteria certification by organizations, companies, vendors, and user groups for Information Technology (IT) products.

In this survey, you will be provided with a total of 28 questions, either in the form of short answer questions or multiple-choice questions,
which focus on different angles of the adaption circumstance of Common Criteria certification and the certified products. This survey should take up to 15 minutes to complete.

Involvement in the project is voluntary and participants can stop the survey at any time but after submission data cannot be withdrawn as the survey is anonymous. The completion of a survey indicates implied consent to participate.

The given information by the participants will be processed and saved in a database and will be accessed only by authorized researchers involved in the research project. The information will be used only for statistical and research purposes, as well as possible audits. By participating in this study and giving the requested information, the participants authorize the researchers to storage their answers for a limited time with

the previously indicated purposes.

The results will be made public and published in a scientific journal publication related to the topic, and the participants can contact the Principal Researcher to access any findings. Disseminated results will not include any information that identifies individual participants. Confidentiality of information offered is subject to legal limitations (e.g., subpoena, freedom of information claim, or mandatory reporting in some professions).

Since the survey will be performed solely online, there is no request for physical contact among all involved parties. Moreover, the questionnaire is only about the participant's experience and views in adopting Common Criteria Certification, so there are no identifiable risks for the project except discomfort. By identifying the adoption barrier to determine if organisations have concerns related to regulatory issues as well as determining organisations' attitudes towards being measured against cyber standards will pave the way for widespread adoption of Common Criteria.

For follow-up support, please contact Prof. Chang-Tsun Li on changtsun.li@deakin.edu.au or (+61) 3 522 73559.

Complaints
If you have any complaints about any aspect of the project, the way it is being conducted or any questions about your rights as a research participant, then you may contact:

The Human Research Ethics Office
Deakin University
221 Burwood Highway, Burwood Victoria 3125
Telephone: 9251 7129
research-ethics@deakin.edu.au
Please quote project number [PJ07004].

This study has received Deakin University ethics approval (reference number: SEBE-2021-38)

Chang-Tsun Li
Professor of Cyber Security
School of Info Technology Faculty of Science Engineering and Built Environment

Deakin University
changtsun.li@deakin.edu.au
+61 3 522 73559
https://www.deakin.edu.au/about-deakin/people/chang-tsun-li

By clicking on the button below, you will confirm that you have read the information in this consent form and are voluntarily agreeing to participate in this research study.

Q1. Can you please tell us the name of your organization?

Q2. Which countries does your organization operate in?
(hold down the Ctrl key to select multiple answers)

Afghanistan
Albania
Algeria
Andorra
Angola
Antigua and Barbuda
Argentina
Armenia
Australia
Austria

Q3. Which one of the following best describes the size of your organization?

- ○ 0-10 employees
- ○ 11-50 employees
- ○ 51-250 employees
- ○ 251-1000 employees
- ○ 1000+ employees

Q4. Which sectors does your organization belong to (please indicate as many as appropriate)?

- ☐ Defence industry
- ☐ Health and social care

- [ ] Food and Agriculture
- [ ] Energy and utilities
- [ ] Resources and Mining
- [ ] ICT (Information Communication Technology)
- [ ] Manufacturing
- [ ] Transportation
- [ ] Environment, water and soil
- [ ] Education
- [ ] Financial and insurance services
- [ ] Real estate and property
- [ ] Wholesale and retail trade
- [ ] Legal services
- [ ] Others

Questions for IT vendors

Q5. Does your organization produce Information Technology (IT) products which may be implemented in hardware, firmware, or software?

- ○ Yes
- ○ No

Q6. Which categories are relevant to the IT products produced by your organization (please indicate as many as appropriate)?

- [ ] Access Control Devices and Systems
- [ ] Biometric Systems and Devices
- [ ] Boundary Protection Devices and Systems
- [ ] Data Protection
- [ ] Databases
- [ ] Detection Devices and Systems
- [ ] ICs, Smart Cards and Smart Card-Related Devices and Systems
- [ ] Key Management Systems
- [ ] Mobility

- [ ] Multi-Function Devices
- [ ] Network and Network-Related Devices and Systems
- [ ] Operating Systems
- [ ] Products for Digital Signatures
- [ ] Trusted Computing
- [ ] Others

Q7. Which certification standards have you obtained for the IT products of your organization (please indicate as many as appropriate)?

- [ ] ISO/IEC 27001
- [ ] ISO/IEC 27002 (sometimes refer to ISO 17799 or BS7799)
- [ ] ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827)
- [ ] ISO/IEC 15408 (Common Criteria)
- [ ] IEC 62443
- [ ] ISO/SAE 21434
- [ ] ETSI EN 303 645
- [ ] FIPS 140-2
- [ ] NIST SP 800-90
- [ ] PCI (Payment Card Industry)
- [ ] Others

Q8. If your organization has obtained the Common Criteria certification in the past, which Evaluation Assurance Levels have been achieved for the certified IT products (please indicate as many as appropriate)?

- [ ] EAL1: Functionally Tested
- [ ] EAL2: Structurally Tested
- [ ] EAL3: Methodically Tested and Checked
- [ ] EAL4: Methodically Designed, Tested, and Reviewed
- [ ] EAL5: Semi-Formally Designed and Tested
- [ ] EAL6: Semi-Formally Verified Design and Tested
- [ ] EAL7: Formally Verified Design and Tested
- [ ] Protection Profile

Q9. Which certification standards do you plan to obtain for the IT products of your organization (please indicate as many as appropriate)?

- [ ] ISO/IEC 27001
- [ ] ISO/IEC 27002 (sometimes refer to ISO 17799 or BS7799)
- [ ] ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827)
- [ ] ISO/IEC 15408 (Common Criteria)
- [ ] IEC 62443
- [ ] ISO/SAE 21434
- [ ] ETSI EN 303 645
- [ ] FIPS 140-2
- [ ] NIST SP 800-90
- [ ] PCI (Payment Card Industry)
- [ ] Others

Q10. If your organization plans to obtain Common Criteria certification, which Evaluation Assurance Levels are planned to be achieved for the IT products (please indicate as many as appropriate)?

- [ ] EAL1: Functionally Tested
- [ ] EAL2: Structurally Tested
- [ ] EAL3: Methodically Tested and Checked
- [ ] EAL4: Methodically Designed, Tested, and Reviewed
- [ ] EAL5: Semi-Formally Designed and Tested
- [ ] EAL6: Semi-Formally Verified Design and Tested
- [ ] EAL7: Formally Verified Design and Tested
- [ ] Protection Profile

D1. Using the scale provided in the following questions, please indicate the extent to which you DISAGREE or AGREE with each of the challenges that could hinder the adoption of Common Criteria certification by your organization:

Q11. Common Criteria certification does not add any benefits to your products.

Strongly disagree	Somewhat	Neither agree nor	Somewhat agree	Strongly agree

Strongly disagree Somewhat disagree disagree

Q12. The Common Criteria evaluation costs are too expensive compared to the benefits brought into the evaluated products.

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

Q13. The Common Criteria evaluation time is too long compared to the product life cycle.

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

Q14. Your products do not need the Common Criteria certification because they are not IT security products.

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

Q15. The documentation requirements for Common Criteria evaluation are prohibitive so that it is difficult to obtain the Common Criteria certification.

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

Q16. The absence of approved Protection Profiles for the category of your products makes it difficult to obtain Common Criteria Certification.

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

Q17. There is a lack of mutual recognition on Common Criteria certification among the countries where your products are sold.

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

Q18. There is a lack of governmental drive (e.g., security certification requirements) in their procurement policy for Common Criteria certification in the target markets of your products.

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

Q19. Common Criteria certification is not a key driver for purchasing decisions of commercial customers in the target market of your products.

Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
○	○	○	○	○

Q20. If there are any other challenges that hinder your adoption of Common Criteria certification, please list and describe them in the space provided below:

Q21. What kind of incentive would be helpful for your organization for adopting Common Criteria certification?

Questions for IT consumers

Q22. Does your organization use IT products which are implemented in hardware, firmware, or software?

- ○ Yes
- ○ No

Q23. Which categories are relevant to the IT products used in your organization (please indicate as many as appropriate)?

- [ ] Access Control Devices and Systems
- [ ] Biometric Systems and Devices
- [ ] Boundary Protection Devices and Systems
- [ ] Data Protection
- [ ] Databases
- [ ] Detection Devices and Systems
- [ ] ICs, Smart Cards and Smart Card-Related Devices and Systems
- [ ] Key Management Systems
- [ ] Mobility
- [ ] Multi-Function Devices
- [ ] Network and Network-Related Devices and Systems
- [ ] Operating Systems
- [ ] Products for Digital Signatures
- [ ] Trusted Computing
- [ ] Others

Q24. Which certification standards do you look for when selecting the IT products used or to be used in your organization (please indicate as many as appropriate)?

- [ ] ISO/IEC 27001
- [ ] ISO/IEC 27002 (sometimes refer to ISO 17799 or BS7799)
- [ ] ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827)
- [ ] ISO/IEC 15408 (Common Criteria)
- [ ] IEC 62443
- [ ] ISO/SAE 21434
- [ ] ETSI EN 303 645
- [ ] FIPS 140-2
- [ ] NIST SP 800-90
- [ ] PCI (Payment Card Industry)
- [ ] Others

Q25. Which certification standards have been obtained for the IT products used in your organization (please indicate as many as appropriate)?

- [ ] ISO/IEC 27001

- [ ] ISO/IEC 27002 (sometimes refer to ISO 17799 or BS7799)
- [ ] ISO/IEC 21827 (SSE-CMM – ISO/IEC 21827)
- [ ] ISO/IEC 15408 (Common Criteria)
- [ ] IEC 62443
- [ ] ISO/SAE 21434
- [ ] ETSI EN 303 645
- [ ] FIPS 140-2
- [ ] NIST SP 800-90
- [ ] PCI (Payment Card Industry)
- [ ] Others

Q26. If your organization uses IT products with Common Criteria certification, which Evaluation Assurance Levels have been achieved for the IT products (please indicate as many as appropriate)?

- [ ] EAL1: Functionally Tested
- [ ] EAL2: Structurally Tested
- [ ] EAL3: Methodically Tested and Checked
- [ ] EAL4: Methodically Designed, Tested, and Reviewed
- [ ] EAL5: Semi-Formally Designed and Tested
- [ ] EAL6: Semi-Formally Verified Design and Tested
- [ ] EAL7: Formally Verified Design and Tested
- [ ] Protection Profile

Q27. In the absence of IT products with a security certification standard, how do you manage risks associated with potentially poor implementation of security functionality within the products?

Q28. In the absence of IT products with a security certification standard, how do you go about seeking assurances in the security functionality of the products?

Deakin University CRICOS Provider Code 00113B.