Brief for Authors
Major revision to existing Knowledge Area

This is a briefing document for CyBOK authors who are undertaking a major revision to an existing Knowledge Area (KA). It provides background information on the CyBOK process and the role of the authors, together with details of content and presentation. The purpose of the document is to provide the context for authors' work and to promote consistency between CyBOK chapters. If elements of this brief are impracticable for particular knowledge areas, authors are invited to propose alternatives.

More information about the CyBOK process and other aspects of the project can be found on the CyBOK website [1].

1 INTRODUCTION

A *body of knowledge* is the foundation knowledge that is generally accepted in underpinning a discipline. It is documented in books, published papers, reports and standards.

The Cyber Security Body of Knowledge (CyBOK) is a guide to the body of knowledge of the Cyber Security discipline. It provides a summary of foundation knowledge in cyber security with reference to seminal and other high quality documentation.

The CyBOK will be used to identify learning pathways in the subject to facilitate the design of courses ranging from school to PhD, including industry-specific education such as apprenticeships or continuing professional development. This remit requires the CyBOK to be accessible to a wide range of readers, from education planners at school level to security specialists in academia and industry.

The overall structure of the CyBOK is modelled on the IEEE Software Engineering Body of Knowledge (SWEBOK) [2]. It is organised as a series of chapters documenting specific Knowledge Areas (KAs). Each chapter is expected to be 15-20 published pages, most of which will be descriptive material subdivided into topics. Each KA chapter will include a reference list, cross-referenced to topics identified in the main text.

2 TERMS

The UK National Cyber Security Centre (NCSC) defines Cyber Security as:

The protection of devices, services and networks — and the information on them — from theft or damage.

This definition excludes electronic warfare or military intelligence gathering, except from the perspective of a defender.

As far as possible terms should be consistent with the NCSC glossary [3] and the NIST Glossary [4]; in the event of a conflict the NCSC glossary should take precedence. If it is necessary to use terms in different ways they should be defined and included in a chapter glossary, which may otherwise be unnecessary.

3 SCOPE

The scope of the CyBOK is cyber security, as defined above; the knowledge area to be revised by each author will be defined separately.

The documents referenced by the CyBOK are expected to be generally accepted as providing seminal or high-quality foundation material. Authors may select documents that overlap technically in order to provide different levels of description suitable for different audiences, or different perspectives on the same topic. However, the CyBOK will not attempt an exhaustive coverage of everything that has been published on a topic; it will be a matter for the author's judgement to decide what is significant.

Authors may decide that current controversies, issues, or debates are important because they indicate areas of uncertainty. If this is the case then such material should be distinguished as controversial and presented as a separate topic within the knowledge area.

There is a significant body of knowledge which is not unique to cyber security but on which cyber security depends. Examples include mathematical foundations (e.g., number theory), standard computer science (e.g., languages, operating systems), and network theory. As far as possible this will be excluded from the CyBOK; however, it will need to be considered when learning pathways are developed. Authors are, therefore, requested to provide a companion document, in note form, that identifies such knowledge and its relationship to the topics described in the KA chapter (prerequisites), in addition to cyber security topics which are relevant but out of scope for the KA (cross-dependencies).

4 PROCESS AND DELIVERABLES

The project follows an agile development model, working incrementally in a series of three month long 'sprints'. Authors will commit to 6 months work. This will require extensive work in the first 3 months to deliver a draft of the revised knowledge area chapter and respond to comments from the expert peer-review panel. The work in the following three months will respond to curated reviews from the public review process.

In more detail, the development and review process for a revised Knowledge Area (KA) chapter will take the following form:

- The KA author will prepare a marked up version of the published KA, showing places where substantive edits are expected (including headings for new topics/sub-topics, with indicative content listed) for initial review and feedback by the Expert Peer Reviewers. The edits should be based on the change request provided but may also cover other minor topics.
- The Expert Peer Reviewers will comment on the marked-up changes and any other issues they note in the KA as presented.
- The author will prepare a full draft which will be reviewed by the review panel, with changes from the published KA shown by automatic mark-up, generating feedback for the author. This step may be repeated if multiple iterations are required to revise the KA description. It is expected that the reviewers will comment on the KA in totality to ensure balance and flow.

- Once all feedback from the review panel has been addressed, the author will prepare a draft for public release which will be copy-edited prior to the public review phase.
- Given that the documents aim to provide a state of the art consensus for each KA, we consider it vital to include feedback from the wider community via a public review phase. We plan wide community consultation on the drafts through online community engagement, as well as via workshops held nationally and internationally (co- located with major international conferences). Community comments will be curated and filtered by the Executive Board, with the aim of providing only relevant and in-scope comments for further consideration. The author will then respond to these curated comments, updating the chapter as necessary.
- All publicly released drafts (after review by the Expert Peer-Review Panel) will be copy-edited professionally before wider consultation.

The project is committed to an open and transparent public process; however, to make the development manageable the written content will remain embargoed, confidential to the authors and expert panel reviewers, until it has been formally reviewed by the Executive Board (which may seek input from the Steering Committee as needed). All rights to the material produced by this project will be owned by CyBOK project; authors are free to make use of the material that they have developed.

Authors will be paid an honorarium for the work described here, specifically for:

(a) researching and writing a draft major revision to an existing knowledge area chapter,

(b) providing a knowledge dependency summary (prerequisites and cross-dependencies),

(c) responding to peer review and updating the KA chapter,

(d) responding to curated public comments and further updating the KA chapter, and

(e) following completion of the final KA revision, prepare and present/record both a webinar and interview style podcast giving a summary of the KA contents.

5 MANUSCRIPT AND FORMATTING REQUIREMENTS

The general requirements for the format of a knowledge area chapter have been described above, to summarise:

(a) The target size for each KA chapter is 20 pages, A4 size, including a cross-reference list, references, and a glossary if necessary.

(b) The content of each KA chapter should be divided into numbered topics and sub-topics, and a cross-reference table provided between sub-topics and references.

(c) Current debates or controversies should be separately distinguished at the topic level.

(d) The chapter may optionally include further reading suggestions.

(e) The chapter should include a glossary if it is necessary to use terms in a different way to the definitions in the NCSC glossary [3], or the NIST Glossary [4].

(f) Acronyms should be expanded on first use, and the chapter should include an acronyms list.

(g) Normal academic practice should be followed for numbered referencing and for quoted material.

The CyBOK project will use LaTeX for document production with Overleaf as the collaboration tool. A LaTeX template will be shared with each author as a style guide.

REFERENCES

[1] http://www.cybok.org

[2]P. Bourque and R.E. Fairley, eds., Guide to the Software Engineering Body of Knowledge, Version 3.0, IEEE Computer Society, 2014; www.swebok.org.

[3]NCSC Glossary, https://www.ncsc.gov.uk/glossary

[4]Kissel, Richard. NIST IR 7298 Revision 2: Glossary of Key Information Security Terms. National Institute of Standards and Technology, 2013. http://dx.doi.org/10.6028/NIST.IR.7298r2