Brief for Authors (new Knowledge Guides and Topic Guides)

This is a briefing document for CyBOK (Cyber Security Body of Knowledge) authors. 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 documents. If elements of this brief are impracticable for particular knowledge guides or topic guides, 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 foundational 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). In addition to KAs, CyBOK Knowledge Guides and Topic Guides are intended as supplementary CyBOK material:

- Knowledge Guides (KGs) represent a review of relevant literature on a topic (typically on an emerging topic) that captures the current state of the field, key issues that learners should know about, emerging techniques to address those issues and open research problems. It should be a standalone document (typically 10-15 pages excluding references) but make reference to the relevant foundational knowledge within CyBOK.
- Topic Guides (TGs) draw together topics from across a number of KAs, to give a unified treatment to a collection of topics distributed across CyBOK. In general, these will be crosscutting themes where practitioner knowledge is more prominent than academic thinking. The great majority of a TG's content should be a synthesis of concepts from existing KA topics, but a small amount of additional material (with suitable references) should be included as needed to provide a comprehensive treatment of the topic. The size of a TG is typically 5-10 pages (excluding references).

An author will usually be responsible for documenting a single KG or TG.

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 KG or TG to be covered 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 KG/TG.

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 KG/TG (prerequisites), in addition to cyber security topics which are relevant but out of scope for the KG/TG (cross-dependencies).

4. Process and Deliverables

Authors will commit to 4 months work. This will require work in the first 3 months to deliver a draft of the KG/TG and respond to comments from the expert peer-review panel. The work in the following month will be to finalise the KG/TG ready for public release.

In more detail, the development and review process for a KG or TG will take the following form:

- The KG/TG author or authors will prepare a strawman proposal for initial review and feedback by the CyBOK Executive Board.
- The author(s) will prepare a full draft which will be reviewed by a review panel of at least three expert reviewers, generating feedback for the authors. This step may be repeated if multiple iterations are required to revise the KG/TG draft.

- Once all feedback from the review panel has been addressed, the author(s) will prepare a final version for agreement with the CyBOK Executive Board, which will then be copy- edited professionally prior to public release.

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 KG/TG,
b) responding to peer review and updating the KG/TG,
c) following completion of the final KG/TG, preparing and recording both a webinar and interview style podcast giving a summary of the KG/TG contents.

5. Manuscript and Formatting Requirements

The general requirements for the format of a KG and TG have been described above, to summarise:

a) The target size for each KG is 10-15 pages, A4 size, including a cross-reference list, and a glossary if necessary, excluding references.
b) The target size for each TG is 5-10 pages, A4 size, including a cross-reference list, and a glossary if necessary, excluding references.
c) The content of each KG/TG should be divided into numbered topics and sub-topics, and a cross-reference table provided between sub-topics and references.
d) Current debates or controversies should be separately distinguished at the topic level.
e) The KG/TG may optionally include further reading suggestions.
f) The KG/TG 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].
g) Acronyms should be expanded on first use, and the KG/TG should include an acronyms list.
h) Normal academic practice should be followed for numbered referencing and for quoted material.

The CyBOK project will use LaTeX for document production with Bitbucket 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