# Paper #4: Compare / Contrast the ENISA and Commonwealth Approaches to Developing National Cybersecurity Strategies

## Scenario:

Your company has assigned you to serve as an industry subject matter expert and advisor for a *cyber policy competition* team for a local university. This year, the team will be competing in an international Cyber Policy competition in Washington, DC. The policy question for this year’s competition is: *what is the best approach for developing a national cybersecurity strategy?* The competition will have one U.S. team and nine additional teams from Europe (4 teams) and the Commonwealth nations (5 teams).

The university students have asked you to help them understand the problem space and the likely approaches that competing teams will take. To accomplish this goal, you have decided to **prepare a white paper in which you compare the *European Union Agency for Network and Information Security* (ENISA) guidance document for cybersecurity strategies to a similar document prepared by the *Commonwealth Telecommunications Organization* (CTO)**. ENISA provides cybersecurity guidance for member states of the European Union (<http://europa.eu/index_en.htm> ). CTO provides cybersecurity guidance for members of the *Commonwealth of Nations* (<http://www.commonwealthofnations.org/>).

Your starting point for your analysis will be outlines of the two documents (Table 1 and Table 2) which were provided to the teams by the competition’s organizers.

## Research:

1. Review the document outlines provided in Tables 1 and 2 (at the end of this document).
2. Download and review the full documents
   1. CTO: [http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20‌Approach%20‌for%20‌National%20‌Cybersecurity%20Strategies.pdf](http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf)
   2. ENISA: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport>
3. Develop five or more points which are common across the two documents. (Similarities)
4. Identify and review at least three unique items in each document. (Differences)
5. Research three or more national cybersecurity strategies from EU or Commonwealth nations which were written in or available in English (see the list in Appendix 1 of the CTO document). How comprehensive are these documents when compared to either the ENISA or the CTO guidance? From these documents and the ENISA / CTO guidelines, develop an answer to the question: Why should every nation have a cybersecurity strategy?

## Write:

Write a five (5) to eight (8) page white paper in which you summarize your research and discuss the similarities and differences between the two guidance documents. You should focus upon clarity and conciseness more than length when determining what content to include in your paper. At a minimum, your white paper must include the following:

1. An introduction or overview of *national cybersecurity strategies*. Explain the purpose of a national cybersecurity strategy and how it is used. Answer the question: why should every nation have a cybersecurity strategy? (Make sure that you address the importance of such strategies to small, resource-poor nations as well as to wealthy, developed nations.)
2. A separate section in which you discuss the common principles and guidelines (similarities) found in both guidance documents (ENISA & CTO).
3. A separate section in which you discuss the unique aspects of the CTO principles and guidelines for national cybersecurity strategies.
4. A separate section in which you discuss the unique aspects of the ENISA principles and guidelines for national cybersecurity strategies.
5. A section in which you present your recommendations to the competition team as to the approach (next steps) they should take in further refining their answer to the competition question: *what is the best approach for developing a national cybersecurity strategy?*

## Submit For Grading

1. Submit your white paper in MS Word format (.docx or .doc file) using the OPEN Data Assignment in your assignment folder. (Attach the file.)
2. You must also submit your white paper to TurnItIn before the due date for this assignment.

## Additional Information

1. Your white paper should use standard terms and definitions for cybersecurity concepts. The following sources are recommended:
   1. ISACA Glossary <http://www.isaca.org/pages/glossary.aspx>
   2. Guidelines on Security and Privacy in Public Cloud Computing <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>
   3. *Glossary* sections in the two guidance documents (ENISA & CTO)
2. You are expected to credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must comply with APA 6th edition Style requirements. Failure to credit your sources will result in penalties as provided for under the university’s Academic Integrity policy.
3. Use APA 6th edition style (formatting) for the organization and appearance of the MS Word document that you submit to your assignment folder. This includes margins, section headings, and consistent use of fonts (Times New Roman 12 in black), paragraph styles (first line indent by ½ inch), and line spacing (double). Formatting requirements and examples are found under Course Resources > APA Resources. Your file should contain both a title page and a separate References page. Use page breaks to ensure that the title page and references page are separate from the body of the paper.
4. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs. These items are graded under Professionalism and constitute 15% of the assignment grade.

**Table 1. Outline for *Commonwealth Approach for Developing National Cybersecurity Strategies* (Commonwealth Telecommunications Organisation, 2015).**

|  |
| --- |
| 3 CREATING AND USING A NATIONAL CYBERSECURITY STRATEGY  3.1 Development of the Strategy  3.1.1 An approach to design of the strategy: risk-based and outcome-focused  3.1.2 The use of a maturity model  3.1.3 Key performance indicators  3.1.4 Resources and market forces  3.1.5 Communicating its concepts and ideas  3.2 Delivering the Strategy  3.3 Reviewing the Strategy  4 KEY ELEMENTS OF A CYBERSECURITY STRATEGY  4.1 Introduction and background section  4.2 Guiding principles section  4.3 Vision and strategic goals section  4.4 Objectives and priorities section – using a risk-based approach  4.5 Stakeholder section  4.6 Governance and management structure  4.7 Strategy implementation section  4.7.1 Legal and regulatory framework  4.7.2 Capacity Building  4.7.3 Awareness  4.7.4 Local technical capability  4.7.5 Incident response  4.8 Monitoring and evaluation |

**Table 2. Outline for *National Cyber Security Strategies: Practical Guide on Development and Execution* (European Network and Information Security Agency, 2012).**

|  |
| --- |
| 2 National cyber security strategy lifecycle  3 Develop and execute the national cyber-security strategy  3.1 Set the vision, scope, objectives and priorities  3.2 Follow a national risk assessment approach  3.3 Take stock of existing policies, regulations and capabilities  3.4 Develop a clear governance structure  3.5 Identify and engage stakeholders  3.6 Establish trusted information-sharing mechanisms  3.7 Develop national cyber contingency plans  3.8 Organise cyber security exercises  3.9 Establish baseline security requirements  3.10 Establish incident reporting mechanisms  3.11 User awareness  3.12 Foster R&D  3.13 Strengthen training and educational programmes  3.14 Establish an incident response capability  3.15 Address cyber crime  3.16 Engage in international cooperation  3.17 Establish a public–private partnership  3.18 Balance security with privacy  4 Evaluate and adjust the national cyber-security strategy  4.1 Evaluation approach  4.2 Key performance indicators |

**References:**

Commonwealth Telecommunications Organisation. (2015). *Commonwealth approach for developing national cybersecurity strategies*. London, UK: Author. Retrieved from [http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20‌Approach%20‌for%20‌National%20‌Cybersecurity%20Strategies.pdf](http://www.cto.int/media/fo-th/cyb-sec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf)

European Network and Information Security Agency. (2012). *National cyber security strategies: Practical guide on development and execution.* Heraklion, Crete, Greece: Author. Retrieved from <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport>