

# Play NICE: Incorporating Cyber Phraseology Into K-12 Education

Timothy Crisp  
School of Cyber Studies  
The University of Tulsa  
Tulsa, OK, USA  
0009-0007-0266-6542

John Hale  
Tandy School of Computer Science  
The University of Tulsa  
Tulsa, OK, USA  
0000-0002-6664-0655

**Abstract**—Cyberattacks on critical infrastructures motivate a focus on cybersecurity awareness. A knowledge gap exists in the technical and non-technical understanding of cybersecurity, in the workforce. Closing this gap requires a multi-faceted approach --of extreme importance is education. We use the NICE Workforce Framework TKS statements to develop a model of the most generalizable requirements needed to practice cybersecurity. We apply this model to increase cybersecurity language use and comprehension in all K-12 subjects, walking educators through a process incorporating cybersecurity into their lessons.

**Keywords**—*Cybersecurity Education, K-12, Cybersecurity Literacy, NICE Workforce Framework*

## I. INTRODUCTION

Cyberattacks pose grave threats to our critical infrastructures [1-4]. The world needs a more robust cybersecurity workforce, but also a general workforce that is aware, literate and trained to prevent and respond to cyberattacks. Cybersecurity education is now an essential component of K-12 education, which prepares the future workforce. To instill cyber hygiene in the workforce, we propose a model and curricular solution for K-12 education.

This paper is organized as follows: Section II outlines the need for cybersecurity education, describing the current K-12 landscape. Section III presents the national objectives for cybersecurity education and the workforce alongside an analysis of the NICE Framework. Section IV presents our method and analysis for integrating cybersecurity into all K-12 subjects and provides insights based on preliminary efforts. Section V offers concluding remarks along with future work.

## II. NEED FOR CYBER HYGIENE

Cybercrime and cybersecurity are not new to the computer science uniqueness debate, which contemplates whether technology creates new crimes or simply transforms existing ones [5]. In the face of these threats, most of the workforce lack the general awareness and literacy needed to protect themselves [1], [3], [6-9]. At the same time, a gap exists in our education system. This educational gap exists because programs for preparation in IT and computing fail to focus on

cybersecurity hygiene education. This is also manifested by the lack of focused coursework [10].

Cybersecurity education bifurcates into the technical and non-technical (encompassing managerial and psychological) [1], [11]. Technical education focuses on techniques and technologies to prevent, detect, and mitigate cyberattacks. These targets focus on educating and producing employees with the hard skills required to keep systems secure. Managerial and psychological education focuses on developing an individual's ability to recognize signs of attacks through literacy and awareness, resulting in heightened cyber hygiene [7]. This research aims to address the dichotomy of technical and non-technical (managerial and psychological) K-12 cybersecurity education programming at the state level.

There are three broad levels of education for cybersecurity: K-12, college, and on-the-job training [6], [12-13]. The space for education and training is very diverse in need, as on-the-job training focuses on those who are already in the workforce, while college and K-12 are focused on those aspiring to future careers. Some argue that on-the-job training is most needed to strengthen the skills of employees already at organizations, as they pose the greatest immediate risk to an organization's security [14-15]. Others argue that universities need to implement more cybersecurity curriculum into their courses of study for students to grow a cyber workforce skilled to handle emerging challenges [16-17]. Other literature explains how cyber education should be incorporated in K-12 curriculum, building cyber hygiene skills of youth to keep them safe and cultivate a cyber-savvy workforce [12], [17-18].

## III. CYBERSECURITY EDUCATION STANDARDS

Standards are integral to our objective, centered on curriculum for K-12 schools. K-12 institutions are required to offer courses based on their state's graduation requirements and align them to standards established by the state's Department of Education. Often courses do not have state standards which go beyond cybersecurity awareness. (These are generally elective courses.) When states lack standards for courses, academic organizations and curriculum companies generally create standards for them. Research exploring the current standards for K-12 cyber education is lacking as there is only one state currently with a claimed

dedicated set of standards for cybersecurity, and only a few major K-12 curricula designed with standards for cybersecurity. North Dakota (ND) has implemented a cybersecurity K-12 set of standards for the entire state and required it to be implemented by the year 2026 [19].

These standards were created by ND House Bill (HB) 1398 and were established as a part of their “North Dakota Computer Science and Cybersecurity Standards” [19-20]. These standards, however, are not explicitly for cybersecurity but, as with other states, are incorporated in the computer science standards as a Digital Citizenship component. While specific state standards may not exist for cybersecurity, many Computer Science standards have a section covering cybersecurity topics yet exclude cyber hygiene. Oklahoma’s Academic Standards for Computer Science (OASCS) have a cybersecurity component for grades K-10 but are only covered as short units rather than full course subject matter creating a gap in cyber hygiene awareness [21]. Oklahoma’s Computer Science Standards were published in 2023 and implemented in the 2024-2025 school year. These standards focus on Computer Science but include one singular sub-concept for Cybersecurity. This sub-concept relates predominantly to the non-technical side of cybersecurity education – managerial and psychological – focusing on being better digital citizens with good cyber hygiene.

The National Institute of Standards and Technology (NIST) launched the National Initiative for Cybersecurity Education (NICE) in 2008 [17]. NICE fully formed under Title IV “National Cybersecurity Awareness and Education Program” of the Cybersecurity Enhancement Act of 2014 [16]. NICE is designed to “energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development” [18]. The NICE Workforce Framework for Cybersecurity (NICE Framework) was “established to provide a standard approach and common language for describing cybersecurity work and learner capabilities ... seeking to improve communication around stakeholders throughout the cybersecurity ecosystem about how to identify, recruit, develop, and retain talent” [20]. It constitutes an influential and evolving artifact for understanding and speaking about cybersecurity roles and job functions. It also offers a valuable lens through which to perceive cyber hygiene requirements for the workforce.

#### IV. NIST NICE WORKFORCE FRAMEWORKS

##### A. Definition

The NICE Framework was originally established by Special Publication (SP) 800-181 in 2017 and updated with its first revision SP 800-181r1 in 2024 [20]. The initial framework identified seven work role categories outlining areas of work for cybersecurity professionals (Figure 1). Work roles are individual tasks an employee might complete as part of their job – each job can be responsible for more than one work role. Ultimately, the Framework breaks these categories into 52 individual work roles. Figure 1 shows the number of work roles in each category. The Framework adopts a modular approach characterizing the cybersecurity workforce using Task, Knowledge, and Skill (TKS) Statements. Each TKS Statement describes the work an individual conducts for their job. Each task requires a set of skills and knowledge. The current Framework has 2,280 individual TKS Statements.

##### B. TKS Statement Frequency Analysis

We analyze the NICE Framework, yielding a model to support cybersecurity education. This framework is beneficial for K-12 education, as it provides a basis for the tasks, knowledge, and skills an employee needs for good cyber hygiene. Using the framework, educators can establish lessons and assignments to teach learners. There are many curricula, guidelines, and objectives which have used these TKS Statements to develop their content. Using these TKS Statements absent any analysis, an educator might lean on an instinctive understanding of the connections between job roles in the cybersecurity workforce landscape. Here we propose a more systematic approach, yielding a model suitable for teaching cyber hygiene.

The NICE Framework lacks an organization of the TKS Statements which would enable an instructor to start from a standardized introductory baseline. The framework does not categorize the TKS Statements based on generalizability into all work roles. Thus, curriculum development for new or re-skilled learners is challenging, as these individuals do not yet know the work role they will fulfill. In addition, the model we derive should evolve as revisions of the NICE Framework are released. Here, we adopt NICE SP-800-181-r1 and its supplemental documentation on the TKS Statements [19], [21].

*16 Work Roles | 8 Work Roles | 7 Work Roles | 7 Work Roles | 2 Work Roles | 5 Work Roles | 7 Work Roles*



Fig. 1. NICE Framework Work Role Categories.

We propose a model enabling K-12 educators to create content based on TKS Statements most generalizable to all cybersecurity work role categories. This model relies on the frequency in which TKS Statements appear in the seven individual work role categories and, more specifically, the individual work roles of each category. We separate all 2,280 TKS Statements into a frequency of appearance model for each work role and its respective category (Table I). Each of the 52 work roles forms enumerate the TKS Statements from the 2,280 required for their respective roles. 20 TKS Statements were found in all seven work role categories. 37 TKS Statements were found in six of the seven work role categories. Collectively, we regard these 57 TKS Statements as the most generalizable educational targets for integration into K-12 subjects.

TABLE I. NICE Framework TKS Statement Frequencies.

Work Role Categories Covered	Number of TKS Statements	Percent TKS Coverage
7 of 7 Categories	20	1%
6 of 7 Categories	37	2%
5 of 7 Categories	55	2%
4 of 7 Categories	105	5%
3 of 7 Categories	202	9%
2 of 7 Categories	405	18%
1 of 7 Categories	1316	58%
0 of 7 Categories	140	6%
Total TKS Statements	2280	

C. TKS Statement Frequency Analysis Continued

In the initial analysis, we found 20 TKS Statements (Table II) which fit into all seven work role categories in the NICE Framework. However, each category has multiple work roles. Therefore, just because a work role exists inside a category, it does not mean that it exists inside all the work roles.

TABLE II. NICE Framework TKS Statement Frequencies.

K0674	Knowledge of computer networking protocols
K0675	Knowledge of risk management processes
K0676	Knowledge of cybersecurity laws and regulations
K0677	Knowledge of cybersecurity policies and procedures

K0678	Knowledge of privacy laws and regulations
K0679	Knowledge of privacy policies and procedures
K0680	Knowledge of cybersecurity principles and practices
K0681	Knowledge of privacy principles and practices
K0682	Knowledge of cybersecurity threats
K0683	Knowledge of cybersecurity vulnerabilities
K0684	Knowledge of cybersecurity threat characteristics
K0710	Knowledge of enterprise cybersecurity architecture principles and practices
K0751	Knowledge of system threats
K0752	Knowledge of system vulnerabilities
K0791	Knowledge of defense-in-depth principles and practices
K0812	Knowledge of digital communication systems and software
K0915	Knowledge of network architecture principles and practices
K0983	Knowledge of computer networking principles and practices
K1014	Knowledge of network security principles and practices
T1020	Determine the operational and safety impacts of cybersecurity lapses

We hypothesize that the 20 most generalizable TKS Statements must also be inside most if not all of the individual work roles themselves. We extended our analysis to determine which of these were inside each of the individual work roles for each category (Figure 2).

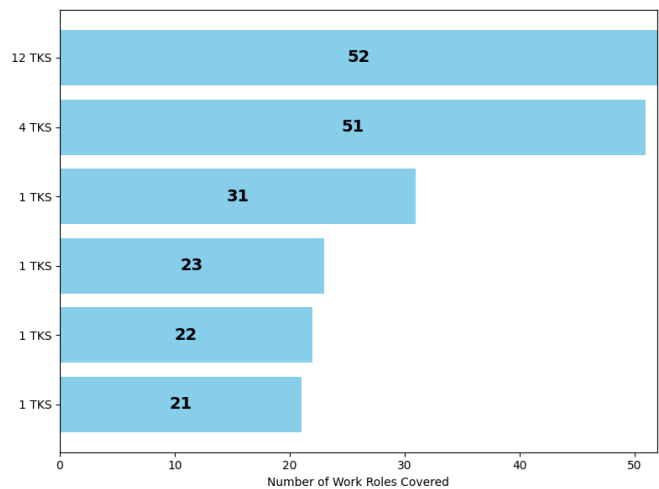


Fig. 2. 20 Most Generalizable TKS Statements Distribution of Work Role Coverage. (Generated by Copilot)

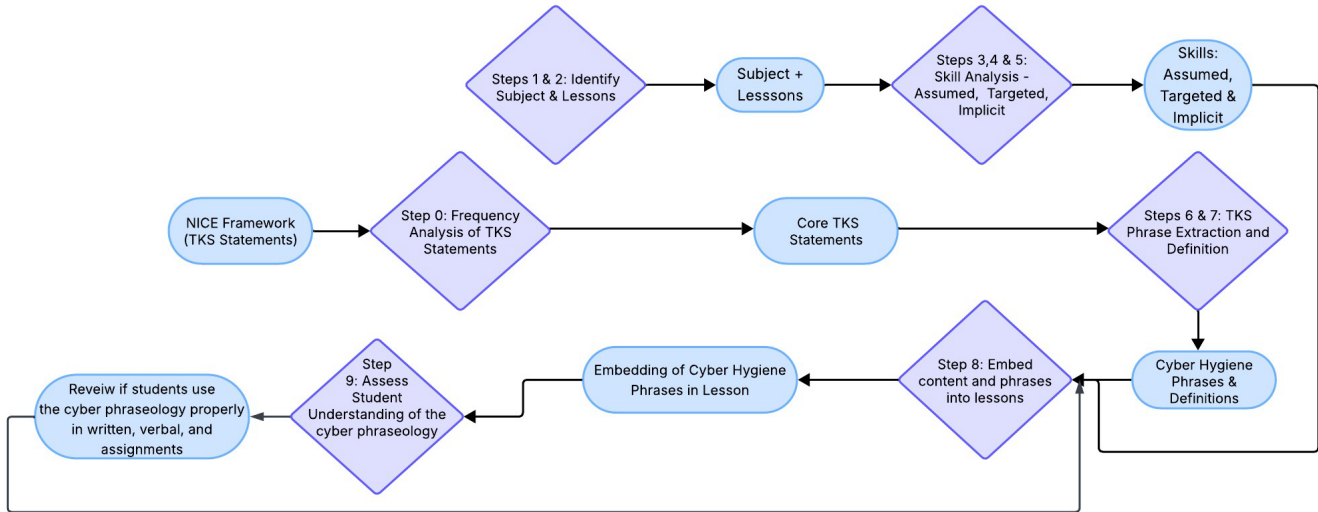


Fig. 3. Model Overview

Here we see that 12 of the 20 TKS Statements appear in all 52 work roles of the NICE Framework and four more appear in all but one. 16 of the original 20 most generalizable TKS Statements are not only generalizable to the seven categories, but also 98% of the TKS statements, with 12 being required for 100%. By utilizing these TKS Statements, K-12 educators can cover the most ground. Additionally, this analysis offers an understanding of when they should teach the material, beginning with the 12 required for all work roles and then moving into the four in 51 of the 52. For the purpose of this research, when using these TKS Statements we can begin with these as the most important to incorporate in our classrooms in order to increase cybersecurity knowledge.

V. INTEGRATING CYBERSECURITY INTO ALL K-12 SUBJECTS

Non-technical (the managerial and psychological) cybersecurity education is extremely important for increasing the cyber resilience of everyday people who do not work in cybersecurity. One component of our approach is the integration of a common cybersecurity language into K-12 classrooms. Science, Technology, Engineering, and Math (STEM) education is a path educational institutions can follow to increase the general cybersecurity knowledge through instruction. STEM education is integrated throughout all subjects, using STEM language (terminology) to inculcate a robust understanding of STEM ideas in school [22]. This practice enhances the STEM understanding of students and promotes a STEM-based attainment goal from students globally [22]. This practice can be applied to cybersecurity increasing the cybersecurity knowledge and attainment goals of learners. This section presents a method and process to teach teachers how to integrate cybersecurity topics into their lessons using the NICE Framework TKS Statements.

A. Method

To increase cybersecurity language use in K-12 classrooms, we define a model educators can use to process the most generalizable TKS Statements to learn what terms should be included in their lessons. The model has three components: (1) a Worksheet, (2) a Critical Thinking Guidance Sheet, and (3) the most generalizable 20 TKS Statements. An eight-step process uses a guided worksheet to complete the steps necessary to develop classroom statements incorporating terms generalizable to cybersecurity.

This model (Figure 3) using the worksheet can be exercised by an individual and was designed to be given in a professional development guided presentation. As an instructor becomes more familiar with cybersecurity language, this process will become more natural, and the frequency of cybersecurity terminology used in their classroom will increase. (1) The first step in this process is simple for teachers to complete: identify the subject. In this step, the instructor names the course subject (e.g., math or science) for which they will be developing classroom statements. (2) In step two, the teacher considers the unit or lesson they will teach next in their classroom. Table III shows steps 1 and 2 completed using an example of an English teacher planning classroom statements on cybersecurity for literary elements.

TABLE III. Steps 1 and 2 of Integrating Cybersecurity Language Through all K-12 Subjects

<b>Step 1</b>	<i>What subject(s) do you teach?</i>	English
<b>Step 2</b>	<i>When school resumes what is your next unit lesson?</i>	Frankenstein (the graphic novel)-Literary Elements

(3) The third step of this process is to consider the following question: what skills do students need to know before the lesson? Here, an instructor must assess the knowledge and skills that a student already possesses. To develop classroom statements including cybersecurity language, an instructor must understand the difference between information they will cover, and knowledge students already know (see Table IV).

(4) In the fourth step, the instructor analyzes the skills/knowledge a student will learn. Here a teacher will examine the objectives and standards from their lesson plan, documenting them from their curriculum. The goal of this step is to frame the remaining steps towards the goals of the unit/lesson. An example of this step can be seen in Table IV.

TABLE IV. Steps 3 and 4 of Integrating Cybersecurity Language Through all K-12 Subjects

<b>Step 3:</b> What skills do scholars need to know before the lesson is taught? Fill in your replies below:		
<b>Prior Knowledge</b>		
Reading Comprehension	Table of Contents	Use of a Dictionary
Timeline of a Story	Identifying Main Ideas	Summarizing
Parts of Speech	Asking Questions	Annotating Texts
<b>Step 4:</b> What skills will scholars learn in this lesson?		
<b>Learned Skills</b>		
Conflict	Mood	Plot
Character	Setting	Symbolism
Theme	Tone	

(5) The fifth step of this process asks teachers to characterize the implicit skills or underlying competencies students will learn. This step is often quite difficult, as it challenges the instructor to think outside of the lesson plan and the inherent skills they will be teaching. When a lesson is created, it is designed to assist students with retaining and meeting the standards. However, every lesson has what is known as a hidden curriculum to educators, which is the idea that teachers teach students skills without them knowing. Often this hidden curriculum is generalized to be more from the social/psychological area, but this concept can also be applied to underlying competencies a lesson gives students from the academic content [3], [23-24]. Ultimately, students are learning objectives not explicitly called out in the classroom. These are often gained from the teacher describing or answering questions about content. Table V continues the English example showing hidden curriculum and underlying competencies students gain from classroom

discussions of reading. A document was created to guide instructors through this process, discussing common implicit skills/underlying competencies from major subjects and elective courses.

TABLE V. Steps 5 of Integrating Cybersecurity Language Through all K-12 Subjects

<b>Step 5:</b> What are the implicit skills/underlying competencies scholars will use/learn during this lesson? (Use the guided suggestions on the handout sheet to help spark your thought processes).	
<b>Implicit Skills/Underlying Competencies</b>	
Pattern Recognition	Symbolic Interpretation
Understanding Authorial Intent	Organization
Graph Theory	

(6) The sixth step asks the teachers to engage with the NICE Workforce Framework TKS Statement Frequencies, specifically the 20 which appear in all work roles from the framework. When reviewing the 20 TKSs, the extended analysis indicates that teachers should focus on the 16 TKS Statements which appear in 98% or more of all the work roles. Only the most generalizable TKS Statements are given to instructors for two reasons: First is to not overwhelm instructors with the responsibility of understanding 2,280 TKS Statements. Second, is to use the cybersecurity language most generalizable to the field. Teachers are asked to do two things in the sixth step. The first is to read through the 20 TKS Statements and analyze them for emerging words. Once teachers have read through these TKS Statements, they are asked to document these terms in the worksheet. Working in a Professional Development (PD) session or with other participants is encouraged here, as each individual will recognize different emerging words. Table VI continues the English example for step 6.

TABLE VI. Steps 6 of Integrating Cybersecurity Language Through all K-12 Subjects

<b>* This next step might require you to Google, as it requires an understanding of the competencies behind the 20 TKS statements we will use from the NIST Framework. *</b>	
<b>Step 6:</b> Analyze the provided, most generalizable TKS statements (20 given to you) and find the words from each that stand out the most. Fill in your responses below:	
<b>Emerging Words...</b>	
Principles and Practices	Networking
Cybersecurity	Defense-In-Depth
Privacy	Vulnerabilities
Digital Communication	

(7) Step 7 asks the instructor to research the words emerging in the previous step. Instructors are encouraged to use the words “in cybersecurity” while researching the emerging words guiding them to the most effective definition of the term. It is imperative that instructors research what the terms used in the most generalizable 20 TKS Statements mean in cybersecurity. Understanding these common terms helps instructors comprehend and grasp the objective of the model – including cybersecurity language into their class. Table VII shows this step continuing with the English example.

TABLE VII. Steps 7 of Integrating Cybersecurity Language Through all K-12 Subjects

<b>Step 7:</b> Google/research those words or write what you know about them:	
<b>Word Meanings...</b>	
Principles and Practices are the <u>foundational concepts</u> used in a line of work, field of study ... various contexts	<u>Networking</u> is the practice of connecting and securing multiple systems, devices, and networks to <u>communicate</u> and <u>share data</u> .
Cybersecurity is the practice of <u>CIA, IAAA, and Protection and Defense</u> .	Defense-In-Depth is the practice of establishing <u>redundancy</u> and <u>resilience</u> with <u>multiple defense/protections</u> for threats.
Privacy is the <u>protection</u> of <u>information</u> and systems from <u>unauthorized</u> access or use	Vulnerabilities are weaknesses of flaws that can be exploited in a system, app, or network.
Digital Communication Transmitting data and ensuring it is secure with: <u>encryption</u> , <u>authentication</u> , <u>secure protocols</u> , <u>non-repudiation</u> , etc.	

(8) The final step prepares the teacher to use the literate aspect development, which they have researched, in the lesson they analyzed at the beginning of the process. This asks the teacher to consider phrases they would use in their classroom to teach the upcoming unit or lesson and incorporate these phrases by adapting their normal verbiage to incorporate the emerging words. An example is talking about “errors,” “holes,” or “gaps” as “vulnerabilities” instead. Such minor shifts have proven effective in the incorporation of STEM languages and can be effective here as well [22]. Table VIII shows step 8 concluding the English example.

(9) As instructors and curriculum designers alike begin to engage in this process, an increase in the usage of cybersecurity language will occur. Step 9 consists of a feedback loop, where teachers can use the assessment method of their choice to test students learning attainment, understanding if there is an increase use and knowledge of cyber phraseology. Hearing the same terminology used in cybersecurity throughout other contents and in different contexts will help students better understand concepts related to cybersecurity. If students are struggling to grasp the

concepts, instructors should loop back to Step 8, reconsider and adjust the embedding of phrases in their course.

TABLE VIII. Steps 8 of Integrating Cybersecurity Language Through all K-12 Subjects

<b>Step 8:</b> Add these phrases/words above to a few statements you could use in class which tie into the implicit skills/underlying competencies/incidental learning you wrote down above:	
<b>Classroom Statements</b>	
As you identify the <u>vulnerabilities</u> in the plot, think about ways you could fix the flaws. Let’s write those down.	When setting out the timeline of the plot, think about cybersecurity and privacy using a timeline of Hackers events to tell the story.
What patterns did you recognize in this Chapter? How could you <u>network</u> between the patterns?	

*B. Preliminary Experience and Results*

The model was presented at the 2024 NICE K-12 Cybersecurity Education Conference and tested before two groups of instructors. The first group was a practice run in preparation for the conference. This was conducted at a local Oklahoma high school and middle school where one of the co-authors currently teaches courses in Cybersecurity Basics and Computer Science Principles. The teachers participating were from different subjects and levels of administration. Teachers who participated discussed how beneficial this model was in increasing their understanding of Cybersecurity. When speaking with the teachers a few weeks later, they expressed how they had used some of these phrases in their classroom. Key takeaways from this experience include:

- The structured model helped instructors have a better understanding of cybersecurity terminology.
- Instructors felt more confident in understanding cybersecurity.
- The model assisted in thinking about the implicit skills their lessons taught.

The second presentation was conducted at the NICE K-12 Cybersecurity Education Conference in San Antonio, Texas. This presentation was attended by directors and administrators of NICE and the NICE K-12 division, teachers, curriculum developers, administrators, cybersecurity professionals, and higher education employees. The response was an overwhelming appreciation and engagement in the process. Teachers were excited to return to their schools to use the phrases they had developed by walking through the model in the presentation. Others were eager to obtain copies of the presentation and model to use in their districts to encourage teacher’s support in increasing Cybersecurity Languages in their school. Administrators from NICE were very eager to see where the research led, and how it would align with the forthcoming release of NICE Framework version 2.0.0.

## VI. CONCLUSIONS AND FUTURE WORKS

The prevalence of cyberattacks on critical infrastructures motivates a focus on cyber awareness. However, a knowledge gap exists in the workforce. Eliminating this gap requires concerted efforts at the K-12 level to instill good cyber hygiene in the next generation of workers. We have proposed a model leveraging NIST's NICE Framework that K-12 educators can use to embed cybersecurity phraseology in lessons across subjects to increase literacy, awareness and cyber hygiene for all students. This approach extracts the most common and generalizable Task, Knowledge and Skill (TKS) Statements in NICE to derive a foundational lexicon for cybersecurity. The resulting set of phrases can be embedded with lessons on virtually any subject. This offers educators a systematic method for enhancing the cyber hygiene of their students.

## ACKNOWLEDGEMENT

This project was supported in part by federal award number ARPAYY001807 awarded to the State of Oklahoma and administered by OCAST and OMES, by the U.S. Department of the Treasury. Matching funds were provided for this project by the George Kaiser Family Foundation.

## REFERENCES

- [1] S. L. Garfinkel, "The cybersecurity risk," *Commun. ACM*, vol. 55, no. 6, pp. 29–32, Jun. 2012, doi: 10.1145/2184319.2184330.
- [2] M. Gracy, B. R. Jeyavadhanam, P. K. Babu, S. H. Karthick, and R. Chandru, "Growing Threats Of Cyber Security: Protecting Yourself In A Digital World," in *2023 International Conference on Networking and Communications (ICNWC)*, Apr. 2023, pp. 1–5. doi: 10.1109/ICNWC57852.2023.10127398.
- [3] T. Moffitt, "2020's Most (and Least) Cyber-Secure States | Webroot," *Webroot Blog*. Accessed: Nov. 10, 2022. [Online]. Available: <https://www.webroot.com/blog/2020/04/03/2020s-most-and-least-cyber-secure-states/>
- [4] "NICE Framework History," NIST, Jul. 2024, Accessed: Apr. 10, 2025. [Online]. Available: <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/about/nice-framework-history>
- [5] H. T. Tavani, "The uniqueness debate in computer ethics: What exactly is at issue, and why does it matter?," *Ethics and Information Technology*, vol. 4, no. 1, pp. 37–54, Mar. 2002, doi: 10.1023/A:1015283808882.
- [6] J. Jacob, W. Wei, K. Sha, S. Davari, and T. A. Yang, "Is the Nice Cybersecurity Workforce Framework (NCWF) Effective for a Workforce Comprising of Interdisciplinary Majors?," *Proceedings of the 16th International Conference on Scientific Computing (CSC'18)*. Las Vegas, USA., Aug. 2018, Accessed: Nov. 09, 2022. [Online]. Available: <https://par.nsf.gov/biblio/10095246-nice-cybersecurity-workforce-framework-ncwf-effective-workforce-comprising-interdisciplinary-majors>
- [7] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *Journal of Information Security and Applications*, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/j.jisa.2018.08.002.
- [8] "(ISC)<sup>2</sup> 2022 Cybersecurity Workforce Study." Accessed: Nov. 10, 2022. [Online]. Available: <https://www.isc2.org/443/Research/Workforce-Study>
- [9] "2024 ISC<sup>2</sup> Cybersecurity Workforce Study." Accessed: Apr. 13, 2025. [Online]. Available: <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>
- [10] F. Chiosea, "The State of Cybersecurity Education in K-12 Schools," p. 12.
- [11] D. Kocsis and D. Segal, "Cyber Hygiene, Cyberpsychology, and Impacting the Future Workforce," *AMCIS 2022 TREOs*, Aug. 2022, [Online]. Available: [https://aisel.aisnet.org/treos\\_amcis2022/79/](https://aisel.aisnet.org/treos_amcis2022/79/)
- [12] S. Alrabaee, M. Al-Kfairy, and E. Barka, "Efforts and Suggestions for Improving Cybersecurity Education," in *2022 IEEE Global Engineering Education Conference (EDUCON)*, Mar. 2022, pp. 1161–1168. doi: 10.1109/EDUCON52537.2022.9766653.
- [13] "Cyber Security for Everyone: An Introductory Course for Non-Technical Majors," *JCERP*.
- [14] M. Baker, "STRIVING FOR EFFECTIVE CYBER WORKFORCE DEVELOPMENT," p. 26.
- [15] "Kaspersky Security Bulletin 2021. Statistics." Accessed: Nov. 10, 2022. [Online]. Available: <https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/>
- [16] Joint Task Force on Cybersecurity E, *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY, USA: ACM, 2018. doi: 10.1145/3422808.
- [17] "ACM Supplement to CSEC 2017: Content for a Foundational Cybersecurity Degree Course." Accessed: Apr. 13, 2025. [Online]. Available: <https://dl.acm.org/doi/book/10.1145/3715982>
- [18] G. Javidi and E. Sheybani, "K-12 Cybersecurity Education, Research, and Outreach," in *2018 IEEE Frontiers in Education Conference (FIE)*, Oct. 2018, pp. 1–5. doi: 10.1109/FIE.2018.8659021.
- [19] K. Dempsey, "North Dakota Computer Science and Cybersecurity Standards".
- [20] "HB1398." Accessed: May 21, 2024. [Online]. Available: <https://ndlegis.gov/assembly/68-2023/regular/documents/23-0970-03000.pdf>
- [21] "2023 Computer Science Standards\_0.pdf." Accessed: Apr. 22, 2024. [Online]. Available: <https://oklahoma.gov/content/dam/ok/en/osde/documents/services/literacy-policy-and-programs/oklahoma-academic-standards/2023-OAS-Computer-Science-Standards.pdf>
- [22] T. R. Kelley and J. G. Knowles, "A conceptual framework for integrated STEM education," *IJ STEM Ed*, vol. 3, no. 1, Art. no. 1, Dec. 2016, doi: 10.1186/s40594-016-0046-z.
- [23] P. W. Jackson, *Life in classrooms*. New York: Holt, Rinehart and Winston, 1968.
- [24] G. Biesta, "Good Education in an Age of Measurement: On the Need to Reconnect with the Question of Purpose in Education," *Educational Assessment, Evaluation and Accountability*, vol. 21, no. 1, pp. 33–46, Feb. 2009, doi:10.1007/s11092-008-9064-9. [Online]. Available: <https://link.springer.com/article/10.1007/s11092-008-9064-9> (subscription required). Accessed: Apr. 15, 2025.