CYSE 595 Topics: Entrepreneurship in Cybersecurity

Old Dominion University

Dr. Brian Payne

# A Career Interest Inventory Based on The NICE Cybersecurity Framework

Brad Herron

06/18/2022

## ABSTRACT

"The NICE Framework supports those in the cybersecurity field and those who might wish to enter the cybersecurity field, to explore Tasks within cybersecurity Categories and work roles. It also assists those who support these workers, such as human resource staffing specialists and guidance counselors, to help job seekers and students understand which cybersecurity work roles and which associated Knowledge, Skills, and Abilities are being valued by employers for in demand cybersecurity jobs and positions. These workers are further supported when vacancy announcements and open position descriptions use the NICE Framework's common lexicon to provide clear and consistent descriptions of the cybersecurity tasks and training that are needed for those positions. When training providers and industry certification providers use the common lexicon of the NICE Framework, those in the cybersecurity field, or those who might wish to enter the cybersecurity field, can find training and/or certification providers that can teach the tasks necessary to secure a cybersecurity job or to progress into new positions. Use of the common lexicon helps students and professionals to obtain KSAs that are typically demonstrated by a person whose cybersecurity position includes a given work role. This understanding helps them to find academic programs that include learning outcomes and knowledge units that map to the KSAs and Tasks that are valued by employers" (Newhouse, Keith, Scribner, and Witte, 2017 ).

The product that is the focus of this assignment is a career inventory based on the knowledge, skills, abilities as outlined in the Nice Framework and likes/dislikes of the individual taking the assessment. This would be very similar to a Strong or Myers-Briggs inventory but based specifically on the field of cybersecurity. However, because of the nature of online students and employment, the idea is really to create a web-based application so that it is paper-free, green, and provides quick automated results.

This product is integral because it addresses the problem of folks looking to enter into the field of cybersecurity by educating them on the various roles in cybersecurity while helping them chart their path, plan their academics, while also saving them time and money. So many folks begin this process of trying to get a job in cybersecurity without knowing the roles. This solution could help alleviate that issue.

There are a lot of folks aiming to get into cybersecurity without knowing what in cybersecurity they might consider pursuing, as there are a host of positions available. This product is a career assessment that helps folks plot a career-path into the cybersecurity field as there are 57 different roles in cybersecurity. This would not recommend industry-neutral certifications or require any kind of membership. It's solely a career assessment to help guide individuals looking to make either a career change into one of the many fields or for students early in their academic career to focus their studies.

In total, the assessment will allow folks to really evaluate their interests and dislikes by answering questions specific to the knowledge, skills, and abilities as outlined in the NICE Cybersecurity Framework. The results of the assessment will aim to provide the participant certain roles within cybersecurity to research. The additional aim is to arm the participant with a clearly defined path to either independently study or plan their academic pursuit that provides them with enough knowledge and baseline skills.

## LITERATURE REVIEW

“A balanced cybersecurity workforce incorporates a basic understanding of technical skills along with other baseline interdisciplinary skills such as understanding and formulating policies, practices, risk management, business standards, frameworks, politics, governance and

much more. These “Interdisciplinary skills” cover different avenues such as Criminology, Human Psychology, Management, Law, Governance, etc. This demands a holistic education in cybersecurity (Jacob, Wei, Sha, Davari, and Yang 2018).

As Jacob et al. (2018) indicated in the preceding paragraph, it is critical for learners to have a basic level understanding of the concepts of different areas of academics which aren’t simply computer science-type courses in nature. Now, more than ever, businesses need and have a desire to have a cybersecurity workforce that is multi-dimensional in different business-related areas. Therefore, it is important for learners to cast a wide enough net, academically, to be a well-rounded applicant when they are ready to join the applicant pool. Furthermore, it is also advantageous for institutes of higher learning to incorporate other elements in their cybersecurity courses to help students become a more well-rounded applicant in the job market. This multidimensional approach all but ensures students have exposure in business-like settings before entering into the job market.

These interdisciplinary skills are important to ensuring a well-rounded talent pool within the cybersecurity sector. Being able to identify, through an assessment, a propensity for such knowledge, skills, and abilities would go a long way in the learner procuring such employment upon completion of their studies.

It is also imperative that the assessment provides an “integrated, conceptual framework for examining the relationships between cross-cultural issues in personality and career assessment. Along with these two issues of the cultural-general and the cultural-specific, it is equally important to acknowledge the cultural contextual issues in personality and career assessment as well as the personality-culture nexus” (Marsella and Leong, 1995). That is, in the creation of such an assessment, and within the confines of the assessment questionnaire

framework, cross-cultural issues should be taken into consideration into the crafting of questions based on the knowledge, skills, and abilities. This might prove to be a rigid requirement based on the specific terms for the knowledge, skills, and abiliites in the NICE framework, but should be a key consideration as pointed out by Marsella et al. (1995).

Crafting such language within the assessment will improve the assessment process for the learner (who will no doubt come from various backgrounds, genders, identities, and cultures) and provide a much more engaging experience. This, too, will aim to provide the learner with accurate results.

"As part of the initiative, the NICE Cybersecurity Workforce Framework aims to codify cybersecurity talent; define the cybersecurity workforce in common terms; and tie the workforce's various jobs, competencies, and responsibilities into a common architecture" (Paulsen et al., 2012).

"All the combined KSAs formulate competencies, which reveals the performance level of the combined KSAs. The specific actions needed to complete job tasks are directly associated with the KSA's. Therefore, the competency gaps involving additional training will be identified once the KSAs are determined. Besides discovering competency gaps, expressed that the measures determining the level of task performance are none other than the KSA's.

"Different jobs relate to several KSA's in the context of cybersecurity. Specific jobs require a low level of combined KSA's. In contrast, some need a high level of combined KSA's. Moreover, KSA's are not certainly exchangeable between job functions or career fields. Hence, while determining cybersecurity KSAs, an initial set of KSAs for all job functions must be the prime area of concentration" (Alammari, Sohaib, and Younes, (2022).

This is why it is imperative to develop such an assessment based on the KSA's of the NICE Cybersecurity framework. Students, upon entering a technical or cybersecurity focused academic program have a basic grasp on what each position entails and whether they would like what each profession offers as a career. This is one of the purposes of this assessment; being able to answer a series of question related to each position and engaging in an exploration of top-scoring positions under the framework. This would assist the learner in charting off on a career fairly early in their academics, saving them both time and money.

One of the important aspects of the NICE Framework, as outlined in this article is having a commonality in language as it pertains to job functions and roles within the cybersecurity sector. "The NICE Framework has been developed to help provide a reference taxonomy that is, a common language, of the cybersecurity work and of the individuals who carry out that work. The NICE Framework supports the NICE mission to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development" (Petersen, Danielle Santos, Wetzel, Smith, and Witte 2020).

This integration of systems further highlights the absolute need of higher institutions and academics to further align their curriculum to an agreed-upon language as it relates to the NICE framework. This consistency is of paramount importance so that the learner has, from the beginning of their academics to conclusion, an alignment of knowledge, skills, and abilities as described in their course listings. This synchronization of language is also extremely vital for institutions of higher learning in maintaining vitality in their cybersecurity-focused courses and curriculum so as to attract fresh talent into their programs.

"Cybersecurity awareness for students in higher education has been and still is being researched to better understand students' attitude, knowledge, behavior, and other relevant impacting factors Khader,Karam, and Fares (2021)". This article concludes the high importance of necessity related to students in higher education having a baseline knowledge of cybersecurity best practices so that they are better informed of business practices before heading into the job market, making for a robust candidate with a wide-range of abilities and knowledge.

Ghosh and Francia (2021), in their article developed a really good framework that will help to accomplish the aforementioned higher education curriculum requirements. They spoke on the critical importance of such an educational framework from an institutional perspective.

"There is much to do in this domain. A comprehensive list of competencies needs to be developed; this would benefit employers and higher education institutions in terms of effectively assessing skills and competencies at various levels. Higher education institutions need to effectively design assessment tools and techniques with which to measure skills and competencies, and work closely with industry partners to evaluate the effectiveness of those tools and techniques. It is time to ask whether traditional lectures and lab-style delivery of courses are meeting the needs of today's employers and imparting relevant skills and competencies to graduates. Additional future directions for enhancing competency-based learning, particularly in the area of cybersecurity, include the following:

1. develop a dynamic and artificial intelligence-based system that provides an effective learning path that is in line with the learner's abilities;
2. expand the data collection and evaluations of scenario-based learning approaches and identify possible actions for continuous improvement;

3. design and implement digital and verifiable credentials for cybersecurity competency pathways that are industry-endorsed; and
4. enable an effective communication mechanism and collaborative platform wherein industry and academia can actively and constantly communicate to address the competency gaps that evolve due to rapid technological advancement."

The above-cited journal is extremely comprehensive in that it lays bare what should be best practices in academia: that communication between institutes of higher learning and those in the profession of cybersecurity should intentionally have open communication based on technological advances which would aid academia in updating their courses.

"The purposes of the NICE Framework, a competency is a measurable cluster of related Task, Knowledge, or Skill statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job or via apprenticeships), or other learning experiences" (Wetzel, 2021). Such is the importance updating those teaching and instructing in academics. If students are being taught, then they absolutely must be taught using up-to-date technology and best practices.

## OVERVIEW

Determining how this problem and innovation relate to material covered in additional classes taken outside of my major is a difficult question to answer, as my major is strictly in cybersecurity at the graduate level. That is, the entirety of my coursework is cybersecurity-centric. However, if I were to relate this innovation to additional degrees and courses I have

taken, I can sufficiently say that a career assessment is integral to personal growth especially if taken in an academic setting.

One of the major issues I have faced, academically, is knowing how I wanted to tailor my academics to a specific career. Having an assessment that deals exclusively with jobs that fall under the broad heading of 'cybersecurity' would certainly help a student just as an assessment to research different types of counseling might assist someone looking to be a counselor. That is, the belief of this author is that being able to pin-point and research different types of careers, rather than using a broad term for a career, is extremely beneficial. As it stands, researching roles requires a learner to either survey the CISA website or cross-reference NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, (Newhouse, Keith, Scribner, and Witte, 2017 ), which has categories and jobs listed in the below fashion:

**Table 2 - NICE Framework Specialty Areas**

| Categories | Specialty Areas | Specialty Area Descriptions |
|---|---|---|
| Securely Provision (SP) | Risk Management (RSK) | Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. |
| | Software Development (DEV) | Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices. |
| | Systems Architecture (ARC) | Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes. |
| | Technology R&D (TRD) | Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility. |
| | Systems Requirements Planning (SRP) | Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs. |
| | Test and Evaluation (TST) | Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT. |
| | Systems Development (SYS) | Works on the development phases of the systems development life cycle. |
| Operate and Maintain (OM) | Data Administration (DTA) | Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data. |
| | Knowledge Management (KMG) | Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content. |

Cross-referencing in such a way is a mediocre way to research jobs and, to this author, seems to be what should be a later phase of job research. It is the opinion of this author that a skills-based assessment should lead the researcher to the aforementioned website and publication. The publication and website should not lead the learner to explore academic options. Academic options should be tailored in such a way that it provides the knowledge, skills, and abilities to the learner upon graduation.

## DETERMINING EFFICACY

To determine efficacy of the assessment, a follow-up questionnaire will be provided to the assessment-taker that asks them to provide their input on the skills-based assessment. This questionnaire will ask the following questions:

1. Did you find the skills-based assessment to be worth your time?
2. Did the quantity of questions seem too little, too much, or about right?
3. Did you understand the purpose of the skills-based assessment?
4. Did you learn about other positions within the realm of cybersecurity you didn't otherwise know about?
5. Did you agree with the positions provided to you based on your assessment?
6. If you disagreed with the positions provided, why did you disagree?
7. If you agreed with the positions provided, will you be further researching those jobs that closely aligns with your skills-based assessment results?
8. What would you change about this assessment?

9. Would you recommend this assessment to others within your professional/academic network?
10. Overall, what did you dislike most about this assessment?

The reasoning for the above-listed questionnaire is to determine whether the assessment-taker is pleased with the assessment and results and whether they would make any improvements, and whether they would be willing to share it and recommend the assessment with their network. The sharing bit is important for this innovation because it shows whether the recipient has confidence that they just engaged with a quality product. If they took it and were receptive to the results, but unwilling to share it with their professional/academic network, then the product would need to be fine-tuned further so as to warrant confidence in the consumer. Consumer confidence in this innovation is critical towards the overall success of this assessment.

## WHAT IS NEEDED TO TURN INNOVATION INTO REALITY?

In order to turn this specific innovation into a reality there are a few things that will be required, as specified in this section.

The project requires interest, first and foremost. If there is no interest or publicity to generate interest, then all the technology to capture that interest means nothing. Having a social media presence is integral with plenty of time to gather interest. The plan would include 3 months of heavy social media posting and interest gathering before making the assessment public.

There is also the need to have a well drafted assessment aligning with the NICE Cybersecurity Workforce Framework with specific attention paid to the listed knowledge, skills, and abilities. Once this has been drafted, results from the assessment must be provided that

aligns the unique knowledge, skills, and abilities to specific jobs under the cybersecurity profession for the individual to further research. From there, a separate questionnaire will be provided no longer than 12 questions in duration, asking the assessment-taker their opinion on the quality of the skills-assessment.

In synopsis, what is genuinely needed is a website that houses an assessment that links to the various careers as outlined on the NICE Cybersecurity Framework website, along with strong interest from the community.

## WHAT'S NEXT?

What comes next is a further refinement of the assessment. This will be a multi-faceted approach by linking the knowledge, skills, and abilities in the questionnaire to the knowledge, skills, and abilities in the NICE framework. A sample of the assessment is as follows, which was taken directly from the NICE Cybersecurity Workforce Framework and based on the knowledge skills and abilities for a Cyber Policy and Strategic Planner (OV-SPP-002):

Instructions: Please place a 'yes' or a 'no' next to each item below and whether they are of any professional or academic interest to you. If you do not know whether it is, please leave the item blank.

### Abilities:

1. A0003: Ability to determine the validity of technology trend data.
2. A0033: Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.

3. A0037**:** Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.

**Knowledge:**

4. K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.
5. K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
6. K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
7. K0004: Knowledge of cybersecurity and privacy principles.
8. K0005: Knowledge of cyber threats and vulnerabilities.
9. K0006: Knowledge of specific operational impacts of cybersecurity lapses.
10. K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
11. K0127: Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).
12. K0146: Knowledge of the organization's core business/mission processes.

13. K0168: Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
14. K0234: Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).
15. K0248: Knowledge of strategic theory and practice.
16. K0309: Knowledge of emerging technologies that have potential for exploitation.
17. K0311: Knowledge of industry indicators useful for identifying technology trends.
18. K0313: Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).
19. K0335: Knowledge of current and emerging cyber technologies.
20. K0624: Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list)

**Skills:**

21. S0176: Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.
22. S0250: Skill in preparing plans and related correspondence.

**Tasks:**

23. T0074: Develop policy, programs, and guidelines for implementation.
24. T0094: Establish and maintain communication channels with stakeholders.

25. T0222: Review existing and proposed policies with stakeholders.
26. T0226: Serve on agency and interagency policy boards.
27. T0341: Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.
28. T0369: Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.
29. T0384: Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.
30. T0390: Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.
31. T0408: Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.
32. T0425: Analyze organizational cyber policy.
33. T0429: Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.
34. T0441: Define and integrate current and future mission environments.
35. T0445: Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.
36. T0472: Draft, staff, and publish cyber policy.
37. T0505: Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.

38. T0506: Seek consensus on proposed policy changes from stakeholders.
39. T0529: Provide policy guidance to cyber management, staff, and users.
40. T0533: Review, conduct, or participate in audits of cyber programs and projects.
41. T0537: Support the CIO in the formulation of cyber-related policies.

## CONCLUSION

There is still a considerable amount of work to do in order to perfect the assessment, and a ton of mapping to do to the various KSA's within the NICE Cybersecurity Workforce Framework. However, throughout the included journal articles, it has been made abundantly clear that the need for such an assessment is needed in within academia and those that wish to enter into the cybersecurity sector. Knowing where to begin is a huge first step that should be walked over methodically with as much though and introspection as possible. Cybersecurity is a very diverse field, filled with folks that range in technically capable coders up to auditors specializing in governance, risk, and compliance (who do not know how to code). The one thing these occupations have in common is that their respective employer is a business of some sort that is attempting to shore up their defenses or the cybersecurity posture of their clients. Cybersecurity is a business decision and not making such a business decision could have a disastrous impact on not only businesses, but on the folks that are employed by the business.

Let's take, for instance, a company named Global Payments Inc., that was hit with a data incident in 2012. Simply focusing on the number of executives that left the company post-incident is quite staggering. The inference made is that the incident had large scale ramifications on key leadership, though it isn't outwardly spoken through SEC filings. Essentially, seven key members of board leadership resigned or moved to different positions within the company in the span of two years post-incident. That kind of turnover, plausibly, could have been offset by

employing individuals that crafted their career in cybersecurity earlier in the process. That guarantee cannot obviously be made, but it's not out of the question to infer that had folks that had the KSA's in place within their IT department that the incident would have stopped before costing the company key leadership and untold amounts of monetary damages.

That is the purpose of this assessment: to align students with careers that they would work to obtain knowledge of before applying for their first job, and to supply businesses with much needed cyber talent which is much-needed. According to The Cyentia Institute (2020), the top one hundred cyber incidents from 2015-2020 totaled "$18 billion in reported losses and 10 billion compromised records." That is an incredibly staggering amount that could have been offset by a better talent pool. Though there are a lot of folks waiting to procure such a position, there are currently close to 500,000 vacant cybersecurity roles that are vacant throughout the United States (CBS News, 2021) with as many as 3.5 million positions being available in 2025 according to Cybercrime Magazine (2018).

## REFERENCES


Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Computer Science, https://doi.org/10.7717/peerj-cs.827

"U.S. Has Almost 500,000 Job Openings in Cybersecurity." Accessed June 20, 2022. https://www.cbsnews.com/news/cybersecurity-job-openings-united-states/.

Cybercrime Magazine. "Cybersecurity Jobs Report: 3.5 Million Openings In 2025," February 23, 2018. https://cybersecurityventures.com/jobs/.

The Cyentia Institute. "IRIS 20/20 Xtreme" 2020

Ghosh, T., & Francia III, G. (2021). Assessing Competencies Using Scenario-Based Learning in Cybersecurity. Journal of Cybersecurity and Privacy, 1(4), 539. https://doi.org/10.3390/jcp1040027

Jacob, J., Wei, W., Sha, K., Davari, S., & Yang, T. A. (2018). *Is The Nice Cybersecurity Workforce Framework (ncwf) Effective For A Workforce Comprised Of Interdisciplinary Majors*? The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. Information, 12(10), 417. https://doi.org/10.3390/info12100417

Marsella, Anthony J., and Frederick T. L. Leong. "Cross-Cultural Issues in Personality and Career Assessment." *Journal of Career Assessment* 3, no. 2 (March 1, 1995): 202–18. https://doi.org/10.1177/106907279500300207.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. https://doi.org/10.6028/nist.sp.800-181

Paulsen, Celia, Ernest McDuffie, William Newhouse, and Patricia Toth. “NICE: Creating a Cybersecurity Workforce and Aware Public.” *IEEE Security & Privacy* 10, no. 3 (May 2012): 76–79. https://doi.org/10.1109/MSP.2012.73.

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, and Greg Witte. “Workforce Framework for Cybersecurity (NICE Framework),” November 15, 2020. https://www.nist.gov/publications/workforce-framework-cybersecurity-nice-framework.

Wetzel, Karen. “NICE Framework Competencies: Assessing Learners for Cybersecurity Work (2nd Draft).” National Institute of Standards and Technology, December 15, 2021. https://doi.org/10.6028/NIST.IR.8355-draft2.

## SELF-REFLECTION

To the Director of the Old Dominion University Advanced Technology Center,

The work provided above provides many reasons why an assessment for those pursuing academics in the cybersecurity profession is integral towards their academic and professional development but also why it makes a good business decision in the long run. Technology, cyber-criminals, and bad actors and now moving faster than our workforce can move. Time is unfortunately not on the side of the business. We have to, as a community, provide the necessary tools to those seeking to gain entrance into this new battlefield and, to begin that journey, one must sufficiently plan out their first steps and I believe this assessment that maps to the NICE Cybersecurity Workforce Framework is a step in the right direction.

From a business standpoint alone, it is a worthwhile endeavor so as to help alleviate the burden of students in discovering their true passion within the field of cybersecurity which encompasses well over fifty different positions that fall under seven different categories. Those categories as taken from the NIST Special Publication 800-181 (National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework) is as follows:

1. Securely Provision;
2. Operate and Maintain;
3. Oversee and Govern;
4. Protect and Defend;
5. Analyze;
6. Collect and Operate;
7. Investigate.

I won't dive into each job under each category, but suffice it to say that knowing where one wants to end up professionally requires an in-depth analysis of what each profession requires via knowledge, skills, and abilities upfront. This is where this cybersecurity skills assessment is an

important tool for learners that have career aspirations of entering into the cyber workforce.

Should you have any questions pertaining to this project, please do not hesitate to contact me.

Thank you, again, for your consideration.

Sincerely,

Brad Herron