Dr. Stephen R. Orr IV is currently the National Security Agency (NSA) visiting Professor for Cyber Security Studies at the United States Naval Academy. He holds a Ph.D., M.S., and B.S. degree in Computational and Information Sciences. Dr. Orr has held analytical, technical, operational, and leadership positions at both Headquarters and the field. His expertise and career has focused on offensive and defensive cyberspace operations. Most recently, Dr. Orr was part of a team that won NSA's prestigious Deckert/Foster Award for Excellence in SIGINT engineering.

Dr. Orr's most recent assignment was the Executive Director of J3, Operations for United States Cyber Command. In this capacity he was responsible for directing command operations spanning from future planning, through operations execution within the authorized computer network operations mission space.

Dr. Orr's research interests include the intersection of cybersecurity and human factors, cyber effects, and the application of emerging technologies.

This proposal attempts to address the challenge of what a follow on Scholarship for Service (SFS) could look like in the twenty years since it was first established, while addressing multiple general topic areas to cybersecurity education. It is through this proposed academic construct that private and public sector challenges could be addressed. Simply put, it is proposed that we evolve the **centers of academic excellence construct to focus on the "*at least three dozen specializations*" that exist in the cybersecurity discipline**. Diversifying the expertise at any one academic center of excellence has the ability to produce many students that are average at everything, and good at nothing. By restructuring the fundamental institutional model, these centers of academic excellence **and specialization** would create a monopoly on **producing expertise** in one of the many subdisciplines of cybersecurity. In turn, students would graduate with the broad liberal arts education that inspires creativity and critical thinking, complemented with specialized skills to meet the private and public sector cybersecurity challenges. Furthermore, this institutional construct provides a gateway for solving the more general topic areas of cybersecurity education.

The National Security Agency (NSA) originally created the Center for Academic Excellence in Information Assurance Education (CAE-IAE) in 1998, with the Department of Homeland Security (DHS) joining as a partner in 2004. Since that time te CAE in IA Research component was added in 2008 to encourage universities and students to pursue higher-level doctoral research in cybersecurity. Later, the CAE-Cyber Operations program was established, which focuses on technologies and techniques related to collection, exploitation, and response. This construct has, and continues to pay dividends to enhance the national security posture of our Nation. **The specialization designator allows academia to take the lead by voluntarily constructing a monopoly on specialized cybersecurity education**. This evolution would further enhance the NSA and DHS sponsored Centers of Academic Excellence, while also "future-proofing" the education we provide.

To be clear, it is not proposed that these institutions would **only teach** any one of the subdisciplines of cybersecurity. Nor that there would be only once academic institution to focus on any one specialization. **Specialization requires a solid foundation and core competencies**. For example, a fundamental understanding of computational and information concepts such as programming, operating systems, and networking; policy, legal, and ethics would be necessary. Each of the documented specializations would further focus on these particular areas allowing the academic center of excellence to be designated as producing graduates with a particular specialty. However, given this is a dynamic field it is guaranteed that the specialization requirements of tomorrow will not be the same as the specialization requirements of today. This proposal allows for academic institutions to adapt to meet the specialized requirements without significantly disrupting their entire academic program, as the fundamental core competencies will remain the same. Collectively, academia would meet the demands of private and public institutions today, while having the ability to adapt and change to the dynamic needs of the future. **Thus, “future-proofing” the academic education through specialization is achieved by adapting to the cybersecurity challenges of today and tomorrow, while providing a core foundation in computation and information science concepts**.

The proposed academic centers of excellence and specialization **creates a natural opportunity to partner with cybersecurity vendor-neutral training and certification providers, or supplanting them by meeting the needs of the market they currently fill**. Vendor-neutral certifications typically validate a candidate’s unbiased knowledge or skills of a particular technology principles. This is done through traditional tests and hands-on, skill-based scenarios. The specialization designator lends itself to providing more specific, short-term knowledge and skills to meet the demands of today. This specialization, combined with a traditional broad understanding of computational and information sciences provides a win-win-win scenario for the student, academia, and industry. An academic institution that currently offers a version of this proposal is the University of Maryland University College (UMUC). They offer technical programs that combine broad understanding of fundamental computation sciences with cybersecurity training and certification to meet industry demands. Creating academic centers of excellence and **specialization** could build and improve upon this model while increasing value of a college education. **Specialization through academic centers of excellence creates centers of gravity to address the mix of education methods, industry practice, and government needs**.