As I sat down to write this statement, news of the Marriott data breach was just breaking. More than 500 million people had just their identifying information, passport ids, and credit card numbers stolen. I find these cases frustrating because I helped to develop technology specifically to stop these types of breaches: a combined deception, data tracking, and anomaly detection system that could have identified the Marriott breach years earlier, if not prevented it entirely. For me, conducting research is not only a matter of intellectual interest – it is also an opportunity to develop new ideas and technologies, like a breach detection system, that can have a positive impact. I am pursuing a PhD in Security and the NDSEG Fellowship because I want to continue conducting research in security and machine learning and eventually become a professor in these fields.

I became interested in a career in research as an undergraduate at Swarthmore College, and later became interested in security when I joined Allure Security Technology and started working on breach detection. As a sophomore, I won a fellowship to study low power wireless sensor networks with Swarthmore Professor Eric Cheever. I enjoyed the experience and pursued further research opportunities, working with a scientist at Woods Hole Oceanographic Research Institute to publish a paper on burst sampling current measurements, and conducting experiments in multi-task learning reinforcement learning at the Emergent A.I. laboratory at Bryn Mawr. After I joined Allure Security, I found applying machine learning techniques to develop a breach detection system to be an exciting challenge, and the increasing frequency of high profile data breaches lent my work added urgency.

I decided to pursue my interest in security and machine learning in a research setting, so I started a Masters at Columbia University and joined the Intrusion Detection Lab under Professor Salvatore Stolfo. Working with Professor Stolfo, I developed simulated user bots for testing insider threat detection systems that model user behavior. To test them, I modeled several intrusion detection systems using anomaly detection algorithms such as single class SVMs and Probabilistic Graphical Models, and demonstrated that the SUBs could be programmed to trigger alerts by performing abnormal behaviors. To generate realistic behavior, I developed a new method, applying a multi-task learning approach to jointly modeling event sequences and timing with Recurrent Neural Networks, and published my results with two other students (who worked on other aspects of the project) in IEEE SPW.

Now, as a PhD candidate at Columbia University, I am working with Professor Suman Jana on dynamic program gradient analysis for vulnerability detection—a research direction that has practical applications in addition making fundamental contributions. My extensive research experience, coursework in machine learning and security, and background as a professional software engineer make me exceptionally qualified to pursue this research. The NDSEG Fellowship will help me to become a professional researcher and professor, and continue giving back through my applied research, teaching, and mentorship of future engineers and scientists.