House Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection Hearing:
"Challenges of Recruiting and Retaining a Cybersecurity Workforce"
2pm, September 7, 2017

Prepared Statement for Record
Dr. Michael Papay
Vice- President, Cybersecurity Initiatives &
Chief Information Security Officer
Northrop Grumman

Thank you Chairman Ratcliffe, Ranking Member Richmond and Members of the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection for holding today's hearing on the critical topics of attracting, retaining, educating and training our nation's cyber workforce. As our government, military and society overall become increasingly dependent upon digital technology, it is a national AND economic security imperative to ensure that we have the cyber trained workforce to meet this demand.

My name is Dr. Michael Papay and I am Vice President of Cyber Initiatives and Chief Information Security Officer (CISO) for Northrop Grumman, a leading cyber provider across the federal government and producer of innovative solutions from autonomous systems to strike platforms to space products. Given the often sensitive and critical national security nature of our work; it is absolutely essential for resilient cybersecurity to be a key component to all that we do. From original code, to hardware, to uninterrupted mission performance while enduring cyber threats, our customers trust us to deliver systems that enable them to confidently execute the mission in any environment, including cyber space. We are proud of our strong reputation earned through 70 years of integrity, innovation, dedication to the customer, and a proven track record of performance. As important as technology is, at Northrop Grumman we firmly believe that our employees are the single most important aspect of cybersecurity. Therefore, we have made it a top priority to not only support the development of a larger cyber qualified workforce globally but also to increase its diversity.

Thank you again for having me here today and I hope that my testimony is useful. I look forward to your questions.

Attracting and Retaining Employees

Northrop Grumman is at the forefront of cyber research, development and technology, and it is our people that make this possible. While Northrop Grumman, like the DHS and the federal government, must continue to work to overcome a perception hurdle for cyber talent—we can offer prospective employees something unique—the opportunity to do really exciting, cutting edge work that is vital to our national security. For many cyber professionals (and employees across Northrop Grumman and the federal government) it is this sense of mission that drives them.

As part of our effort to ensure that our cyber employees are continually challenged and provided opportunities for growth, we move them around inside the company from customer to customer, tough problem to tough problem. We utilize rotational programs that expose and train our cyber workforce in defending our network, enabling our customers' missions, and supporting full spectrum cyber operations. We work with employees to help them create their own growth along the cyber career path, give them the time to take the training necessary to maintain their certifications, and keep their knowledge and skills fresh. We even offer educational assistance in some instances.

To provide our employees, customers and even policymakers with the macro understanding and technical skills cyber often requires, Northrop Grumman created its own, in- house "Cyber Academy". We also utilize a matrix model for customer mission support and employee development – allowing us to hire for critical skills and redeploy our talent across programs. We are committed to providing positions that work best for our employees by allowing flexible work schedules and opening up work locations in customer-approved non-traditional cyber hubs throughout the country to broaden our talent pool.

At Northrop Grumman, we are focused on attracting all those who are interested and qualify through a sense of mission, passion for solving complex challenges and desire to work on cutting edge technologies that they are unable to do anywhere else in the world.

Partnering with the Federal Government and DHS Cyber Training

In 2012, I had the privilege of participating in the Homeland Security Advisory Council Task Force on CyberSkills, an initiative that was launched to help develop a national security workforce as well as enable DHS to recruit and retain its own cyber talent. I applaud DHS for adopting many of the Task Force's recommendations. At Northrop Grumman, I am pleased to note that we have incorporated the majority of these recommendations as part of our internal cyber workforce strategy. Members of my team also participated in the DHS Cyber Education and Workforce Development Working Group and then the NIST National Initiative for Cybersecurity Education (NICE). Northrop Grumman representatives are members of both the Collegiate Working Group and the K-12 Working Group. Our engagement brings industry perspective in full collaboration with government and academia. We also contribute to the NIST NICE Workforce 2.0 model which creates a framework for professionalization of the cyber career.

Partnering with our federal government customers on cyber workforce education and training is critical to supporting a national security mission and our mutual success. One of the key findings of the CyberSkills Task Force was the need to provide more cyber training to DHS employees and I am pleased that Northrop Grumman has helped support this initiative. Starting in 2014, as part of our National Cybersecurity & Communications Integration Center (NCCIC) contract, we began using 39 cyber training courses to help DHS employees increase their efficiency and improve retention. Our training program heavily leveraged our internal Northrop Grumman Cyber Academy for a large portion of the course content and developed a three level competency model. Hundreds of DHS employees received targeted training ranging from how to review cyber threat analysis reports to effectively coordinating with partners. Northrop Grumman cyber practitioners provided advice and guidance on national-level cyber security policy as well as implementation and support of new or existing technical solutions to enhance the mission. These training plans aligned to Cyber Skills and Cyber Pay initiatives, with incentives tied to requisitions and future hirings.

Northrop Grumman Cyber Workforce Development

Growing a cyber workforce from the ground up begins with inspiring youth to pursue this field. At Northrop Grumman and for our customers, in working to build a cyber workforce, we look at the continuum of education – from elementary school through the professional ranks – and are collaborating with academia and organizations worldwide to help address this issue and build a diverse, highly skilled workforce.

For more than seven years – Northrop Grumman has partnered with the Air Force Association to present the CyberPatriot National Youth Cyber Education Program. CyberPatriot is one of our most successful and impactful initiatives and features the wildly popular annual cyber defense competition. It started in 2009 with eight teams and I'm proud to say over 4,400 teams participated this past year from all 50 states, Canada, and Department of Defense Dependent Schools in the Pacific and Europe. Given the fact that teams average about five students, we are reaching tens of thousands of youth each year who are learning how to harden and protect computers and networks. A full 87 percent of CyberPatriot participants go on to pursue STEM degrees in college. In addition to deep technical skills, the students, through the program structure, their mentors and hands-on experience, also develop their talents in cyber ethics, collaboration, communication and leadership – all life skills that enhance their career readiness. Northrop Grumman has awarded more than $350,000 in scholarships to winning teams. Like others in industry and government, the company has employed these high school students as paid summer interns, more than 300 to date, working side by side with our cyber professionals. Many of these interns have stayed with Northrop Grumman, returning summer after summer for paid internships through high school and then college. While most STEM programs report a female participation rate around 12 percent, I am especially proud that CyberPatriot boasts 23 percent female participation! None of this could be accomplished without the academic partner of the program, the University of Texas San Antonio's Center for Infrastructure Assurance and Security. To that end, we have found that you cannot only focus on higher education or at the high school level. In many cases, students have already decided upon their desired field by the 5th or 6th grade. Therefore, the earlier you can expose students to STEM topics in an engaging and exciting way as we do with the CyberPatriot Elementary School Cyber Education Initiative, the greater likelihood they will pursue a STEM path.

University Partnerships

Northrop Grumman is actively engaged with universities across the country to provide an industry perspective on cyber curriculum and degree programs to prepare students for real world challenges. We helped launch the nation's first cyber honors program at the University of Maryland College-Park called ACES, the Advanced Cybersecurity Experience for Students. ACES is a living learning community for exceptional students from a variety of majors to enhance their cyber studies. We've also assisted in creating the nation's first undergraduate Cybersecurity Engineering degree at George Mason University in Fairfax, Virginia. Further, at the University of Maryland- Baltimore County (UMBC), we are providing grants to students from diverse academic and socio-economic backgrounds to pursue cybersecurity education. At great schools ranging from Cal Poly Pomona to the University of Cincinnati and dozens of others across the country our employees are actively engaged in helping to develop curriculum, fund hands-on student projects and educate future cyber professionals.

Diversity

Because cyber is such a complicated and dynamic challenge, we need a workforce that brings with it diversity of thought, culture, education, experience and problem solving – diversity drives innovation and breeds success. Diversity is truly a strategic asset. Working with university and professional organizations that cater to diverse populations is a great way to attract cyber employees and build a stronger, ethnically and racially diverse workforce. We partner with the Society of Hispanic Professional Engineers, Women in Technology, Women in Cyber Security, and Society of Women Engineers to name just a few organizations. We need to ensure that young girls, minorities and other underrepresented populations recognize that they are welcome and can succeed in the cyber workforce. This past year working with a small, disadvantaged business located in Baltimore, Maryland we developed the Cyber Warrior Diversity Program at Morgan State University and Coppin State University, two Historically Black Colleges and Universities (HBCU). This training is designed to prepare individuals to defend information systems and networks by training, testing and providing certifications in accordance with the DoD Information Assurance Workforce Improvement Program. Additionally, the Northrop Grumman Foundation is funding a three-year, $2 million program with the National Society of

Black Engineer's (NSBE) designed to expand the nation's engineering workforce through a partnership with Historically Black Colleges and Universities (HBCUs). The Northrop Grumman Corporation/NSBE Integrated Pipeline Program will provide 72 engineering students with $8,000 scholarship grants, internships with Northrop Grumman and year-round academic and professional development support. The program's three HBCU partners - Florida A&M University, Howard University and North Carolina A&T State University - will receive grants, technical assistance and a package of programs researched and managed by NSBE.

Expanding the diversity of the cyber workforce is critical to not only ensuring that we have a sufficient number of cyber professionals but also the range of perspectives and backgrounds necessary to counter a constantly evolving threat.

Breaking Barriers

I am honored to be here today representing Northrop Grumman and proud of our company's efforts to help develop a robust pipeline of innovative thinkers, engineers and passionate professionals who will secure our nation's cyber future. A few final thoughts to leave the committee with:

- Clearances: Beyond just a shortage of cyber professionals, there is also a lack of cleared cyber professionals. We need to figure out ways to improve the clearance process to ensure that both the federal government and contractors have the cleared employees to do all the critical national security work that is required.

- More Cyber Trained Federal Employees: Cyber training across the federal government is inconsistent. The federal governments as a whole needs to put a greater emphasis on ensuring its employees have the cyber understanding and tools to effectively and securely do their jobs.

- Increased Partnerships and Coordination: There is no single answer to addressing the shortage of cyber workers. Continuing to work across academia, government and industry is essential to leveraging investments, best practices and collectively

working together to ensure that our great nation continues to securely grow and prosper in this increasingly digital age.

I would be happy to answer any questions and Northrop Grumman looks forward to working with the Committee on this effort.

Thank you again.