House Energy & Commerce Committee Hearing:
Cyber Threats and Security Solutions
10:00 am, May 21, 2013

One page Overview of Dr. Mike Papay's Statement:

Northrop Grumman is one of the leading cybersecurity providers to the federal government and has expansive and in-depth knowledge, experience and expertise in these critical aspects of our nation's technology framework. We build, supply, and manage cyber solutions for customers that include the Department of Defense, intelligence community, civilian agencies, international governments, state and local government and the private sector. Northrop Grumman is honored to be trusted with the challenge of protecting some of the world's most targeted systems.

The Defense Industrial Base's information sharing program has demonstrated the benefits of industry-government collaboration. Northrop Grumman was a founding member of this groundbreaking framework. While this effort has demonstrated that public/private information sharing can yield many successes, we also learned that some of the toughest challenges are not technological but cultural and legal. Northrop Grumman was proud to announce last week that it will participate in the next generation government- private sector information sharing program, DHS' Enhanced Cybersecurity Services (ECS) program.

Given our experience, Northrop Grumman very much appreciates the seriousness and urgency of the cyber threat. We do believe that the President's Executive Order (EO) is an important step in the right direction. The EO's ultimate success will be determined by the effectiveness of the individual agencies' efforts in implementing their assigned responsibilities. We appreciate the government's ongoing outreach to industry and we recently actively engaged with NIST to support the development of its Cybersecurity Framework. However, the EO alone cannot address the full range of cybersecurity issues. Legislation is still required to facilitate and encourage companies to secure their own networks and break down the barriers to sharing cyber threat information.

We applaud the House of Representatives recent passage of cybersecurity legislation, especially the strong bipartisan vote in favor of the Cyber Intelligence Sharing Protection Act, which we hope will build momentum towards bills passing both chambers.

Northrop Grumman is committed to utilizing our experience to support the development of successful cyber policies. We encourage legislation that improves the agility of the federal acquisition process to address rapidly evolving cyber threats, increases investments in cybersecurity technology and training of our current workforce, and supports the development of the next generation of scientists and engineers. We must be mindful, however, that our nation's cybersecurity cannot be fixed with one law or policy change. Effective cybersecurity policies should be risk- based and as adaptable as the threat itself. These cyber efforts must also carefully balance civil liberties and greater security. These are not mutually exclusive goals. Indeed, if we do not strengthen our cyber defenses, we imperil the civil liberties that we hold dear.

House Energy & Commerce Committee Hearing:
"Cyber Threats and Security Solutions"
10:00 am, May 21, 2013

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

Chairman Upton, Ranking Member Waxman and other members of the committee, Northrop Grumman appreciates the opportunity to discuss this critically important topic with you. My name is Mike Papay and I am the Chief Information Security Officer and Vice President for Cyber Initiatives at Northrop Grumman. In this capacity I am responsible for both Northrop Grumman's internal network security and I lead the company's cyber strategy development.

Secretary Janet Napolitano recently stated in a joint hearing before the Senate Committee on Commerce, Science, and Transportation and Senate Committee on Homeland Security and Governmental Affairs, quote, "We know that our adversaries are seeking to sabotage our power grid, our financial institutions, and our air traffic control systems. These intrusions and attacks are coming all the time and they are coming from different sources and take different forms, all the while increasing in seriousness and sophistication," unquote. I would add that emerging cyber threats also are targeting many of our nation's corporations, including small businesses, and individuals.

Exploitable vulnerabilities in our information infrastructure pose one of the most significant threats to our national and economic security facing us today – perhaps the most significant threat. The age in which we live is built on digitized information. Everything we do, the way we learn, the way we communicate depends on and produces digitized information. Digitized information governs the

medical care we receive, the security of our bank accounts, the quality of the water we drink and the food we eat, our ability to communicate with one another, and our access to the energy to heat our homes in the winter, keep them cool in the summer and power our way of life. As we become increasingly dependent on computers and digital technology, the quality of our lives improves. At the same time, we also become more vulnerable to threats to that technology, cyber attacks. If we hope to maintain our freedom, our security and our standards of living in this age, we must enhance and strengthen our cyber defenses.

Broadly defined, cybersecurity refers to the protection of our digitized assets from exploitation and attack on networks, systems, information, physical infrastructure, users and their privacy. Northrop Grumman is one of the leading cybersecurity providers to the federal government and has expansive and in-depth knowledge, experience and expertise in these critical aspects of our nation's technology framework. We build, supply, and manage cyber solutions for customers that include the Department of Defense, intelligence community, civilian agencies, international governments, state and local government and the private sector. Northrop Grumman is honored to be trusted with the challenge of protecting some of the world's most targeted systems. We pride ourselves on developing innovative solutions to tackle the toughest cyber challenges. We understand that effective cybersecurity not only means defending computers, networks and data, but also includes enhancing the security of the products we manufacture. From unmanned aircraft to radar systems, we work to make our products less vulnerable to cyber attacks.

Over the past decade, Northrop Grumman has implemented a set of internal cybersecurity controls that we continue to evolve to protect our own and our customers' intellectual property and

sensitive data. Essential elements of our cybersecurity practices include leveraging threat information from multiple sources and deploying cutting edge technologies. We have implemented security standards and architectural approaches, as recommended by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) Community and SANS Critical Security Controls.

We also focus on internal cybersecurity awareness training as part of our internal protection efforts. Northrop Grumman has developed its own internal cybersecurity training and a "Cyber Academy" that provides more in-depth cyber education to our employees and senior leaders. To further heighten cybersecurity awareness, Northrop Grumman conducts internal spear phishing exercises on our employees to enhance awareness.

Given the dynamic nature of cyber threats, it is essential to make the necessary investments to stay ahead of the threat. Northrop Grumman partners with a range of universities and has created the Cybersecurity Research Consortium with MIT, Carnegie Mellon, Purdue and USC to facilitate the development of next- generation cyber solutions. As part of the Consortium, Northrop Grumman sponsors graduate fellowships to research and address the hard problems of our customers. Our goal is to accelerate the pace of innovation in cybersecurity and ensure a talent pipeline of top researchers in this field. In addition to the Cybersecurity Research Consortium, Northrop Grumman has supported the establishment of the CYNC Cyber Incubator at University of Maryland- Baltimore College. The CYNC program sponsors innovative, technology-driven startup companies, addressing critical market needs for companies from across the country looking to further develop and commercialize their technologies.

These investments not only are focused on technological innovation, but also are meant to help build the talent pipeline for the next generation of cybersecurity innovators.

According to a 2010 U.S. Department of Commerce study, the number of science, technology, engineering, and math (STEM) jobs is expected to grow 17% in the next decade. I was privileged to serve on the 2012 Homeland Security Advisory Council's Task Force on CyberSkills. This Council focused on identifying far-reaching improvements that would enable DHS to recruit and retain the cybersecurity talent it needs. One of the council's recommended objectives was to radically expand the pipeline of highly qualified candidates for cyber jobs through innovative partnerships with community colleges, universities, organizers of cyber competitions, and other federal agencies. Northrop Grumman sees this as a critical objective for our company as well, which is why we have sponsored the nation's first ever cybersecurity honors program at the University of Maryland- College Park. We are also focusing our educational efforts on middle and high school students as the founding sponsor of the CyberPatriot program, which this year hosted over 1,200 teams from all 50 states, and DoD schools in Europe and the Pacific.

Due to the complexity and prevalence of cyber threats, no organization can or should face them alone. Industry specific peer-to-peer information sharing is critical because at the end of the day, we are all in this together. Northrop Grumman participates in many other industry venues committed to high levels of cybersecurity, including the Transglobal Secure Collaboration Program (TSCP), Internet Security Alliance, National Security Telecommunications Advisory Committee, and National Infrastructure Advisory Council.

The Department of Defense's Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Program has demonstrated the benefits of industry-government collaboration. Northrop Grumman was a founding member of this groundbreaking framework, first established in 2007. The program had to overcome initial skepticism, even among participants, that industry members and the government could collaborate effectively to address cybersecurity risks. While the program demonstrated that public/private information sharing can yield many successes, we also learned that some of the toughest challenges are not technological but cultural and legal. As we all worked together, we found that sharing cyber threat information empowered us to respond faster, be proactive in defense, and more effectively secure the sensitive information that our Nation entrusts in us.

Northrop Grumman was proud to announce last week that it will participate in the next generation government- private sector information sharing program, the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program. ECS is an information sharing program to assist critical infrastructure owners and operators in enhancing the cybersecurity protections of their information systems from unauthorized access, exploitation and data exfiltration. Under ECS, DHS will share classified and unclassified cyber threat "indicators" with designated Commercial Service Providers, and the Commercial Services Providers will utilize the threat indicators to provide approved cybersecurity services to authorized critical infrastructure entities.

Given our experience, Northrop Grumman very much appreciates the seriousness and urgency of the cyber threat. We do believe that the President's Executive Order (EO) is an important step in the right direction. The EO sets the broad parameters for dealing with cybersecurity. The EO's ultimate success will be determined by the effectiveness of the individual agencies' efforts in implementing their assigned responsibilities. We appreciate the agencies' ongoing outreach to industry with respect to

those activities and we are committed to participating in those efforts. For example, we recently actively engaged with the National Institute of Standards and Technology (NIST) to support the development of its Cybersecurity Framework. Successful cyber strategies will constructively build upon what is currently working and not simply layer on new bureaucracy or requirements that add costs without improving overall cybersecurity. Either way, the EO alone cannot address the full range of cybersecurity issues. Legislation is still required to facilitate and encourage companies to secure their own networks and break down the barriers to sharing cyber threat information.

We applaud the House of Representatives passage of the Cyber Intelligence Sharing and Protection Act, the Federal Information Security Amendments Act, the Cybersecurity Enhancement Act, and the Advancing America's Networking and Information Technology Research and Development Act in the past few weeks. We are optimistic that this package of bills, especially the strong bipartisan vote in favor of the Cyber Intelligence Sharing and Protection Act, will help build momentum towards legislation passing both chambers.

Northrop Grumman strongly supports policies that accomplish the following cybersecurity goals:

- Strengthening critical infrastructure protection;
- Facilitating the two way sharing of threat information across the public and private sectors,
- Ensuring the protection of personal information and proprietary data;
- Requiring autonomous, continuous monitoring and threat assessment to enable the real-time situational awareness of the nation's networks and missions;

- Improving the agility of the federal acquisition process to address rapidly evolving cyber threats;
- Ensuring that the cyber risk of each program or product acquired by the government for critical functions are appropriately considered;
- Increasing investments in cybersecurity technology and training of our current workforce and supporting the development of the next generation of scientists and engineers;
- Ensuring the necessary marketplace incentives to encourage industry leaders to continue raising their levels of cybersecurity;

Northrop Grumman is committed to utilizing our experience to support the development of successful cyber policies. We must be mindful, however, that our nation's cybersecurity cannot be fixed with one law or policy change. Effective cybersecurity policies should be risk-based and as adaptable as the threat itself. These cyber efforts must also carefully balance civil liberties and greater security. These are not mutually exclusive goals. Indeed, if we do not strengthen our cyber defenses, we imperil the civil liberties that we hold dear.

Please consider Northrop Grumman a resource. We look forward to working with Members of Congress on both sides of the aisle and the administration to make our world safer and more secure.

Thank You. I would be happy to answer any questions that you may have.