United States Senate Committee on Energy and Natural Resources
Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry

February 14, 2019

Testimony of Major William J. Keber
Executive Officer, West Virginia National Guard's Critical Infrastructure Protection Battalion

Good morning, Chairman Murkowski, Ranking Member Manchin, and members of the Committee on Energy and Natural Resources, thank you for the invitation and opportunity to participate in today's hearing on the Status and Outlook for Cybersecurity Efforts in the Energy Industry.

My name is Major William Keber, and I am the Executive Officer for the West Virginia National Guard's Critical Infrastructure Protection (CIP) Battalion. Our organization is a distinctive one that conducts assessments and training to improve the security and operation of our nation's critical infrastructure. Our unit started in 2005 when Major General James A. Hoyer, then a Lieutenant Colonel, presented a concept to West Virginia National Guard leadership proposing assessment activities to support homeland defense. Over the past fourteen years we have conducted infrastructure protection assessments and training events for the Department of Energy, Department of Transportation, the Defense Industrial Base, the Department of Homeland Security, and the Department of Defense. Since inception, our teams have conducted 3,583 assessments and 2,662 training events, educating 59,237 individuals as of January 2019. We have conducted assessments in support of national events such as the State of the Union, Republican and Democratic National Conventions, the National and World Scout Jamborees, Presidential visits, and the Superbowl, just to name a few.

In this testimony I will address three topics. First, I will cover how our organization historically contributed to protecting our nation's infrastructure and assessed cybersecurity. Second, I will describe the current steps we are taking to further enhance cybersecurity assessment practices. Third, I will discuss how we are contributing to workforce development and contributing to the broader defense industry along with other interdependent industries.

I. History of WVNG's Critical Infrastructure Protection Assessments

The West Virginia National Guard's CIP Battalion has a diversified portfolio that currently supports the Department of Homeland Security, Department of the Army, and United States Coast Guard. Additionally, we are in discussions with the Department of the Navy and the Nuclear Regulatory Commission to collaborate on future physical security and cybersecurity projects.

We support DHS's Cybersecurity Infrastructure Security Agency by creating Infrastructure Visualization Platform products, assisting facilities self-assess utilizing DHS's Infrastructure Survey Tool, conducting training for the Office for Bombing Prevention, and assisting its Regional Resiliency Assessment Program by assessing natural gas and petroleum pipelines. We support the U.S. Coast Guard by conducting Port Security and Resiliency Assessments and the Department of the Army by conducting Mission Assurance Assessments and training. Both Coast Guard and Army teams reference DoD Mission Assurance Benchmarks and assess risk with an all threats, all hazards approach.

Our teams have always assessed networks and communications architectures against cybersecurity concepts and principles, but never had the authorities to conduct deep analysis on the network to validate the information given. Assessment team members were relegated to questioning site representatives through interviews and annotating their physical observations. Recent Congressional legislation has opened the doors to evaluate cybersecurity, thereby allowing us to expand our capabilities and methodologies.

II. Current Status to Evolve Assessments and enhance Cybersecurity

The National Defense Authorization Act of 2017, Section 1650 directed the Department of Defense to evaluate cyber vulnerabilities within its critical infrastructure. Integrating upon other efforts, the Office of the Secretary of Defense decided to include this within its preexisting Mission Assurance construct. This was a natural fit because cybersecurity is one of the 17 programs that Mission Assurance Assessments evaluate.

The West Virginia National Guard has developed a relationship with the Cybersecurity Branch at the National Aeronautics and Space Administration's (NASA) Independent Verification and Validation (IV&V) in Fairmont, West Virginia. Members of this team have years of experience conducting blue and red team cyber assessments against some of our nation's most complex and sensitive technological architectures. Both organizations have a common objective and that is to ensure mission success for our respective organizations. The collaborative sharing of best practices has significantly enhanced both organizations' assessment teams.

We are currently working in conjunction with a cybersecurity community of interest that includes Army Cyber, NASA, Idaho National Labs, the National Security Agency, the Threat Systems Management Office, the Navy, and the U.S. Army Corps of Engineers to formalize our approach and bring together the best practices from each of these organizations.

We are working to develop a comprehensive approach and methodology for our cyber assessments. We will cover key cyber infrastructure areas such as the perimeter, networks, endpoints, applications, control systems, and the policies and procedures that govern them. We plan to conduct network architecture reviews, traffic analysis either live or offline, policy and procedure document review, access control evaluation, and wireless vulnerability assessments. Most importantly, we are striving to replicate these systems in a lab environment to research potential vulnerabilities, determine possible attack vectors, test resiliency, identify systemic concerns, and evaluate the impacts in a safe manner. We will document and report our findings and incorporate recommendations for risk mitigation into the Army's preexisting remediation processes.

III. Workforce Development and Benefits for the Cybersecurity and Energy Communities

In the last six months Army Cyber and the West Virginia National Guard have contributed to enhancing workforce development by sending team members to specialized training. The West Virginia National Guard has organized cybersecurity training in partnership with the University of Charleston in Charleston, West Virginia conducting Certified Ethical Hacker and Certified Incident Handler courses. Additionally, the WVNG has access to a decommissioned coal power plant. We use this facility to give trainees the opportunity to see firsthand the vast systems involved with Industrial Control Systems and power generation.

Our partners at Army Cyber have organized training at Idaho National Labs, SANS, and through internal training organizations. Courses include Industrial Control System training, Army Penetration Testing Course; Communications Security Course, and SANS courses such as ICS/SCADA Security Essentials, Essentials for NERC CIP, and ICS Active Defense and Incident Response.

Our teams have the unique experience not found in other organizations and can provide future benefits to the Defense and Energy industries. For instance, we have Engineers, Master Electricians, and Network Administrators that have been working in the energy and industrial sectors for decades. These unique

citizen soldiers can actively serve in uniform for a period of time and later return to industry providing valuable skills and knowledge they acquired.

To summarize, the West Virginia National Guard's Critical Infrastructure Protection Battalion is uniquely positioned to provide the Department of Defense and other related sectors insight and assistance pertaining to infrastructure protection and cybersecurity for industrial and interconnected systems. We will continue to move forward in our efforts to expand our cybersecurity activities and help more organizations secure this great nation of ours.

Thank you again for the opportunity to discuss our efforts to enhance cybersecurity within the West Virginia National Guard at today's hearing.