Public Hearing

"Election Integrity Reforms"

Testimony

House State Government Committee

October 15, 2018

Department of Military and Veterans Affairs

Major Christine Pierce

Pennsylvania National Guard Cyber Defense Branch Chief and

Defensive Cyber Operations Element Team Chief

Good morning Chairman Metcalfe and Chairman Bradford, committee members, ladies, and gentlemen. I am Major Christine Pierce, the Pennsylvania National Guard Cyber Defense Branch Chief and Defensive Cyber Operations Team Chief. I am honored to be here today to testify alongside the Department of State on Elections Security and Reform, but particularly want to share how our Pennsylvania National Guard (PANG) is supporting the Commonwealth with elections cybersecurity.

Our preparations for the upcoming November elections date back to the 2016 Presidential election. Because of the attention that the 2016 elections were drawing in the media, National Guard cyber teams were being called upon to provide cybersecurity support to their states' electoral systems. The PANG Cyber Team supported the Office of Administration (OA) and the Department of State (DOS) throughout the duration of the election. As you know, the DOS is responsible for voter registration and processing election results. Many of those processes are now done through web applications, servers, and databases that, if not properly protected, could be susceptible to cyber-attacks by potential hackers trying to perpetrate fraud or subvert Pennsylvania's election process. Those risks dramatically increase during the election cycle.

In order to mitigate the risk of fraud or interference with our electoral process, the DOS, the OA's Office for Information Security, and the PANG Cyber Team worked together to proactively monitor our electoral applications and systems. The PANG Cyber Team worked closely with the OA's enterprise security specialists, forensics analysts, network administrators, and incident response teams to monitor and investigate any cybersecurity incidents that could have impacted the DOS' voter registration application or election night returns application. We also assisted with the monitoring of the public facing election reporting site while continuously backing up the elections system servers.

The PANG Cyber Team also supported the mid-term elections in May of this year and is ready to support the Commonwealth during the upcoming November elections, just as we have in the past.

In addition, the PANG Cyber Team has been actively involved in other efforts to secure our voting systems including participating in the Election Security Interagency Workgroup. Through this DOS initiative, the PANG Cyber Team, the County Commissioners Association of Pennsylvania (CCAP) representatives, county election directors, DOS staff, and county and state IT directors discuss security issues, share training resources, and conduct county-level security self-assessments to improve the county's security posture. This collaborative effort has allowed the PANG Cyber Team to tell our story, engage with the counties, raise awareness about our team's capabilities and offer our cybersecurity assistance. Some of the assistance that the team provides includes Penetration Testing, Vulnerability Assessments, and Security Assessments of State Agency and Local Government Networks. We can also provide Vulnerability Remediation

Assistance; Cyber Incident Response; General Cybersecurity Assistance and Support (election support, cyber exercise development etc.); Cybersecurity Awareness Training and Education. Finally, we can provide software/electoral systems testing or training at the Joint Cyber Training Facility on Fort Indiantown Gap and the services of a Mobile Cyber Training Team for any specific training a county may desire.

The PANG was a key player in the cybersecurity election tabletop exercise hosted by the DOS a few months ago and the election security tabletop exercise hosted by the Pennsylvania Emergency Management Agency last month. These events provided an opportunity for participants involved in any part of the elections process to test their internal processes, exercise their incident response plans, collaborate with each other, share experiences and information, and just walk through all of those "what-if" election security scenarios.

In June 2018, the DOS engaged the Federal Department of Homeland Security (DHS) to conduct a Risk and Vulnerability Assessment (RVA) against DOS' electoral systems environment. The PANG Cyber Team was invited to shadow DHS' assessment team to better familiarize ourselves with our internal electoral systems and to learn DHS's penetration testing methodology and overall security best practices.

With everything that we hear in the national media regarding the vulnerability of our election systems, gaining the confidence of our voters has been a top priority in Pennsylvania. Pennsylvania is doing a lot of great work to ensure the security of its elections and voters need to know and hear this story. For example, Acting Secretary Torres and I participated in a Voter Roundtable Panel Discussion in August in Philadelphia. The Roundtable was hosted by the National Commission for Voter Justice and our participation in the event gave us the opportunity to share information about what the Commonwealth is doing regarding election security and to answer questions from the Commission and the public. The feedback that we received at the event was very positive. The Commission appreciated the information that we shared. They indicated that they now have a better understanding of our efforts to secure the election process and greater confidence in the security of the electoral process. Finally, they indicated that they now have reliable information that they can share with their members regarding Pennsylvania's efforts to secure our elections.

From my perspective, as the Commander of the PANG Cyber Team providing election security support for the last couple of years, I can attest to the fact that Pennsylvania has a great team of local, state, and federal partners who truly care about maintaining the integrity and security of our elections and do their absolute best to ensure that our votes are secure and accurate. This team works vigilantly to ensure that we have multiple layers of security in place, monitor and assess any potential vulnerabilities, implement the necessary technical controls, share resources, share information, train and exercise the response plans, and build relationships with

stakeholders and subject matter experts. Transparency and communication are the keys to our success as we continually strive to ensure the security of the election process. Thank you, I would be pleased to answer any questions that you may have.