Testimony

House Republican Policy Committee

March 28, 2022

Commonwealth Cybersecurity

Defensive Cyber Operations Element

MAJ Christine Pierce

PA National Guard Cyber Branch Chief

Defensive Cyber Operations Element Team Chief

112th Cyberspace Operations Squadron

Lt. Col Thomas Love

Commander

Chairman and Members of the House Republican Caucus Policy Committee, I am Major Christine Pierce, PA National Guard Cyber Branch Chief and Defensive Cyber Operations Element (DCOE) Team Chief.

I was assigned to the Pennsylvania National Guard Joint Force Headquarters in 2013 to start the first ever cyber program for the PA National Guard. "Cyber" was becoming the new buzzword as every state was trying to determine their role in cybersecurity. The cyber program started with one full-time soldier and a small traditional guardsman team that expanded to a full Army DCOE, which then incorporated the Air Force 112th Cyberspace Operations Squadron (COE) once they were stood up. I have approximately 19 years of experience in the Information Technology (IT) field with the last 10 years being in cybersecurity, policy, and cyber law.

The PA Defensive Cyber Operations Element conducts Defensive Cyberspace Operations – Internal Defensive Measures to secure the National Guard portion of the Department of Defense Information Network (DODIN). The PA DCOE protects critical infrastructure, provides cybersecurity compliance and readiness, and responds to cyberspace emergencies as directed by the Governor or Adjutant General. The PA National Guard is a supporting agency, requests to provide cyber support during emergencies to commonwealth agencies or critical infrastructure the PA National Guard receives a mission assignment from the Pennsylvania Emergency Management Agency (PEMA). For non-emergency events coordination with the Office of Administration (OA) and Pennsylvania State Police is required but PEMA mission assignments are not issued. We are a Pennsylvania first response asset that provides surge capacity to national capabilities and focuses on domestic cyber operations. We collaborate and build relationships with local, state, and federal government organizations as well as with academia, private industry, and international partners. One of the many ways the DCOE trains for their federal mission of protecting the DODIN and maintains their cybersecurity skillset is through our state and government partnerships and providing cybersecurity assistance to our community. We are a highly technical and trained team and want

to give back to our community using our advanced skillsets for the overall benefit to the commonwealth. We live, train, and work in the same communities that we are out there trying to protect so it is a win-win situation for both the DCOE and the organizations we partner with.

I like to say that the DCOE is a small, but mighty Army cyber defense team because despite various efforts over the last 9 years to increase our force structure in the commonwealth, we have not had the resources to grow, but have increased our state missions and support to our commonwealth partners to the best of our ability. Our federal mission is our primary mission, but we have devoted much of our time and resources to assist with increasing the overall cybersecurity posture within the commonwealth. Currently, the DCOE is a 9-person team consisting of seven cybersecurity professionals and two cyber intelligence analysts. All members of the DCOE are required to complete thousands of hours of training and represent a highly advanced skill set complimentary to Information Assurance, Cybersecurity Operations, Cyber Incident Response, Cyber Defense Infrastructure Support, Cyber Threat Hunting and Intelligence Analyzing. The PA DCOE possesses the ability to collect and analyze intrusion artifacts (viruses, malware, etc.) to enable mitigation of potential incidents; performs incident triage to determine scope, urgency, and impact; correlates threat assessment data to provide increased situational awareness within the cybersecurity community; and serves as technical subject matter experts in cyber defense and cybersecurity best practices. The DCOE also provides additional capabilities to include, but not limited to cybersecurity assessments and detection, networking, passive network monitoring, log analysis on hosts and networks to detect any anomalies or suspicious behavior, Advanced Persistent Threat anomaly detection, auditing, intrusion detection and prevention, threat and incident mitigation, defense in-depth integration, incident response and recovery, forensics analysis, incident reporting, and cybersecurity planning and policy development. The DCOE is required to maintain industry standard cybersecurity certifications and participate in a major collective cyber defense exercise annually to test their skills and certify the team in a virtualized environment designed to replicate real-world cybersecurity challenges, current

threats, new technologies and tools, and overall incident response capabilities in a high-stress environment.

In addition to the training DCOE members receive as members of the team, each individual team member brings a wealth of cybersecurity experience and knowledge from their civilian employment. All the traditional (citizen-Soldier) DCOE members are employed outside of their National Guard position in the cybersecurity field to include working for private and government cybersecurity companies with positions in cloud security engineering, performing security assessments, cybersecurity consulting, and various other distinct position in the field.

Since 2014, when the cyber branch and DCOE was officially established in the Pennsylvania National Guard, we have had a tremendous impact to not only the commonwealth, but also across the National and Global cybersecurity community.

Impact to the commonwealth. Over the last several years, cyber incidents and attacks have been on the rise and malicious actors have increasingly been targeting our state and local governments, academic institutions, critical infrastructure, and our private industry. There is a shortage in general with skilled cybersecurity professionals in the workforce, so we saw the growing need within our own communities to assist with cyber incident prevention. The DCOE has an overarching MOU with OA that encompasses all state agencies that fall under their jurisdiction and all state agency cybersecurity assistance events are coordinated between the DCOE and OA. We wanted to be proactive and use our advanced cybersecurity skills to help protect our infrastructure in the commonwealth, so the DCOE started a cyber community outreach program and began offering various cybersecurity services to our commonwealth partners. Our program includes building partnerships and relationships within the cyber community amongst federal, state and local government, private industry, critical infrastructure, and academic institutions. The DCOE believes in a collaborative cyber approach and getting out in the community to discuss capabilities, share information, collaborate, and build those relationships within the cyber community. This facilitates communications among partners so in

the event of a cyber incident, a collaborative group is already established, the trust and relationships are already built, capabilities are known, and roles are identified. The DCOE has collaborated with over 50 commonwealth organizations and those partnerships include generating Memorandums of Agreement between each organization as well as the signing of Nondisclosure Agreements when conducting sensitive security assessments with those organizations. Additionally, as part of the cyber community outreach program, the DCOE conducts cybersecurity assessments for our partners. To date, the DCOE has completed close to 40 cyber assessments for county governments, local governments, state agencies, and academic institutions. These assessments range from an initial vulnerability assessment to assist the organization with identifying any physical and network vulnerabilities within their environment to a follow-on penetration test to identify and exploit any vulnerabilities discovered and then to a red team engagement where the DCOE acts as a malicious cyber actor, and the target is very specific with the overall goal being to test the organization's ability to detect and respond to suspicious behavior. Since the DCOE builds a lasting partnership and relationship with each organization they assist, they have the unique opportunity to not only build up the level of trust with each organization, but also assist the organization with the vulnerability remediation process and internal cybersecurity training. Because a nondisclosure agreement is in place, any information shared between the DCOE and the organization remains private and confidential and will not be shared outside of those personnel that signed the nondisclosure agreement.

Since 2018, the DCOE has been supporting state, local, and education partners one week during each month with general cybersecurity assistance. This has given the DCOE the opportunity to train in a real-world environment, building partnerships across the commonwealth, and providing a service to our community. The DCOE has also been called to respond to a Denial-of-Service attack at a local high school and a Ransomware attack on a county government network in an incident response effort.

In addition to providing security assessments and incident response support to the commonwealth, the DCOE has also been an integral part of the commonwealth's

elections security efforts. The DCOE assisted in the cybersecurity for every PA election since 2016 to include all Special, Primary, General, and Presidential Elections. The DCOE supports the state with general election security by being a member of the state election security workgroup, conducting vulnerability assessments on county government networks to identify any vulnerabilities within county electoral systems prior to any elections, working with state partners on Election Day on standby in the event of a cyber incident that requires DCOE incident response, and supporting the PA Department of State with electronic poll book demonstrations and vulnerability identification.

With regards to general cybersecurity support to the commonwealth, the DCOE coordinates with various agencies, including OA and PEMA and is a member of various professional cybersecurity organizations and workgroups and leads the state cyber training and exercise workgroup that developed from the initial Pennsylvania Cyber Incident Annex Planning workgroup and encompasses all of the key cyber stakeholders within the commonwealth. The purpose of the workgroup is to coordinate and develop key cyber training events for the commonwealth as well as plan annual tabletop exercises to test and validate our PCIA.

The DCOE has a Joint Cyber Training Facility at Fort Indiantown Gap where we conduct our own internal team training, host training for our cybersecurity partners, and conduct research and development of in-house cybersecurity tools, methodologies, and processes. Our cyber training facility has a virtual cyber training environment with red team / blue team cyber training capability. The facility also has the Army GuardNet network, the Airforce network, a commercial network, and the PA.gov network. The facility also has an Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) cyber trainer incorporated into the virtual training environment for real-world operational technology training. The facility is Unclassified so there are no access limitations.

One of the training initiatives the DCOE pursued over the last few years was the development of our Wi-Fighter cyber challenge. The PA DCOE developed a virtualized cyber "hacking" competition to recruit and train high school, college, military units, and civilian mission partners. Several iterations/challenges of the

event have been developed to accommodate different scenarios, in-person events, or full virtual events. One version of the in-person event is a race against the clock where each team attacks to exploit the opposing team's missile control system before getting exploited themselves – the goal is to launch the opposing team's missile first (real Nerf missile launcher)! This exercise teaches many real-life cyber security concepts in a way that cannot be learned from books. One of the virtual challenges training goals is to become familiar with the Raspberry Pi Single Board Computer Hardware, gain a foundational understanding of the Linux/Unix Command Line Interface, and demonstrate and internalize this knowledge through Capture the Flag practical exercises. The duration of each Wi-Fighter Cyber Challenge ranges from 4-hours to 3-days, depending on the participants skill level and challenge. The DCOE hosted over 10 of these events at academic institutions (high school and college level), military organizations, and with our civilian partners.

The DCOE also provides a mobile training team that goes out into the community and presents cyber awareness briefs and training, cyber threat briefs, technical and hands on training, cybersecurity career briefings, capabilities briefings, amongst various other types of training and general cybersecurity education.

PA DCOE Impact to the Nation

The PA DCOE participates in a variety of national level cyber exercises and holds key leadership positions in the overall development of the National's Guard's largest cyber exercise, Cyber Shield. The DCOE was also a national leader in the response efforts for the Log4j and Solarwinds cybersecurity vulnerabilities and incidents and set several national level standards adopted by high levels of leadership. The PA DCOE also supported various National Special Security Events (NSSE) events to include the Papal Visit, the Democratic National Convention, and Presidential Inauguration event where the DCOE worked with the PA Governor's Office of Homeland Security, the Pennsylvania Emergency Management Agency, and other state partners to remain situationally aware of any potential cyber threats, share

information, and monitor the cyber threat landscape and prepare for cyber incident response in the event of a significant cyber incident during these NSSE events.

PA DCOE International Impact

The PA DCOE has participated in close to 40 international cyber missions and training events with our partners in the Baltic region of Eastern Europe (Lithuania, Latvia, and Estonia). These events were designed to strengthen collective Information Assurance and Cyber Defense within the Baltic Region, but particularly with our State Partnership for Peace partner, Lithuania, as well as increase the overall cybersecurity posture in the Baltic region; joint participation in EUCOM and NATO led exercise; facilitate regional cyber defense development and multi-national information sharing; and increase diversity of thought and partnership building.

112th Cyberspace Operations Squadron

Chairman Causer and Members of the House Republican Caucus Policy Committee, I am Lieutenant Colonel Thomas Love, Commander of the 112 Cyberspace Operations Squadron at Biddle Air National Guard Base.

I was assigned as the commander of the 112th in October of 2017 and have been serving in various capacities in the military since 1992. I have approximately 25 years of experience in the Information Technology field and 5 in cybersecurity and policy. Before taking command of the Cyberspace operations squadron, I had the opportunity to work on cyber policy issues as part of the Chief of the National Guard Bureau's staff interacting with multiple government and industry agencies as well as members of the congressional staff to help in the development of the National Guards role in cyber security. The 112th Cyberspace Operations Squadron conducts Defensive Cyberspace Operations supporting Air Force Cyber (AFCYBER), United States Cyber Command (USCC), the Air National Guard, and the State of Pennsylvania. Our primary mission is to support the Cyber National Mission Force as a service retained Cyber Protection Team (CPT). The squadron consists of 71 members comprised of Cyber Operations Personnel, Intelligence Personnel,

Network, and Support personnel. The Cyber Protection team consists of 39 members of the squadron and is an operational element of the unit. The CPT can be deployed as a single unit or 3 individual elements of 9 personnel to execute multiple operations.

The Cyber Protection Team provides cybersecurity subject matter experts to protect Air and Space Force assets along with national security interests. The team conducts threat hunting, vulnerability assessments, incident response, and mission assurance through intelligence-driven operations. A typical operation can range from assessing and hardening a personnel database on an Air Force Network to hunting for an adversary on Space Force satellite systems across the globe. The team provides a standard structure with multi-mission capabilities able to detect and defend against Advanced Persistent Threats (APT).

The 71-member squadron is made up of 18 full-time members and 53 citizen/ airmen. These airmen receive extensive technical training to become cyberspace operators. A typical operator will attend no less than 1500 hours of training before they are granted access to our systems. Upon completion of their initial training, they will undergo two additional weeks of system-specific training to become qualified to conduct operations with the CPT. Once qualified every operator is required to maintain certification on the system and receive yearly evaluations.

Our typical airman works in the cybersecurity career field, and many are senior-level operators or directors within the civilian companies and government agencies where they work. While we have a large population that works in the local area, we have members throughout Pennsylvania and from Virginia, Maryland, D.C., Florida, and New Jersey. These members represent agencies across the DoD, the US Congress as well as defense and tech industry companies like VMWare, Facebook, Lutron, Lockheed Martin, Elastic, and COMCAST. Most of our members hold industry certifications including Certified Information Security Systems Professional (CISSP), GIAC: Network Forensic Analyst (GNFA), Certified Forensic Analyst (GCFA), Security Leadership Certificate (GSLC), GCIA, Certified Ethical Hacker,

Cisco Certified Network Associate (CCNA), Sec+, and Certified Information Security Manager (CISM) among many others. Several of our airmen are also members of organizations like InfraGard, Multi-State-Information Sharing and Analysis Center (MS-ISAC), Homeland Security Information network, and collaborate with other agencies throughout the state.

Since the squadron stood up in 2016, we have participated in multiple state, federal, and international cyber exercises and events bringing industry and military expertise to train and protect against cyber threats. Our airmen are a critical resource for both federal and state agencies to defend against cyber-attacks. Along with our state and federal partnerships, the 112 COS has a strong partnership with Lithuania's Ministry of Defense training annually with their cyber defense force. This relationship provides both countries with training that improves cyber skills to protect against cyber-attacks. Starting in 2021 the 112 COS has begun working with Lithuania's Regional Cyber Defense Center to share information on cyber-attacks and potential vulnerabilities to further protect against Advanced Persistent Threats.

The 112 COS Airmen bring a wide range of experience to the fight and make no mistake it is a daily fight in cyberspace. As you are aware, one of the biggest vulnerabilities we face as a nation are cyber-attacks against our critical infrastructure. In 2021 cyber-attacks costs topped 20 billion dollars and was the worst year on record for ransomware attacks up 62% from just two years ago. Having a Cyberspace Operations Squadron within the state of Pennsylvania provides an opportunity to provide additional capacity to help protect the state from these attacks and assist with recovery when a State, Local, Tribal or Territorial entity is impacted by a cyber-event. The 112 COS operators are skilled in training cyber defenders in the latest tactics, techniques, and procedures to detect, harden and remediate a cyber-attack.

Our intelligence personnel are skilled in collecting information and analyzing cyber threats to provide operators with valuable insight used to identify potential attack

vectors or determine possible threat actors based on their methods of attack. This information can be provided to state agencies and shared with both public and private entities to help guard against known APT tactics. When approved by DoD the 112 COS can also utilize their security clearances to gain access to intelligence that could help prevent or remediate a cyber-incident.

Another benefit of having the Cyberspace squadron in Pennsylvania is the ability to train and exercise with government agencies and other mission partners throughout the state. Exercise training and events allows members to come together to learn from one another and builds our resiliency by sharing best practices, developing security awareness, and opening lines of communication between entities to respond to cyber incidents. One example of this is the 112 COS participation in exercises with PJM corporation. PJM is one of the largest energy distribution companies on the east coast headquartered in PA. The training and lessons learned during these events provide open communication and allow for sharing of information and best practices to help secure critical infrastructure with little to no cost to the government but with significant gain to the participating entities.

Access to and collaboration with other Cyberspace Operations Squadrons throughout the Air National Guard specifically with Delaware, New Jersey, and Maryland provide additional resources and information sharing avenues to help detect or prevent cyber incidents. These relationships are key to enhancing our region's cybersecurity posture and provide additional expertise when leveraged during a cyber-event. The 112th COS maintains a good relationship with these units, frequently collaborating on exercises and training events that strengthen our cyber capabilities.

While cyber-attacks continue to rise, there is a unique opportunity in Pennsylvania to leverage our National Guard to provide additional capacity to help increase our state's cybersecurity posture and respond to these attacks. Pennsylvania has a significant number of tech companies, financial, industrial, and federal agencies

coupled with great academic institutions that provide a strong recruiting base for cyber operators.

Thank you for the opportunity to provide this written testimony. If you have any questions or need additional information, please contact the DMVA Policy and Legislative Affairs Director Gilbert "Dusty" Durand at gdurand@pa.gov for further coordination.