Pennsylvania National Guard Joint Cyber Capabilities

112 Cyberspace Operations Squadron

- Federal Mission: Provide Defensive Cyberspace Operations in support of Air National Guard, AFCYBER and USCYBERCOM
- State Mission: Ensure cyber preparedness and incident response for rapid internal state-level and national coordination needed to defend the State of Pennsylvania against any cyber incidents
- Squadron consists of 71 highly trained Citizen/Airmen (18 Fulltime)
  - Can operate in elements of 9 personnel to full 39-member team
  - Cybersecurity and Intelligence Personnel
  - Over 1500 hours of Training to become certified

Cyber Protection Team

- Provide Cybersecurity subject matter experts to protect Air Force Assets and National Security interests
  - Mobile Teams providing full complement of Cyber Protection and Incident Response
    - Able to detect and defend against Advance Persistent Threats

Standard structure, Multi-mission capability

Air Force Taskings

Cyber Mission Force Taskings

Digital Forensics

Incident Response

Vulnerability Assessments

Intel Driven Operations

Cyber Protection Team

- Provides State entities with Incident Response, Information Sharing, Education and Training
  - Able to share information across communities to defend against cyber vulnerabilities
  - If activated and approved can share Intel with agencies
    - Provide analysis of information and Intelligence to critical state infrastructure stakeholders

CTAA Mission

Information Sharing

Cyber Hygiene/ Education

Industrial Control Systems

Exercises

PA Army National Guard | Defensive Cyber Operations Element

Protect & Defend · Detect & Analyze · Respond · Train · Partnerships & Integration

Who We Are

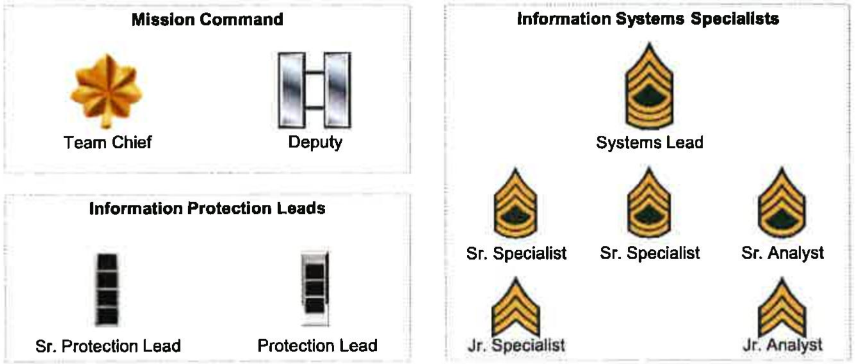
The DCOE is a Pennsylvania State first response asset. We provide surge capacity to national capabilities and focus on domestic cyber operations. We partner with local, state, and federal government organizations as well as academia, private industry, and international partners.

Our Mission

To conduct Defensive Cyberspace Operations – Internal defensive measures to secure the Department of Defense Information Network in Pennsylvania. On order, DCO-E's protect critical infrastructure and respond to State cyberspace emergencies as directed by The Adjutant General or Governor.

Our Team

DCO-E members are highly trained and technically qualified, possessing the skills and knowledge required by today's defensively-oriented cyber forces.



Mission Command

Team Chief

Deputy

Information Protection Leads

Sr. Protection Lead

Protection Lead

Information Systems Specialists

Systems Lead

Sr. Specialist

Sr. Specialist

Sr. Analyst

Jr. Specialist

Jr. Analyst

Services We Provide

Vulnerability Assessments

☑ *Network-based*
☑ *Host-based*
☑ *Wired & Wireless*
☑ *Application Scans*
☑ *Cloud & Vendor Services*
☑ *Mobile Devices & Apps*

Penetration Testing

☑ *External*
☑ *Internal*
☑ *Web Application*
☑ *Social Engineering*
☑ *Physical Security*
☑ *Mobile Devices & Apps*

Vulnerability Remediation Assistance

☑ *System STIG/SCAP Advisory*
☑ *Vulnerability Prioritization*
☑ *Key Vulnerability Patching*

Cyber Incident Response

☑ *Critical Service Restoration*
☑ *Digital Forensics*
☑ *Data Recovery*
☑ *Infrastructure Recovery*
☑ *Malware Advisory*
☑ *IDS Threat Monitoring*

General Cybersecurity Support

☑ *Defend the DODIN*
☑ *Election Support*
☑ *Cyber Exercise Development*
☑ *Cyber Community Outreach*
☑ *State Cyber Workgroups*
☑ *Miscellaneous SME Support*

Training Opportunities

☑ *Cybersecurity Awareness Training*
☑ *Cyber Exercise & Mission Partners*
☑ *Joint Cyber Training Facility at Fort Indiantown Gap*
☑ *Mobile Cyber Training Team*
☑ *Cyber Wi-Fighter Challenges*
☑ *SPP Missions*

Cyber Partnerships and Integration Activities

PA National Guard | Joint Cyber Operations

Protect & Defend · Detect & Analyze · Respond · Train · Partnerships & Integration

Our Impact Since 2014

PA Cyber Assessments

30+ *County, City, State, Local Governments & Public Education Customers*

Cyber Training Exercises

35+ *Cyber Shield, Wi-Fighter, Warfighters, GridEx, FEMA TTX, etc.*

Pennsylvania Missions

5+ *Papal, DNC National Convention & Presidential Inauguration Missions*

SPP Missions

40+ *Amber Mist, Baltic Ghost, Lithuanian Elections, Vigilant Guard, etc.*

Election Support

10+ *Supported Special, Primary & Presidential Elections*

Industry Cyber Events

50+ *PA Cyber Incident Annex Development, CCAP, Public Utility Forum, etc.*

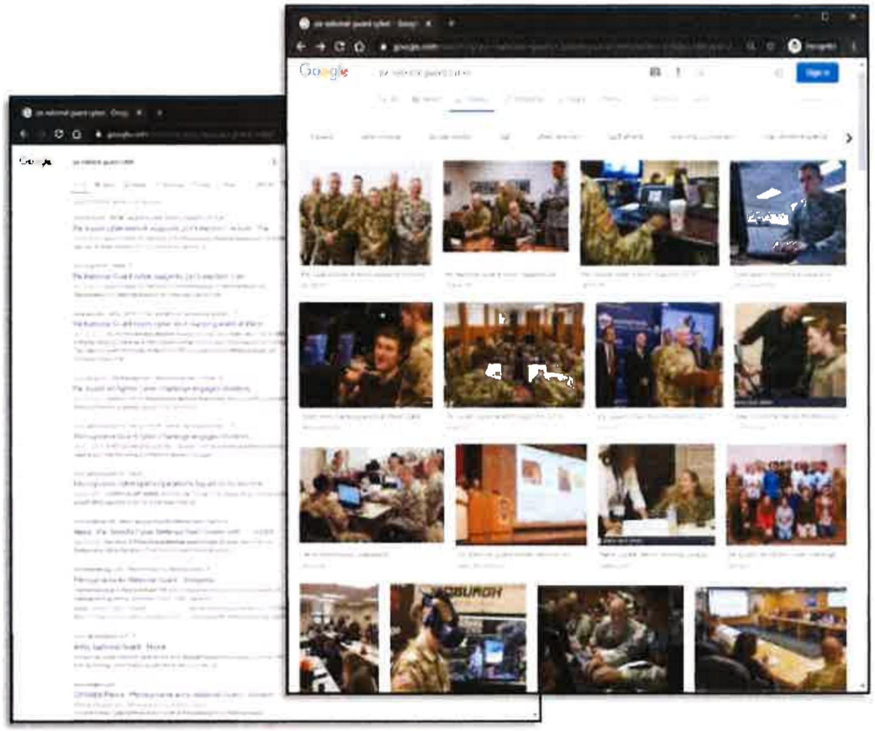
Air Federal Cyber Mission

29 *9000 Hrs. Conducting Defensive Cyber Ops, 7 Major Weapons Systems Analyzed*

Army Federal Cyber Mission

10+ *DOD Network Incident Response, Vulnerability Analysis, Security Inspections*

Just Google
"PA National Guard Cyber"



PA National Guard | Joint Cyber Operations

Federal · Private Industry · International · State · Academia · Partnerships & Integration

Our Partnerships

Federal

US Space Force
Army Cyber Command
FEMA
CISA
DHS
National Governors Assoc.
91st Cyber Brigade
Department of Energy
FERC

Private Industry

FirstEnergy
PJM

International

Lithuania Ministry of Defence
Lithuania Regional Cyber Defence Center
Vilnius University

State

PEMA
OA
GOHS
PACCIC
Public Utility Commission
South Central Task Force
East Central Task Force
CCAP
Department of State
Eastern PA EMS Council
PSP
Adams County
Berks County
Bucks County
Centre County
City of Allentown
City of Bethlehem
Clarion County
Crawford County
Cumberland County
Dauphin County
Delaware County
Elk County
Green County
Harrisburg City
Lehigh County
Luzerne County
Monroe County
Schuylkill County
Susquehanna County
Township of Upper St. Clair
Wyoming County
York County

Academia

Penn State University
Drexel University
Harrisburg University
Agora Cyber Charter
Commonwealth Charter Academy
Community College of Allegheny County
Civil Air Patrol
DeSales University
Hanover Area School District
Carnegie Mellon University
Bloomsburg University
Central Susquehanna Intermediate Unit
Capital Area Intermediate Unit
Gannon University
Valley Forge Military Academy
Hazleton Area School District
State College Area School District
Berks County IU
Colonial IU

How We Integrate and Help Organizations

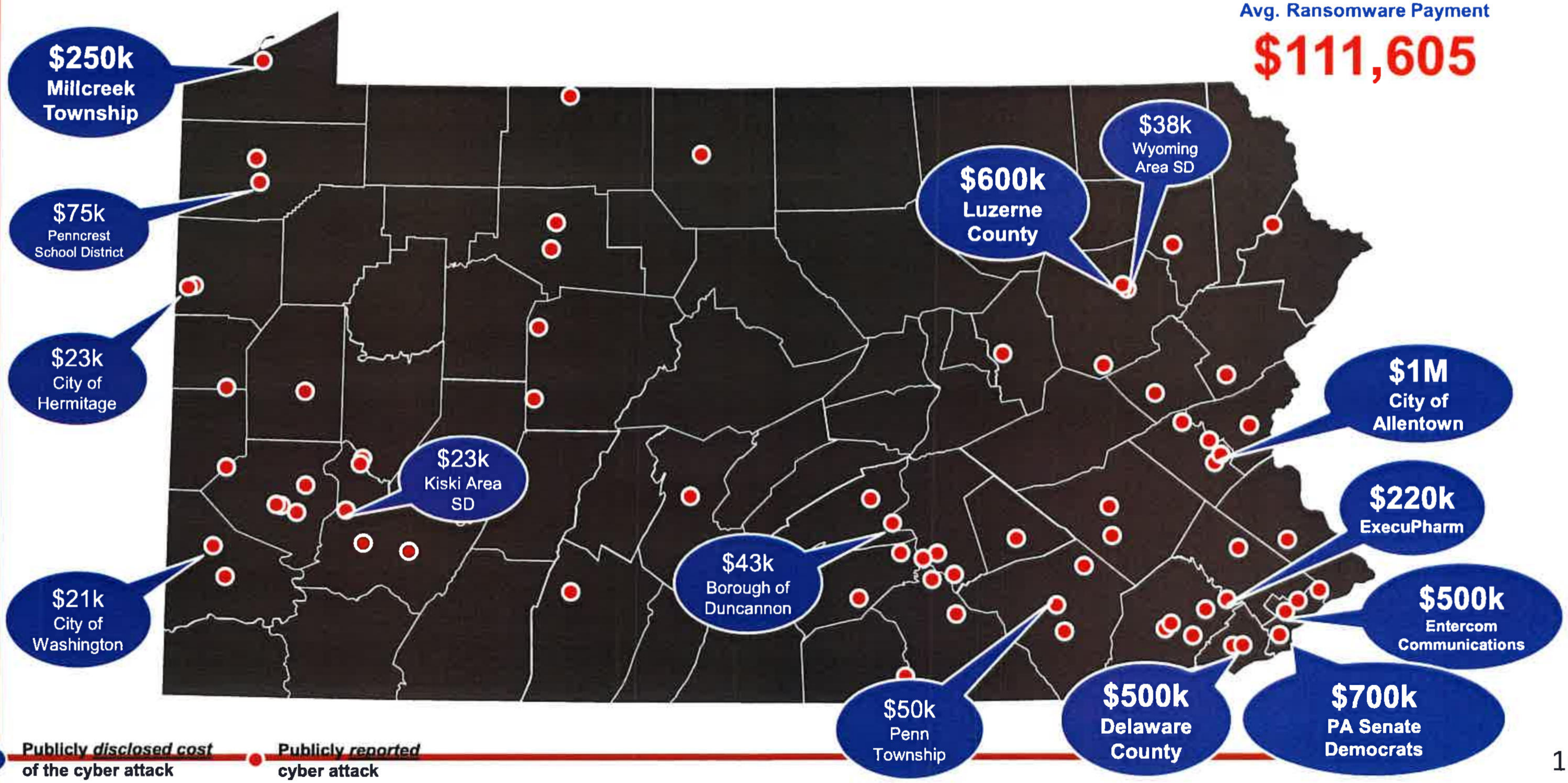
Cyber Assessments, Training & Community Outreach

OUR community is under constant cyberattack.

Is YOUR community or organization prepared?.

Avg. Ransomware Payment

$111,605



$ **Publicly *disclosed cost* of the cyber attack**

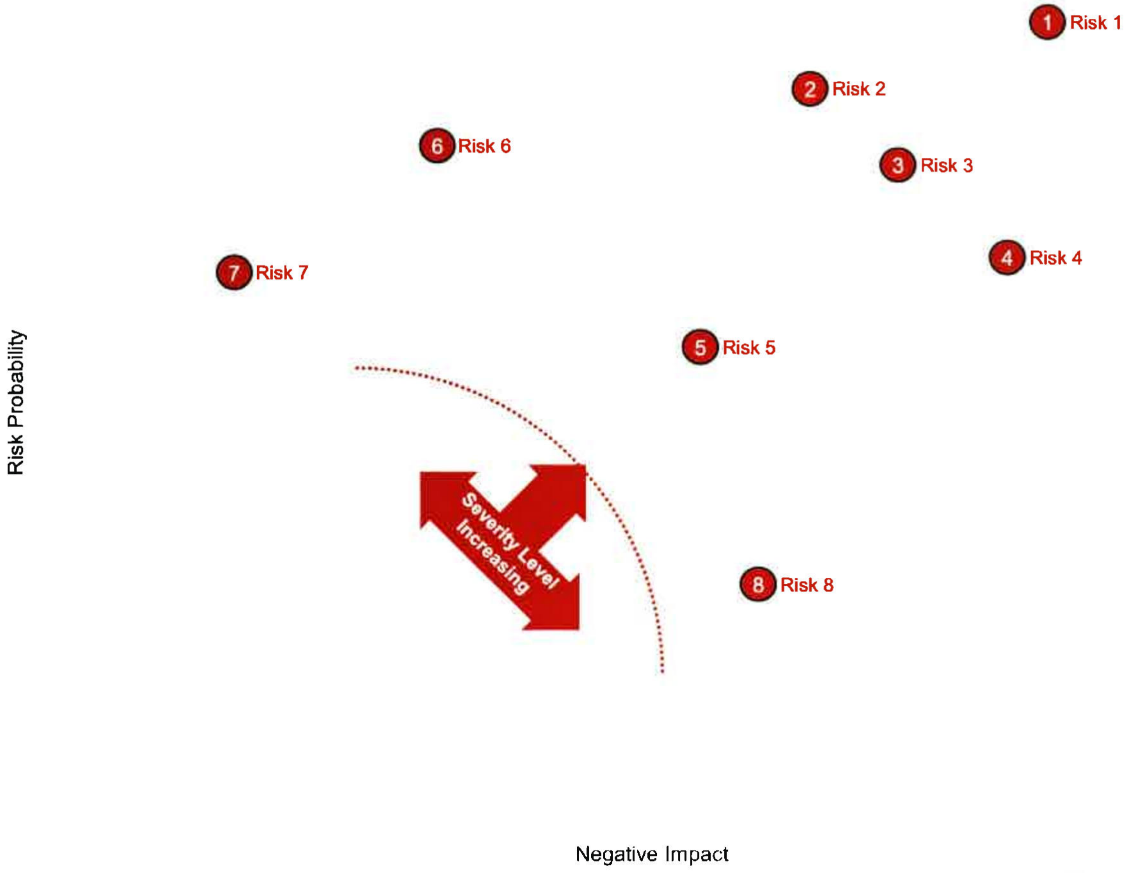
● **Publicly *reported* cyber attack**

We help to focus resources where it matters most.

Prioritize the vulnerabilities and risks to focus customer remediation efforts.

Approach Benefits

- Prioritizing efforts based on severity is a must when you have limited cyber security and IT resources.
- Assessment results are compiled into an actionable list that the organization can work to remediate.
- This approach provides the organization with the clear steps to increase the cyber security posture.
- The PA Guard Cyber Team can be brought in at a regular interval to re-validate or extend the assessment scope.



We validate progress and keep organizations moving forward.

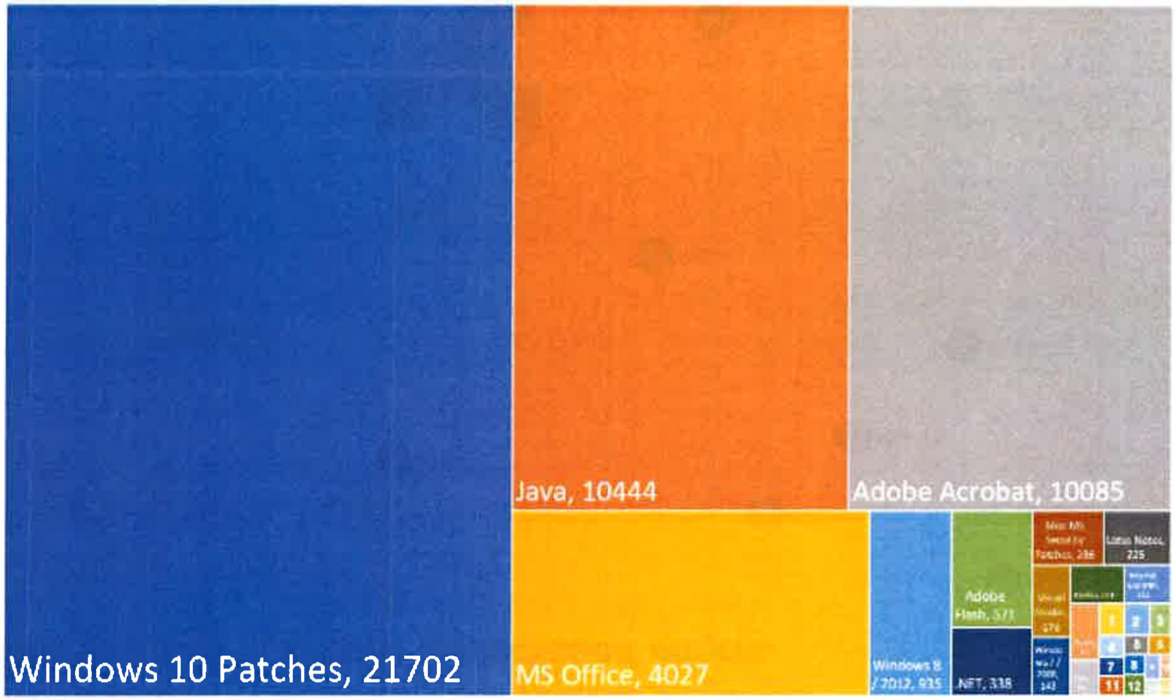
Continue to fortify completed recommendations while continuing to remediate.

Previous Recommendations Progress

Status	Recommendation
✓–	Implement Network Access Control (NAC)
✓	Implement and Configure Splunk (SIEM)
–	Remediate Vulnerable Java SE
✓	Centralized Antivirus Activity Monitoring
–	Audit User and Service Account Permissions
✓–	Disable USB Mass Storage on Hosts
✓–	Review Remote Site IT Compliance
–	Close Physical Security Loopholes
✓–	Users Training for Cyber Awareness
✓–	Baseline and Disable Unnecessary OS Services
✓	Disable Vulnerable Network Protocols
✓–	Implement Network Segmentation & Access Controls
–	Patch Network Devices

✓ Remediation Fully Implemented ✓– Intermediate Solution or Nearly Implemented – Not Implemented

Breakout of Critical and High Vulnerabilities



We provide tactical, tailored, and actionable plans.

To assist with remediation, we will provide a number of written output artifacts

Data Collection

Documented <u>During</u> Testing

- Testing Activity Log
- Enumeration of Network
- Host Target Selection
- Potential Target Vulnerabilities

Executive Report

Message from the Director of the Joint Staff

"Hacker's Journey"

Penetration Testing Timeline

Presented on <u>Last Day</u> of Testing

- Background Information
- Testing Scope, Objectives & Timeline
- Summary of Key Findings
- Prioritized Recommendations
- Appendix of Slides to Date

Technical Report

PA ARNG DCO-E

Technical Report

Provided <u>After</u> the Assessment

- Technical Details of Vulnerabilities
- Step-by-step Through Exploit Process
- Includes Screenshots & Technical Details

Thank You!!

Gilbert (Dusty) Durand
Director, PA DMVA
Policy, Planning, and Legislative Affairs Office

Thomas A. Love
Lt Col, PAANG
112th COS Commander

Christine Pierce
MAJ, SC, PAARNG
J36, DCOE Team Chief

Policy, Planning, and Legislative Affairs Office
BLDG 7-36, Fort Indiantown Gap
Annville, PA 17003