

# WEST VIRGINIA NATIONAL GUARD AIR FORCE

## FOCUS on the FORCE



### Focus on CYBER awareness

Recent cyber intrusions and espionage on our businesses and institutions highlight why cyber is a national priority. The National Guard's cyber capacity will play an integral role as we coordinate with state and federal cyber professionals through Army and Air Guard cyber units and continue to grow our cyber forces.

- The National Guard's Defensive Cyber Operations mission is to defend DoD assets by conducting cyber command readiness inspections, critical infrastructure and vulnerability assessments, realistic training and supporting interagency partners.
- The National Guard supports national security objectives by developing integrated cyber capabilities and building a skilled cyber workforce.
- As a matter of policy, we do not discuss specifics pertaining to the source of threats to DoD systems or any network vulnerabilities.
- We know that a number of nations and groups are actively developing dangerous cyber capabilities and developing and implementing various, in some cases destructive, cyber capabilities.
- The National Guard's network backbone, GuardNet, receives more than 100,000 cyber- attacks each week.
- Department of Defense networks are probed approximately 250,000 times per hour (6 million times per day), with more than a hundred foreign intelligence organizations attempting to steal information or intrude into our networks and systems.
- We regularly receive incident reports pertaining to intrusion activity, and continue to investigate such incidents. Many of the attempted intrusions into DoD's networks and systems involve commercial software applications or operating systems.
- States have an inherent right to self-defense that applies to all domains, including hostile cyber acts.



# YOUR CAREER FUTURE SUCCESS