Recommendation
The National Guard Association of the United States urges the Congress to:
- Support H.R. 1640 and S. 658, the Cyber Warrior Act
- Ensure a continued role for the National Guard in cyber defense strategy and force structure planning, training, equipping and execution

Background
The National Guard can easily leverage itself in the cyber domain by highlighting its unique access to a wealth of information technology talent within its ranks, including Guardsmen working top information technology, banking, medical and defense companies.

Recently, the Chief of the National Guard Bureau, General Frank Grass, stated: “We have a reservoir of Guard members who excel in the information technology field, with many able to leverage experience gained from world-renowned IT corporations…We offer the Defense Department a viable and economical means to bolster its cyber capabilities and, as skills are developed through civilian experience as well as military training, lower the cost to the nation.”

There is an across the board concern that the government is unable to capture or entice the most skilled professionals into a cyber workforce.

In his testimony before the Senate Armed Services Committee, Defense Secretary Chuck Hagel noted that recruiting and training skilled military and civilian personnel needed for cyber operations "will be a challenge" in light of the looming budget cuts facing the department.

The National Guard has unique cyber support capabilities associated with Title 10, Title 32, State Active Duty statues. State Guard leaders can easily and effectively fill cyber roles since they have a distinct knowledge of cyber-vulnerable critical infrastructure, due to the Guard’s longstanding relationships with owners and operators.

As Congress moves forward towards crafting cyber security legislation, they should look towards the Guard’s unique and diverse capacity and capability to address concerns in establishing an effective and proper cybersecurity workforce.

How the Guard Fits:
The Guard possesses unique civilian roles and skills which draw upon synergies with their related civilian careers, leveraging skills developed by high-tech companies.

Can easily transition into duties within Title 10 service.

Bring diverse information and trust between the private sector and the government.

Capture a centralized repository of information which is lacking in the Department of Defense and federal government.

The Air National Guard (ANG) Cyber Warfare and Information Operations support federal and state-level agencies, the Air Force, and Combatant Commanders by conducting cyberspace force application, cyberspace defense, cyberspace support, influence operations, and related planning activities.

Specific missions assigned to ANG units range from network vulnerability assessments to digital media/network analysis to full-spectrum cyber warfare support in both exercises and operations. Execution of these activities occurs from home stations, AF locations and national facilities.

The Army National Guard Cyber Network Defense Teams defend GuardNet, performing vulnerability assessments and conduct traditional Information Assurance operations. Training and experience include network operations, computer forensics, network warfare, and intrusion defenses.