South Carolina State Guard

G-2 Cyber Unit

Commanders Conference

11 February 2023

COL William L. Oden

G-2

Revision Date

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit

Table of Contents

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit

Table of Contents con't

Annexes

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit

Purpose

- The purpose of the SC State Guard G-2 Cyber Unit is to support the National Guard's 125th,135TH,145TH Cyber Protection Battalions and the Defensive Cyber Operations Element (DCOE) State Active Duty (SAD) missions to the extent possible and permissible.
- To work with State and Local Governments when needed for Cyber assistance.
- Provide Cyber forensics for State, Local and private sector agencies if requested through SLED
- Provide Cyber related training for National Guard and SC State Guard Units when requested.
- Leverage Public and Private sector Cyber professionals to support the above missions.
- Provide a Cyber Baseline Assessment for SC State Guard units.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
BACKGROUND/CONCEPT

In 2015 meetings began with SC National Guard G-6 leadership and SC State Guard G-2 leadership to develop the concept of forming a SC State Guard Cyber unit. The SC State Guard already has a leadership hierarchy in place and has extensive experience with emergency response.

The idea was to bring public and private sector personnel with the skill sets for cyber together to form a SC State Guard Cyber Unit to work with and support the SC National Guard.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Background/Concept con't

Critical Infrastructure/people/systems are at greater risk of being targeted/compromised by Cyber incidents during events like Hurricane Florence. State Guard & SC National Guard Cyber Teams are working to counter potential threats.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Cybersecurity/Intelligence/CPT
METL

- Mobilize and Deploy to provide cyber security risk analysis and mitigation to the public.
- Provide Weather Information.
- Provide Unclassified Information on Cyber Events for Situational Awareness.
- Teach, Coach, Train SCSG Force Package on Cybersecurity Awareness/Counter measures.
- Plan and coordinate with National, State, and Local Authorities to be ready for possible cyber events.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Organization

Commander Cyber Security Detachment (COL)
Deputy Commander Cyber Security Detachment (LTC)
Senior Cyber Legal Liaison to National Guard (LTC
Senior Cyber Liaison to National Guard (LTC)
Training Officer (MAJ)
NCOIC (SGM)
Assistant NCOIC(MSG)
Admin Spec (SFC)

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Organization cont. – 5 Cyber Protection Teams

CPT Senior Team Lead
CPT Team Lead
CPT Forensics Analyst-(trained using network and systems forensics tools)
CPT Host Analyst -(has experience with Windows, Linux and iOS operating systems)
CPT Intel Analyst -(has experience gathering information and pulling out pertinent items)
CPT Network Analyst -(has experience with network architecture and configurations)

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Basic Qualifications

- CompTIA A+ Certification or 2 years' experience working with computer systems.
- CompTIA Network + Certification or 2 years' experience working with networks.
- CompTIA Security+ Certification or 2 years' experience working as a systems security specialist.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Alternate Qualifications

- 5-years' experience working as a Computer Systems administrator, Network Administrator or Security Administrator.
- 4-year or higher degree from an accredited Institution in Information Technology or equivalent
- 2-year degree from an accredited Institution in Information Technology or equivalent.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Training/Testing

Training standards will be a combination of National Guard cyber training requirements and National Institute of Standards and Technology (NIST) training standards.

The Cyber Unit will train with the SC National Guard 125th, 135th, 145th Cyber Battalions and the Defensive Cyber Operations Element (DCOE) during their unit drill/training days when possible.
Train with industry partners during cyber exercises when possible.
Utilize free FEMA and DHS Cyber courses when available.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Training Cont.

Partner with State Tech Colleges
Partner with State Funded and private Colleges and Universities (i.e. The Citadel, USC Aiken, Morris College, SC State University and Benedict College)
Partner with out of State Colleges and Universities
Partner with businesses
Partner with the USSS
Utilize in house personnel

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Proposed Entrance Ranks

We have recruited and will be recruiting professionals in the fields of Information Technology and Cyber Security the majority of which have bachelor's degrees with some having advanced degrees.

Commissioned Officers

Based on Education alone:

B.S.	O-1
M.S.	O-2
PhD	O-3

Propose one grade higher for each five years of relevant, qualified experience not to exceed initial entry grade of O-5. Work experience not related to Cyber, Networking, Systems Administration, Computer Administration or Intelligence will not count.

SOUTH CAROLINA STATE GUARD
G- Cyber Unit
Proposed Entrance Ranks Cont.

Warrant Officers

Army Warrant Officer: an adaptive technical expert, trainer, and advisor.

Propose years of work experience to correspond with SCSG typical cumulative Time in Grade.

Also propose initial appointment to WO1 with either a 2-year degree or equivalent combination of college hours and work experience.

WO1	0 years' experience
CW2	1.5 years' experience
CW3	3 years' experience
CW4	7 years' experience

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Recruiting

- Coordinate with Accessions Command on new State Guard recruits
- Reach out to Colleges and Universities that have cyber programs
- Attend recruiting fairs
- Attend recruiting events with National Guard recruiters
- Partner with the Citadel
- Talk with public and private sector employers
- Collaborate with other SC State Guard units to see if they have any cyber trained troops
- Target women and minorities

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Events and Activities

- CERTS – Cyber Education, Research and Training Symposium
- Present at Morris College for Career Day
- InfraGard Cyber Camp at Morris College for Sumter County High School Students
- Responded to two Cyber Incidents

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Organizations where our team members work

Benedict College
Truist Financial
Greenville County School District
CAPTRUST
United States Navy (contractor)
SC Legislative Services Agency
Enviva LP
TRADOC/CCOE
Recorded Future
Guild Mortgage Company
Bank of America Merrill Lynch

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Annex A Sample Services Portfolio

Protecting your passion is our mission.

Put simply – we are here to protect and serve you. G-2 provides pro-bono cyber security consulting to organizations within South Carolina. Our volunteer citizen soldiers are accomplished professionals within IT, security, and intelligence who are dedicated to helping protect others.

Think we could help? Send us an email.
SCSG-CYBER@SG.SC.GOV

Cyber is tough. We are here to help.

G-2 offers free consulting services to qualifying state and local agencies and government-affiliated organizations in South Carolina. The services list* below provides an overview of what we could do to help you:

- Security, Risk, & Compliance Assessments
- Intelligence & Threat Modeling
- Security & Resiliency Strategy
- Cyber Security Awareness Training
- Incident Response & Recovery

*If your needs are not included in this list please let us know – we would be happy to discuss custom solutions for your organization.

SC STATE GUARD CYBER TEAM

The South Carolina State Guard has a long history of service to our state and country. As cyber actors become more prevalent it is important for the State Guard to be able to assist state and local agencies. We have put together a team of highly qualified professionals to provide that assistance.

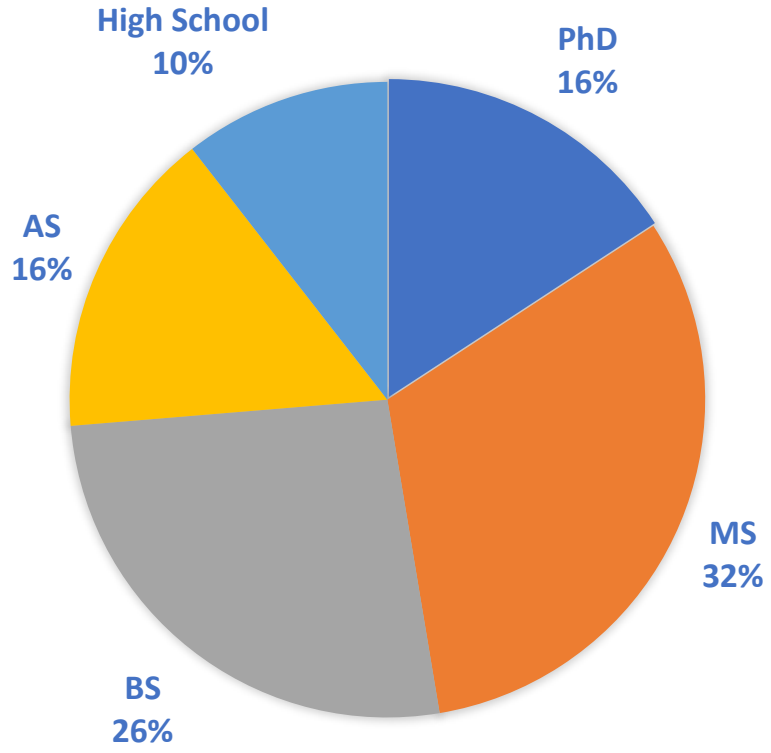
SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Annex A Cont.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Annex B

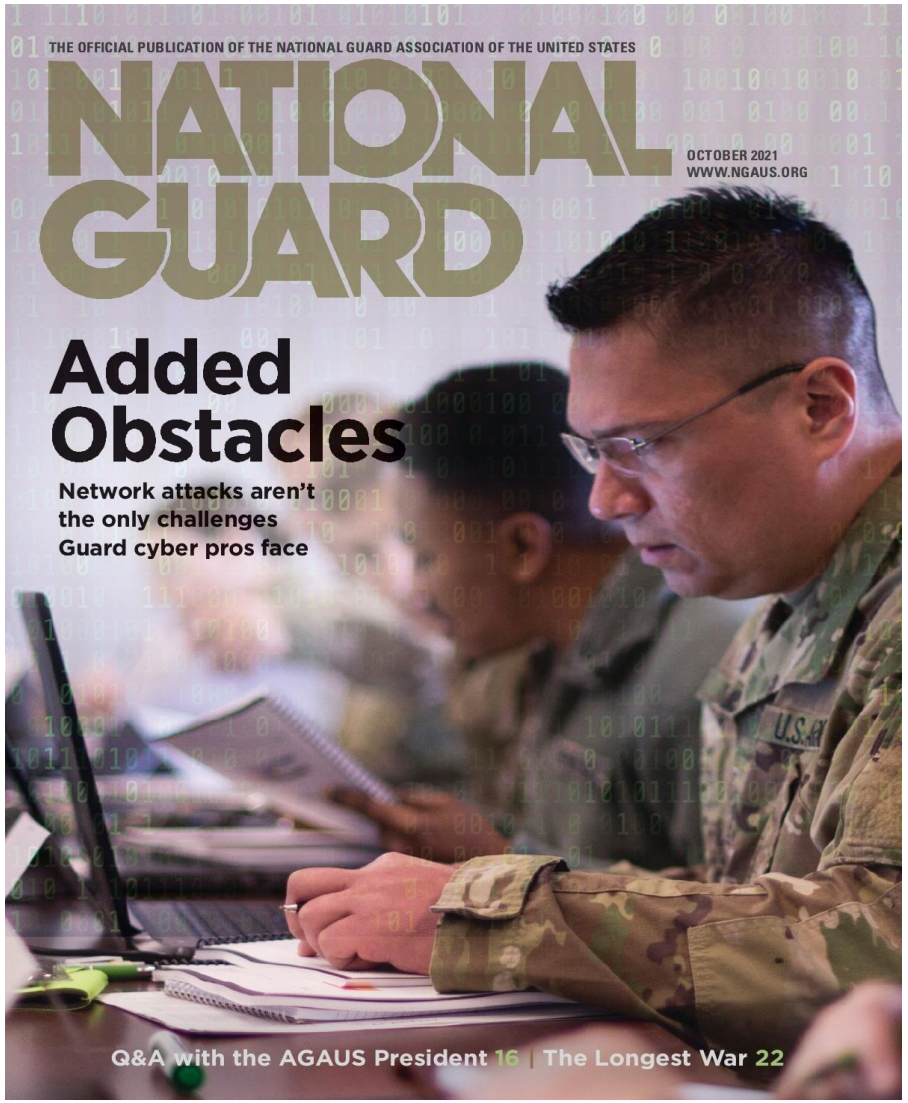
Total Cyber Team Members	**19**
Combined Total Cyber Events Responded to	200+ Cyber Events
Total years of Information Technology experience:	307 years
Combined Total Unique Certifications	79
Total Cyber Team Members with DoD Clearances	4

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit
Annex C

SCSG CYBER TEAM EDUCATION LEVEL



SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit



SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit

ADDED CYBER CHALLENGES

Guard's talented net defenders are often hindered by vague laws, unneeded training requirements

BY DREW BROOKS

KEYSTROKES Members of the South Carolina National Guard Defense Cyber Optic Element participate in last summer's Cyber Shield 21, the Defense Department's largest annual unclassified cyber-defense exercise.

IN A YEAR in which National Guard soldiers and airmen have battled wildfires, picked up after hurricanes, secured the U.S. Capitol and vaccinated millions of Americans against COVID-19, the Guard cyber mission has largely flown under the radar.

But that isn't due to a lack of cyberattacks or Guard responses.

"America's power plants, food supply, water supply, health care, law enforcement and defense sectors have all come under attack," Gen. Daniel R. Hokanson, the chief of the National Guard Bureau, said in June. "These cyber threats extend our adversaries' reach across borders and time zones, and it could have devastating consequences."

Hokanson said there have been attacks in every U.S. state. And while the Guard has not responded to every assault, it often plays a role in helping to strengthen vulnerable state and local networks.

"We have emerged as a trusted and valuable resource in helping our local, state and federal partners defend and mitigate against cyberattacks," he said.

The growing frequency of such attacks have slowly captured the public's attention. Most have impacted limited populations — a single town or branch of a municipal government. But when an attack on the Colonial Pipeline caused gas shortages from Washington, D.C. to Florida earlier this year, the nation began to pay closer attention, says Maj. Gen. Johanna Clyborne, the chair of the NGAUS task force on cyber issues.

Clyborne is dual-hatted as assistant adjutant general for Minnesota and deputy commanding general of the Army Cyber Center of Excellence at Fort Gordon, Georgia. She assumed her NGAUS duties earlier this year.

She says high-profile cyberattacks have raised concerns for local leaders, who in turn have looked to the Guard for help, much as they have throughout the force's history.

"The Guard is best known for responding to floods, riots and natural disasters, but it's also uniquely positioned to help at the state and local level for cyber defense," Clyborne says.

While election security has garnered much of the headlines for the Guard's cyber force in recent years, she notes the Guard has also responded to attacks on government websites and other critical infrastructure, with missions increasing as states develop how to best deploy their cyber personnel.

Speaking earlier this year, Lt. Gen. Jon A. Jensen, the Army Guard director, noted that much of the Guard's cyber force structure was still maturing, with some states relying on "ad hoc units with ad hoc capability."

Despite that, the nation has clearly recognized the "untapped capability" of the Guard in the nation's cyber defenses, he said.

As of October, three Guard cyber teams were conducting cybersecurity missions on behalf of their states, while others were also deployed on Title 10 (federal) status in support of U.S. Cyber Command.

Overall, the Guard's cyber force includes 3,900 service members in 59 cyber units across nearly 40 states. But every state and territory has some capability.

The dual nature of the Guard along with its large number of soldiers and airmen with civilian-acquired cyber skills makes it uniquely qualified to provide cyber support. But it has also led to numerous issues and questions over gray areas that currently exist in state and federal laws and regulations written well before the term "cyber" was commonplace.

Unlike other state responses, the cyber mission cannot be treated as a natural disaster where the force responds to an act of nature. Instead, it must be an ongoing security operation.

"It's been pretty clear we have folks who have the needed skillsets who can be incredible assets to their states," Clyborne says. "But some states have struggled with how best to leverage those assets due to differing laws."

NGAUS, the Adjutants General Association of the United States and the nation's governors have been working with federal authorities to ensure that Guardsmen can conduct both preventative and response cyber missions in their home states in a Title 32 (state) status.

Pending legislation in the Senate would help. Sponsored by Sen. Maggie Hassan, D-N.H., and Sen. John Cornyn, R-Texas, it would make clear that states are authorized to use the Guard to provide cyber support services to states and localities.

Meanwhile, the Guard continues to invest in cyber capabilities, with cyber training ranges in several states, partnerships with universities and local and state government IT offices, and large-scale cyber training exercises.

> **"The Guard is ... uniquely positioned to help at the state and local level for cyber defense."**
>
> **—Maj. Gen. Johanna Clyborne**
> Minnesota Army National Guard
> Chair, NGAUS Cyber Task Force

NGAUS believes the Guard should continue to be a critical partner in planning, developing and executing strategy within the cyber domain. The association has lobbied Capitol Hill for several initiatives that would improve the cyber training pipeline, better allow the Guard to be a conduit for cyber operations between federal, state and local governments and the private sector, and to add full-time staffing for defensive cyber operations.

Some of those issues were raised in early October, when Jensen, the Army Guard director, hosted a panel of Guard leaders to talk about a range of Army issues during the annual meeting of the Association of the U.S. Army in Washington, D.C.

Col. Daniel Lister, the chief information officer for the Idaho National Guard, said the Guard's typical bonuses and incentives, such as college tuition, can't compete with what's offered in the private sector.

Instead, he urged Army leaders to consider unconventional incentives and benefits while fostering an environment where soldiers can apply their cyber skills while also innovating and developing new processes that can benefit the Guard and nation.

"Cyberspace is another fighting domain, and we as an Army need to be completely agile in being able to develop and leverage IT methodologies to transform in to a more agile and software-enabled force," he said. "We have an immense amount of knowledge, experience and skills in the National Guard that allow us to develop technologies and capabilities we can put out to the force."

Much of that knowledge is civilian-acquired, which is not formally recognized by the U.S. military.

"We do enjoy folks coming to the National Guard that arrive with all kinds of certifications, but what we end up doing is telling them they have to go to school to get certified in the skills they already have," said Maj. Gen. Laura L. Yeager, the commander of the 40th Infantry Division and the California Army Guard. "That's additional time away from their families and employers."

Clyborne says Guard cyber leaders are hoping Army and Air Force officials will begin to recognize and give credit for those civilian skillsets. Limiting time away from civilian jobs and families will be a recruiting and retention asset, she says.

Officials are also pushing for incentive pay for cyber professionals, similar to what military pilots receive for their unique skillsets.

Lister, the Idaho Guard leader, said the Guard must look at its cyber force differently than it has in the past in order to avoid losing Guardsmen to better pay and benefits in the private sector. Instead of leaning on its soldiers' and airmen's civilian skillsets, he said, it must strive to bolster them with training that could help them prosper out of uniform.

"Training should be relevant to what they're experiencing out in their civilian careers," he said. "They should gain knowledge and skills within military service that can be applied to their careers outside."

The author can be reached at drew.brooks@ngaus.org.

SOUTH CAROLINA STATE GUARD
G-2 Cyber Unit

Questions?