COLORADO NATIONAL GUARD CYBER

Information Brief

As of 15 APR 2016
• What is the Colorado National Guard?
• Evolution into the Cyber Battlefield
• Colorado National Guard Cyber Capabilities
  – Mission
  – Computer Network Defense Team (CND-T)
  – Cyber Protection Team (CPT)
  – Civilian Education & Certifications
• Cyber Partnerships and Exercises – Past, Present, and Future
Federal Mission: To provide trained units available for active duty in time of war or national emergency, and at such other times as the national security may require.

State Mission: To provide military support to Civil Authorities and respond to State emergencies; to provide support to law enforcement in counter-narcotics.
In Every War...

State units have been in every major war we fought, from the Revolution through Iraq & Afghanistan
A Disturbing Trend
UNCLASSIFIED//FOUO

Hybrid-Warfare

Cyber Crime

Threats from Nation States

Terrorism

Cyber Threats & Exploitation

Homeland

Regional Expansion
Mission

CPT: The **Cyber Protection Team** is a unit capable of evaluating and acting in response to unforeseen and dynamic cyber situations, defending against hostile action and imminent cyber threats, and conducting cyberspace operations to deter, disrupt, and defeat adversary’s in cyberspace operations.

CND-T: Primary mission of the **Computer Network Defense Team** is to defend the National Guard Network and can also be called upon by the Governor to assist in the event of an incident.

“A cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.”
Leon Panetta, Oct 2012
Colorado National Guard Cyber Teams

**CPT**
- Size: 39 personnel (Colorado, Utah, North Dakota, and South Dakota)
- Authority: Title 10, Title 32, and State Active Duty (SAD)
- Deployable: Yes

**CND-T**
- Size: 10 personnel
- Authority: Title 32 and State Active Duty (SAD)
- Deployable: No, it is a non-deployable first responder asset for the Governor or TAG in the event of a cyber emergency
FY17 Teams (stand up in FY16)
CPT 170 - Georgia (Approved TDA)
CPT 171 - California (Approved TDA)
CPT 172 - Ohio - Michigan - Indiana (Approved TDA)

FY18 Teams (stand up in FY17)
CPT 173 - New York - New Jersey
CPT 174 - Colorado - North Dakota - South Dakota - Utah
CPT 175 - Alabama - Kentucky - Tennessee
CPT 176 - Illinois - Wisconsin

FY19 Teams (stand up in FY18)
CPT 177 - Minnesota
CPT 178 - Texas - Louisiana - Mississippi
CPT 179 - Nebraska - Missouri - Arkansas
NOTE:
- Filled: 313 of 413 Personnel (76%)
- Total FY 16: 413 Personnel Authorized
- Current as of: 04NOV15 (FY16 documents)
Industry Certified

- Security +
- C|EH
- CISSP
- CCNA Security
- GSEC
- CASP
- CISM

ADDITIONAL CPT TRAINING:

- JACWC Joint Advanced Cyber Warfare Course
- JNAC Joint Network Attack Course
- Critical Thinking and Structured Analysis (CTSA or equivalent) DIA
- Introduction to TAC
- Analyst's Notebook Familiarization Course
- Analyst's Notebook: Customization and Analysis
- Introduction to PALANTIR
- Cyber Threats Detection and Mitigation
- Basic Cyber Adversary Awareness
- Internet Technologies
- CNE Bootcamp
- Cyber Attack and Defend
- Capabilities Developer's Course
- Cyber Threats Detection and Mitigation
- Certified Ethical Hacker
- Malicious Network Traffic Analysis
- Cyber Operator Training Course (COTC)
- Intermediate Cyber Core
Leveraging Partnerships for Incident Response
Key partnerships are instrumental in testing and improving our response to cyber events.

January 2016
- OIT conducted a technical cyber exercise with Colorado National Guard, Regis University, CIAC, Cyber Task Force, and other industry and academic partners.

October 2015
- OIT led a simulated healthcare data exposure exercise to exercise our response plan.
- Participants included: Connect for Health Colorado, HCPF, CDHS, and Deloitte.

July 2015
- OIT completed a simulated cyber exercise with the Colorado National Guard as part of a broader state emergency response exercise, Vital Connection 2.

August 2014
- OIT completed a combined simulated cyber attack exercise with members of the incident response team, the Colorado National Guard, and Regis University to practice hands-on response to cyber event.
• Date(s): 20-21 August 2016 (7AM-4PM)
• Location: Regis University, Greenwood Village Campus
• Two Tracks:
  – US Army REDCOM Cyber Sustainment Training: Cyber Forensics
    • Participants will have both lecture and hands on via distance learning connectivity
      (7AM-3PM on Saturday and 7-11AM on Sunday)
  – Winter X-Games Power Outage (caused by malicious cyber actors)
    • Building on Threat Intelligence from the ISAO-Sports and 2016 Summer Olympics,
      participants will gain an understanding of current threats, signatures, and vulnerabilities
    • Additionally, we are planning to incorporate an ICS/SCADA “power” exploit based on
      the Threat Intelligence related from the Olympics that demonstrates the impact of a
      cyber incident at the Winter X-Games in Colorado
  – To enhance training and realism, we recommend participants sign up for free Threat Connect
    (www.threatconnect.com) accounts prior to the exercise to better understand Threat Intelligence
Closing Remarks...
QUESTIONS?