The Civilian/Military Response Interface

- The Department of Defense is always in support of civilian authorities
  - The Colorado National Guard is the first military responder for Colorado

- The Department Of Defense provides Defense Support of Civil Authorities when:
  - Civilian resources have been exceeded
  - A civilian capability does not exist
  - Always based on a request for support from some civilian authority
Capabilities

Per the Colorado State Emergency Operations Plan – the National Guard is a supporting agency for all Emergency Support Functions with the exception of Long Term Community Recovery and Mitigation.

National Guard capabilities revolve around ten major components – “The Essential Ten”.

- Command and Control
- Aviation
- Security
- Engineering
- Maintenance
- Transportation
- CBRN(E)*
- Logistics
- Medical
- Communications
Concept of Support

**First Response**

- Local/IC
- County/City

**Initial Attack**

- DoD in IRA
- OEM/SCO
- County/City

**State Level Emergency**

- OEM
- EMAC
- County/City
- DoD in SAD
- JTF-State

**Federal Level Emergency**

- DoD
- FEMA
- Dual Status Command
- State/EMAC
- Fed Agencies

**Mutual Aid**

- Mutual Aid
- DoD in IRA

**Contract**

- DoD in IRA
- OEM
- County/City

**Specialized Expertise**

- DoD
- FEMA
- JTF-State
- Fed Agencies

**Concept of Support**
CPT / DCO-E Comparison

- Cyber Protection Team (CPT) → threats
- Defensive Cyber Operations-Element (DCO-E) → vulnerabilities (CNDSP*)
**CONG Cyber Task Force Packages**

The Colorado National Guard task organizes its cyber forces to provide flexible and adaptable capability to the Governor in order to meet his needs:

**Vulnerability Assessment Package**
- 2-3 Soldiers
- Threat and vulnerability assessment
- Unclassified adversary tactics, techniques, and procedures
- Situation Awareness and Information Sharing
- Training and education

**Advise and Assist Package**
- 2-4 Soldiers
- Cyber analysis capabilities to include forensic examination of networks and systems
- Unclassified adversary tactics, techniques, and procedures
- Situation Awareness and Information Sharing
- Infrastructure support and network monitoring
- Training and education

**Large Vulnerability Assessment Package**
- 6-10 Soldiers
- Threat and vulnerability assessment
- Unclassified adversary tactics, techniques, and procedures
- Situation Awareness and Information Sharing
- Infrastructure support and network monitoring
- Incident response, mitigation, and recovery
- Training and education
- Perform tasks to determine root cause of cyber attacks
## Colorado Critical Infrastructure Identified Life Safety Implications During Cyber Incidents

<table>
<thead>
<tr>
<th>Sector</th>
<th>Life Safety Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water and Waste Water</td>
<td>Lifeline sector *</td>
</tr>
<tr>
<td>Energy</td>
<td>Lifeline sector *</td>
</tr>
<tr>
<td>Communications</td>
<td>Lifeline sector *</td>
</tr>
<tr>
<td>Transportation</td>
<td>Lifeline sector *</td>
</tr>
<tr>
<td><strong>Government</strong></td>
<td>At risk populations likely depend on timely and accurate access to government services for their basic needs.</td>
</tr>
<tr>
<td>Emergency Services</td>
<td>This sector is primarily used to ensure life safety of the population. Loss of access to or use of cyber capabilities could significantly impact essential services.</td>
</tr>
<tr>
<td>Healthcare and Public Health</td>
<td>This sector is directly responsible for life saving care of the population. It relies heavily on access to IT infrastructure to provide essential services. Loss of access to IT infrastructure and data significantly impacts care during cyber incidents.</td>
</tr>
<tr>
<td>Chemical</td>
<td>Manufacturing processes in the chemical sector rely on secure IT operation to safely handle feed stock and to complete chemical manufacturing processes. These operations can pose a substantial danger to local populations if exposed to a cyber attack.</td>
</tr>
<tr>
<td>Dams</td>
<td>Physical dam operation can expose downstream populations to significant volumes of water and create a life threatening situation if not done with proper care and coordination. Automated dam controls exposed to a cyber attack could create this life threatening situation.</td>
</tr>
</tbody>
</table>

Lifeline sectors are specifically called out in the National Infrastructure Protection Plan 2013 as being essential to the operation of most critical infrastructure sectors. Cyber impacts to this sector are assumed to have the potential for negative impact on life safety.