South Carolina National Guard

Defensive Cyber Operations Overview

MAJ Britton Plath

16 February 2023

Cyber Response Overview

- Cyber Response Types
- Cyber Response Request Flow Chart
- Authorities
- SCNG Cyber Incident Management Synchronization Diagram
- Developing SOP’s
- Collective Training
- Engaging the community

Cyber Response Types

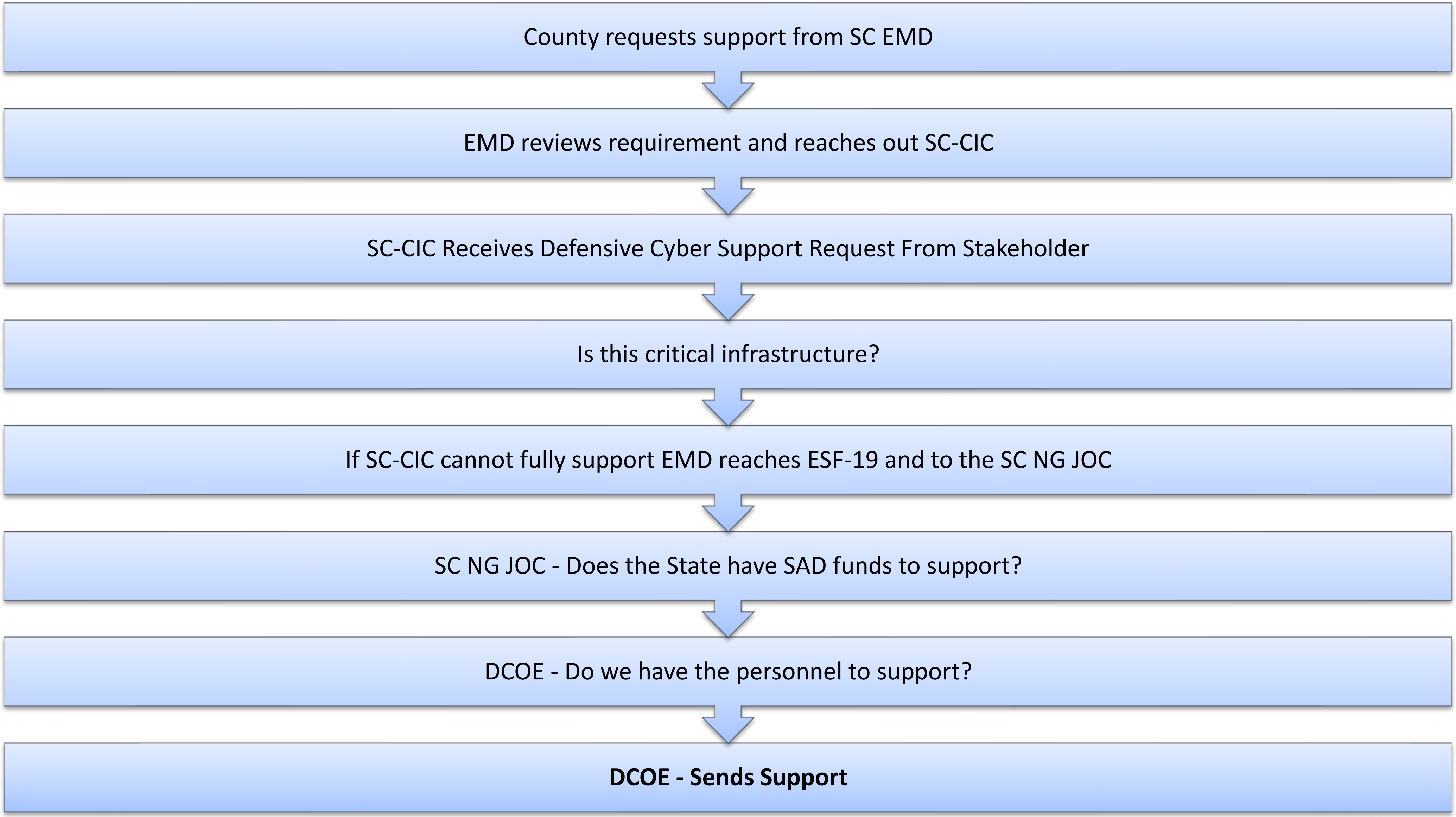
Defensive Cyber Operations defined: Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems**.**

Performing analysis and forensics on IT systems to determine what has been infected and mitigating it if possible. Recovering data if possible, to allow resumption of operations. **We can support our state's stakeholders.**

Offensive Cyber Operations defined: Offensive cyber operations are the latest incarnation of intangible warfare–conflict waged through non-physical means, such as the information space or the electromagnetic spectrum. Attacking a Cyber Attacker.

We can't perform Offensive Cyber Operations since this is for deployed Cyber Defenders on Title 10 only and that our state responses can only be Defensive Cyber support.

Cyber Response Request Flow Chart



County requests support from SC EMD

EMD reviews requirement and reaches out SC-CIC

SC-CIC Receives Defensive Cyber Support Request From Stakeholder

Is this critical infrastructure?

If SC-CIC cannot fully support EMD reaches ESF-19 and to the SC NG JOC

SC NG JOC - Does the State have SAD funds to support?

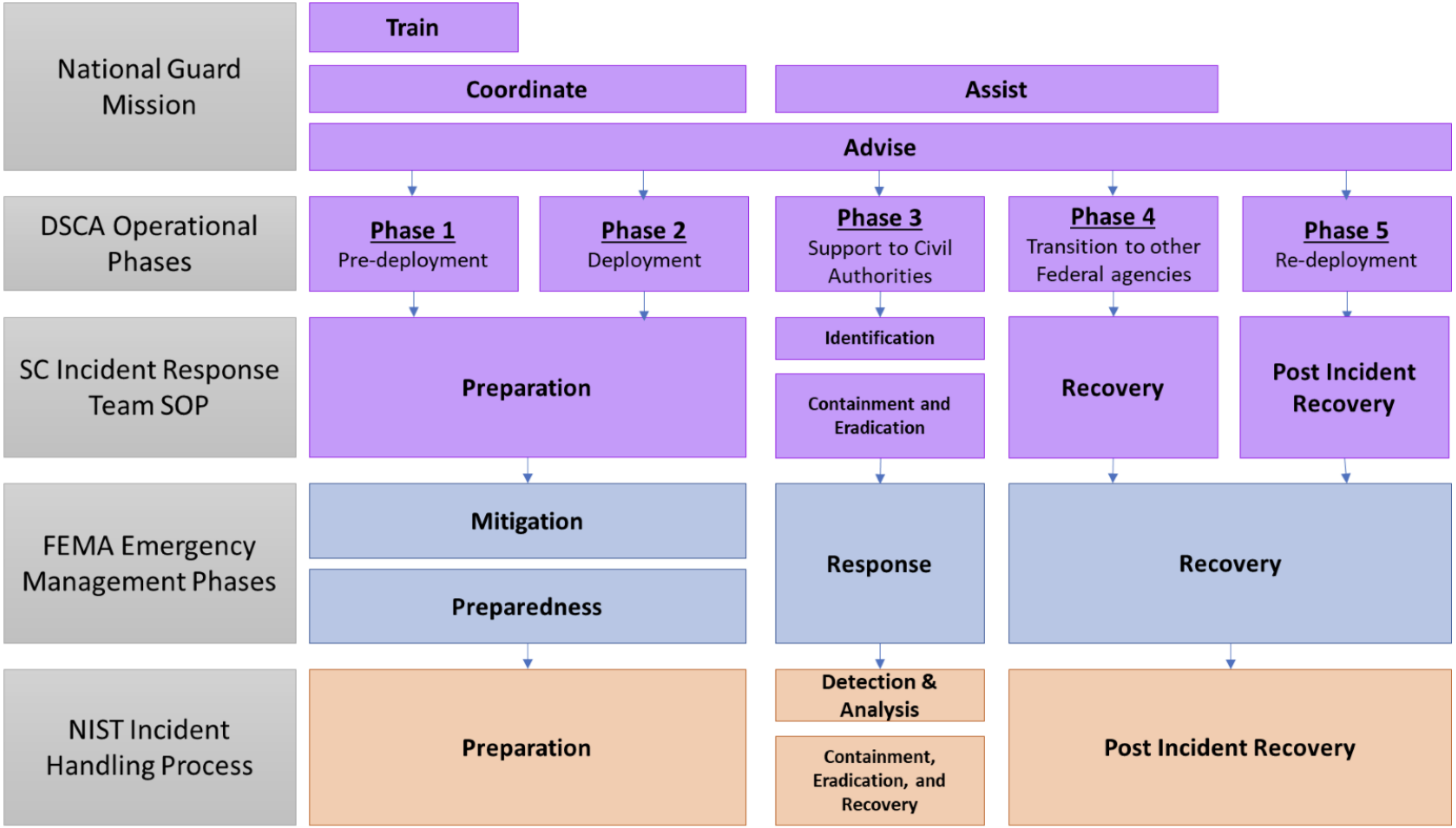
DCOE - Do we have the personnel to support?

DCOE - Sends Support

Authorities

- Title 32
  - Must have a MOU / MOA prior to performing services in a Title 32 status.
  - Actions can be performed under Immediate Response Authority within the first 72 hours.
  - Coordinate, Train, Advise, Assist (CTAA)
  - May “consult” with government entities and public and private utilities, critical infrastructure owners.
- State Active Duty (SAD)
  - SC Code of Laws 25-1-360(16), by TAG approval, with the consent of the Governor, may order volunteers from the National Guard to state active duty for no more than fifteen days provided that funding for pay and allowance funds, as provided in Section 25-1-2200, are available to the Adjutant General without additional state appropriations.
  - Operations will be conducted in SAD status supporting SLED’s South Carolina Critical Infrastructure Cybersecurity (SC-CIC) efforts.
  - Prior to the start of any mission MOU/MOA will be required to define the scope.

SCNG Cyber Incident Management Synchronization Diagram



National Guard Mission	Train				
	Coordinate		Assist		
	Advise				
DSCA Operational Phases	**Phase 1** Pre-deployment	**Phase 2** Deployment	**Phase 3** Support to Civil Authorities	**Phase 4** Transition to other Federal agencies	**Phase 5** Re-deployment
SC Incident Response Team SOP	Preparation		Identification Containment and Eradication	Recovery	Post Incident Recovery
FEMA Emergency Management Phases	Mitigation Preparedness		Response	Recovery	
NIST Incident Handling Process	Preparation		Detection & Analysis Containment, Eradication, and Recovery	Post Incident Recovery	

Developing Playbooks for Incident Response Missions

- Ransomware
- Malware
- Web Applications
- Networks
- ICS / SCADA
- Cloud
- Forensics
- Communications infrastructure (mobile, TV, radio)

Cyber Collective Training

Sep 22 - ICS / SCADA training (Completed at Dominion)

Oct 22 - Forensics/Malware

Nov 22 - Incident Response Handling

Feb 23 - Legal / SANS Holiday Hack Challenge Review

May 23 - Security Onion

July 23 - Network Monitoring

Aug 23 - Firewalls

Sep 23 - Exercise (8 hours)

Key: Green=Completed

Industry and Government Partners

- Government:
  - SC National Guard
  - SC State Guard
  - SLED South Carolina (SC) Critical Infrastructure Cybersecurity (CIC)
  - Department of Revenue
  - US Secret Service
  - FBI
  - DHS
  - NIWC
  - DOE

- Industry:

  SC CIC Program Partners

  Per the U.S. Department of Homeland Security - The 16 critical infrastructure and key resources (CIKR) sectors are:

  - Chemical
  - Commercial facilities
  - Communications
  - Critical manufacturing
  - Dams
  - Defense industrial base
  - Emergency services
  - Energy
  - Financial services
  - Food and agriculture
  - Government facilities
  - Healthcare and public health
  - Information technology
  - Nuclear reactors, materials, and waste
  - Transportation systems
  - Water and wastewater systems

Current SC Cyber Academic Engagements

- University of South Carolina (Columbia)
- University of South Carolina Aiken
- University of South Carolina Beaufort
- The Citadel
- Clemson University
- Francis Marion University
- South Carolina State University
- Morris College
- ECPI University

Questions?