EMAC Committee

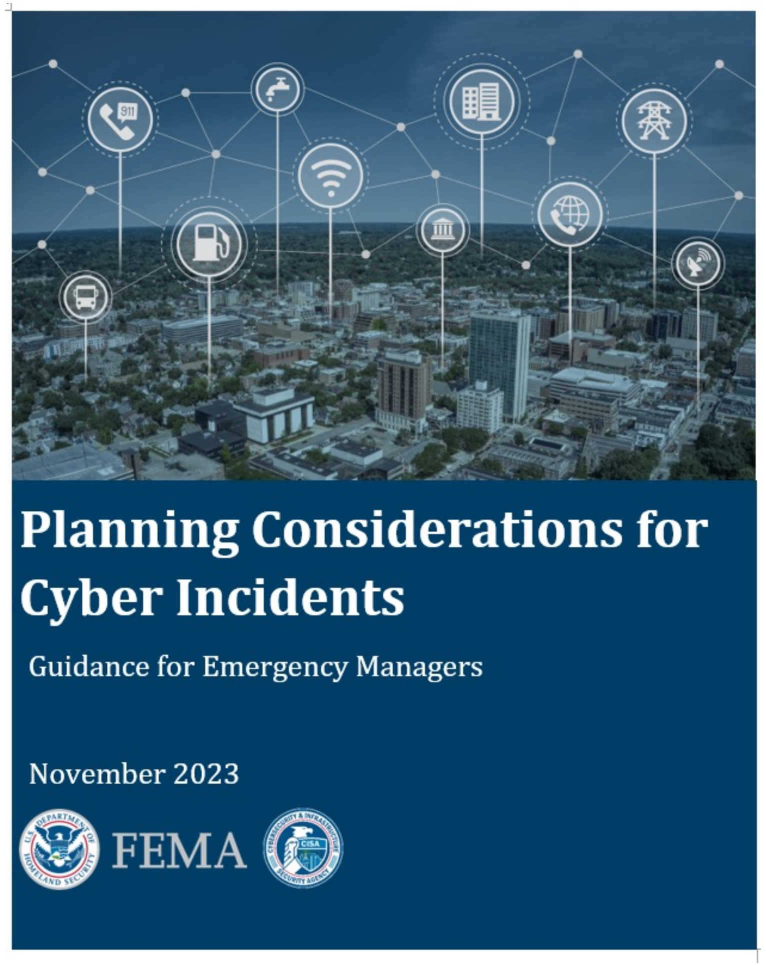
1974 · 2024 NEMA®

National Integration Center Cyber Guidance and Training Update

John Ford, Director, National Integration Center | March 2024

Planning Considerations for Cyber Incidents

- Developed in coordination with the Cybersecurity and Infrastructure Security Agency (CISA)
    - □ Planning Considerations for Cyber Incidents: Guidance for Emergency Managers
    - □ Overview (two-pager)
    - □ Critical Cyber Asset Identification and Prioritization Checklist
    - □ YouTube video highlighting the role emergency managers may play in planning for cyber incidents
- Supports emergency managers in understanding, preparing for, and executing their roles and responsibilities related to cyber incidents



Planning Considerations for Cyber Incidents

Guidance for Emergency Managers

November 2023

FEMA

Why a Planning Considerations for Cyber Incidents Guide?

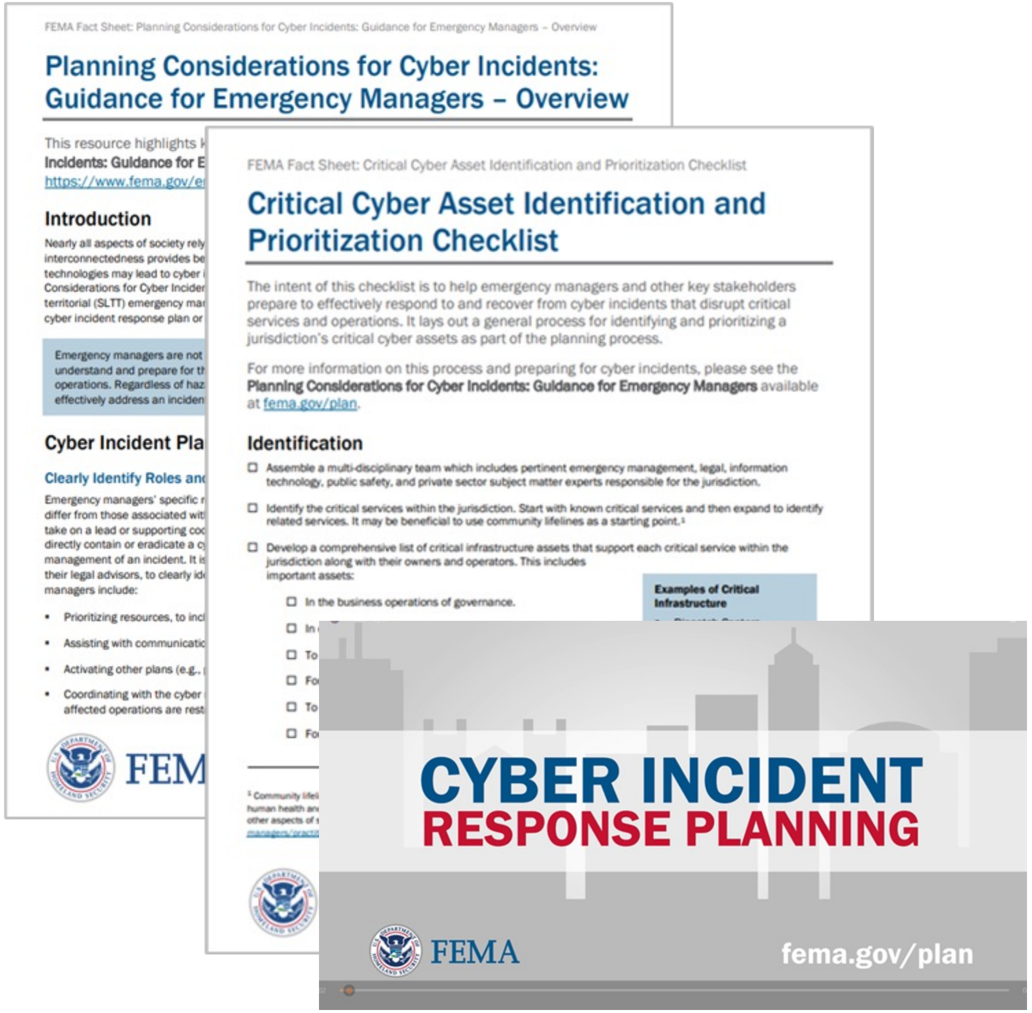
- Developed in response to needs identified in:
  - Annual Threat and Hazard Identification and Risk Assessments
  - Stakeholder Preparedness Reviews
  - Requests from prior public engagement sessions
- Lessons learned from past exercises and events:
  - Provide more clarity on emergency manager roles and responsibilities for a cyber incident
  - Improve communication and coordination of information and planning among cyber practitioners, emergency managers and other key stakeholders to facilitate timely and effective decision-making

2022 THIRA/SPR Analysis for Cyber Plan Update Capability Targets:

- 69% of communities reported that addressing capability gaps or sustainment needs are a high priority
- 80% of communities reported a Planning capability gap
- 80% of communities reported a Training capability gap

Guide and Supporting Materials Content

- The Planning Considerations for Cyber Incidents guide and supporting material include:
  - □ How to use the six-step planning process to develop cyber incident plans
  - □ Potential emergency management roles and responsibilities
  - □ Considerations for key stakeholder engagement and communications strategies
  - □ Common types of cyber incidents and how to assess and prioritize risks
  - □ Information on additional resources



FEMA Fact Sheet: Planning Considerations for Cyber Incidents: Guidance for Emergency Managers – Overview

Planning Considerations for Cyber Incidents: Guidance for Emergency Managers – Overview

This resource highlights k
Incidents: Guidance for E
https://www.fema.gov/e

Introduction

Nearly all aspects of society rely
interconnectedness provides be
technologies may lead to cyber
Considerations for Cyber Inciden
territorial (SLTT) emergency mar
cyber incident response plan or

Emergency managers are not
understand and prepare for th
operations. Regardless of haz
effectively address an inciden

Cyber Incident Pla

Clearly Identify Roles and

Emergency managers' specific r
differ from those associated wit
take on a lead or supporting coo
directly contain or eradicate a c
management of an incident. It is
their legal advisors, to clearly id
managers include:

- Prioritizing resources, to incl
- Assisting with communicatio
- Activating other plans (e.g.,
- Coordinating with the cyber
affected operations are rest

FEM

FEMA Fact Sheet: Critical Cyber Asset Identification and Prioritization Checklist

Critical Cyber Asset Identification and Prioritization Checklist

The intent of this checklist is to help emergency managers and other key stakeholders prepare to effectively respond to and recover from cyber incidents that disrupt critical services and operations. It lays out a general process for identifying and prioritizing a jurisdiction's critical cyber assets as part of the planning process.

For more information on this process and preparing for cyber incidents, please see the **Planning Considerations for Cyber Incidents: Guidance for Emergency Managers** available at fema.gov/plan.

Identification

- □ Assemble a multi-disciplinary team which includes pertinent emergency management, legal, information technology, public safety, and private sector subject matter experts responsible for the jurisdiction.
- □ Identify the critical services within the jurisdiction. Start with known critical services and then expand to identify related services. It may be beneficial to use community lifelines as a starting point.[1]
- □ Develop a comprehensive list of critical infrastructure assets that support each critical service within the jurisdiction along with their owners and operators. This includes important assets:
  - □ In the business operations of governance.
  - □ In
  - □ To
  - □ Fo
  - □ To
  - □ Fo

Examples of Critical Infrastructure

[1] Community lifel
human health an
other aspects of
managers/practi

NIMS Resource Typing: Cyber Security

The NIC, working with Subject Matter Experts from Federal, State, Local, Tribal, and Territorial partners and education entities will review and update the following Resource Types relating to Cyber Security in 2024:

- Computer Network Defense Infrastructure Support Specialist
- Computer Network Defense Analyst
- Cyber Incident Responder
- Cyber Incident Response Team
- Data Administration Specialist
- Digital Forensics Specialist
- Supervisory Control and Data Acquisition Controller Specialist
- Supervisory Control and Data Acquisition Server Specialist

National Cybersecurity Preparedness Consortium

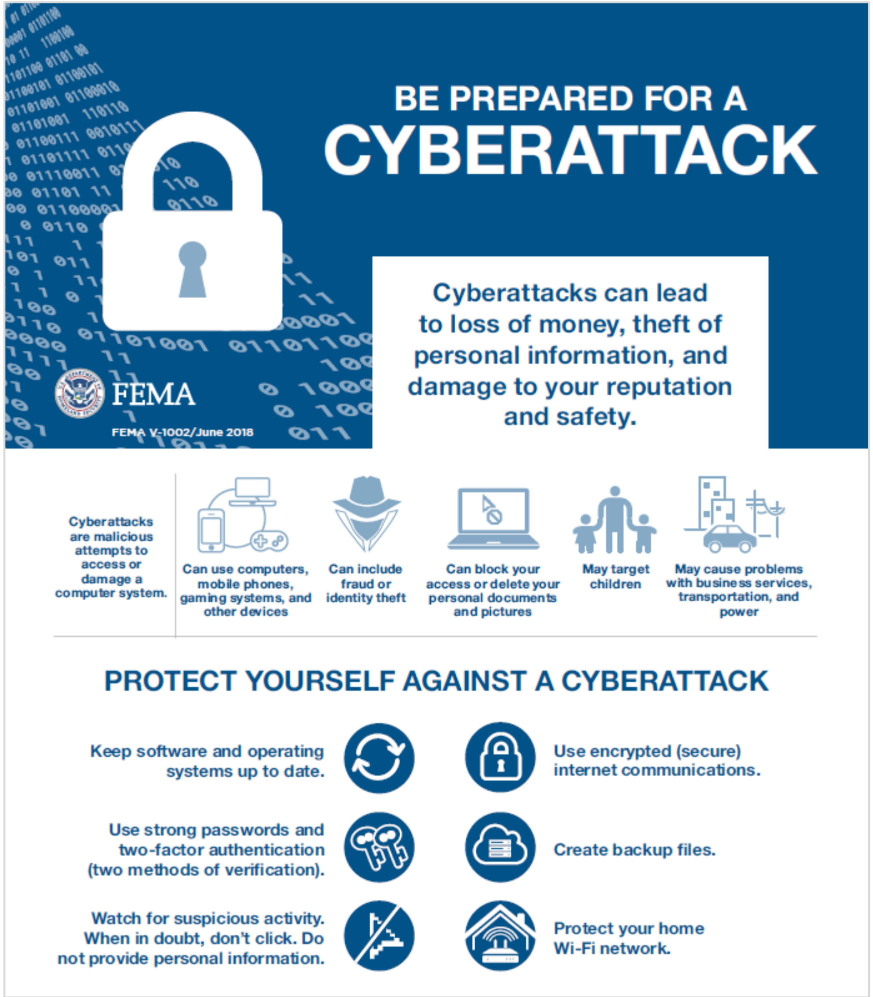
- National Cybersecurity Preparedness Consortium (NCPC)
- Managed by National Training and Education Division's Training Partners Program
- Offers 40 tuition-free, FEMA-certified training courses; additional 19 in development
- For more information, please visit: www.firstrespondertraining.gov
- Cyber Security for Emergency Managers certificate program jointly developed by Emergency Management Institute, CISA, and the National Defense University. Expected completion by the end of the calendar year

NCPC Composition

- Criminal Justice Institute of the University of Arkansas
- University of Texas at San Antonio
- Texas A&M Engineering Extension Service
- Memphis University
- Norwich University Applied Research Institute

Cyberattack Hazard Information Sheet

- Hazard Information Sheet includes information on:
  - □ Preventing a cyberattack
  - □ Limiting damage during a cyberattack
  - □ Reporting the cyberattack
  - □ Additional information about cyberattacks
- Cyberattacks can lead to loss of money, theft of personal information, and damage to your reputation and safety
- For more information, please visit: www.community.fema.gov/ProtectiveActions/s/article/Cyberattack



BE PREPARED FOR A CYBERATTACK

Cyberattacks can lead to loss of money, theft of personal information, and damage to your reputation and safety.

FEMA

FEMA V-1002/June 2018

Cyberattacks are malicious attempts to access or damage a computer system.

Can use computers, mobile phones, gaming systems, and other devices

Can include fraud or identity theft

Can block your access or delete your personal documents and pictures

May target children

May cause problems with business services, transportation, and power

PROTECT YOURSELF AGAINST A CYBERATTACK

Keep software and operating systems up to date.

Use encrypted (secure) internet communications.

Use strong passwords and two-factor authentication (two methods of verification).

Create backup files.

Watch for suspicious activity. When in doubt, don't click. Do not provide personal information.

Protect your home Wi-Fi network.

FEMA

Questions?

John Ford
Director, National Integration Center
John.Ford@fema.dhs.gov

www.fema.gov/plan
https://rtlt.preptoolkit.fema.gov/Public

FEMA

EMAC Committee

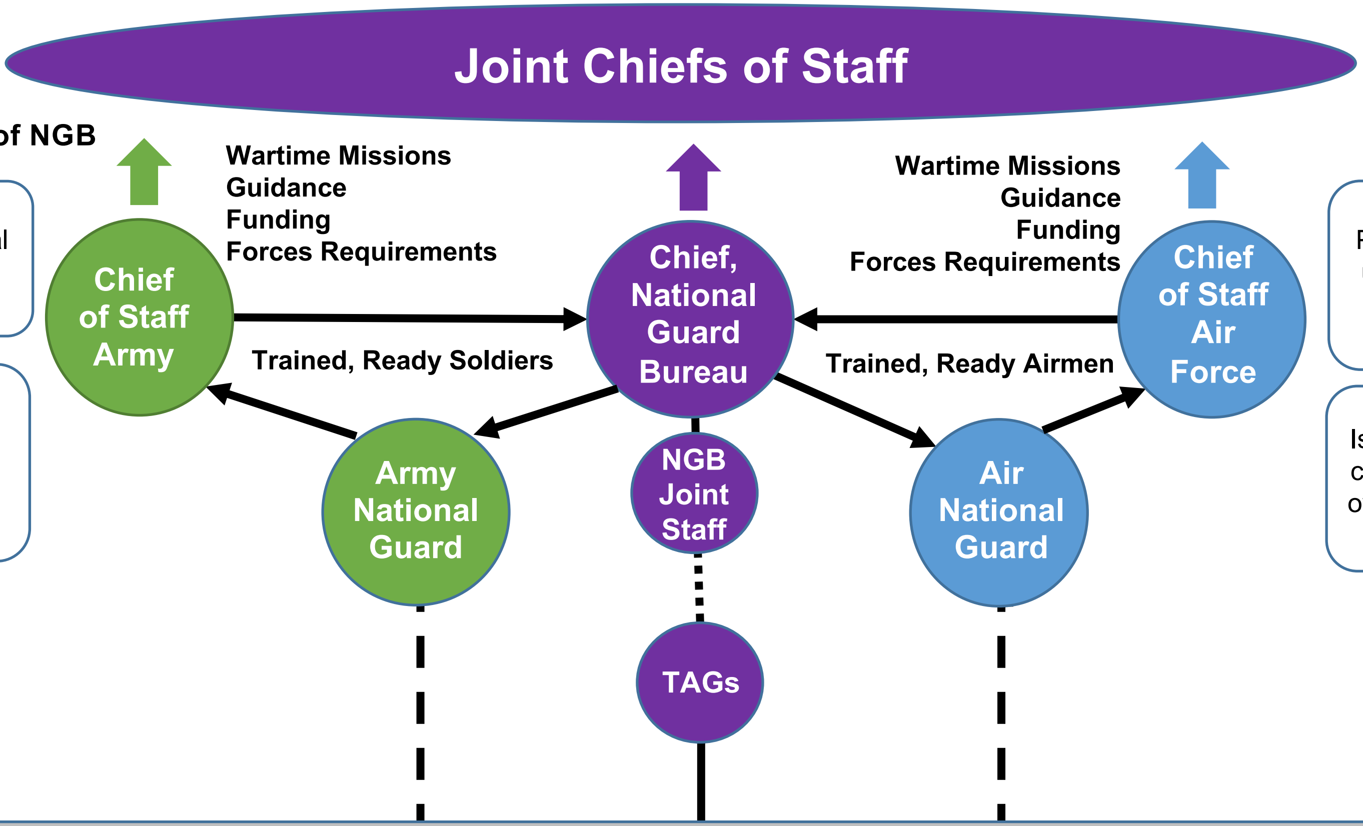
National Guard (NG) Cyber Operations Forces & Capabilities

Mr. Jay Hallam
Cyber Division (NGB-J3/4/7-I Cyberspace Operations)
National Guard Bureau
703-5771-2130
John.w.hallam.civ@army.mil

6 March 2024
Chief, NGB J3/4/7-I
703-607-0895

The NG and National Guard Bureau (NGB)

The Chief, National Guard Bureau (CNGB) is a member of the Joint Chiefs of Staff and principal advisor to the Secretary of Defense, through the Chairman of the Joint Chiefs of Staff (CJCS), on matters involving non-federalized NG forces, and other matters as determined by the Secretary of Defense.



Four Functions of NGB

1. Provide functional staff support to CNGB.

2. Provide situational understanding for CNGB on State NG activities.

3. Is the channel of communications between the DoD and the States.

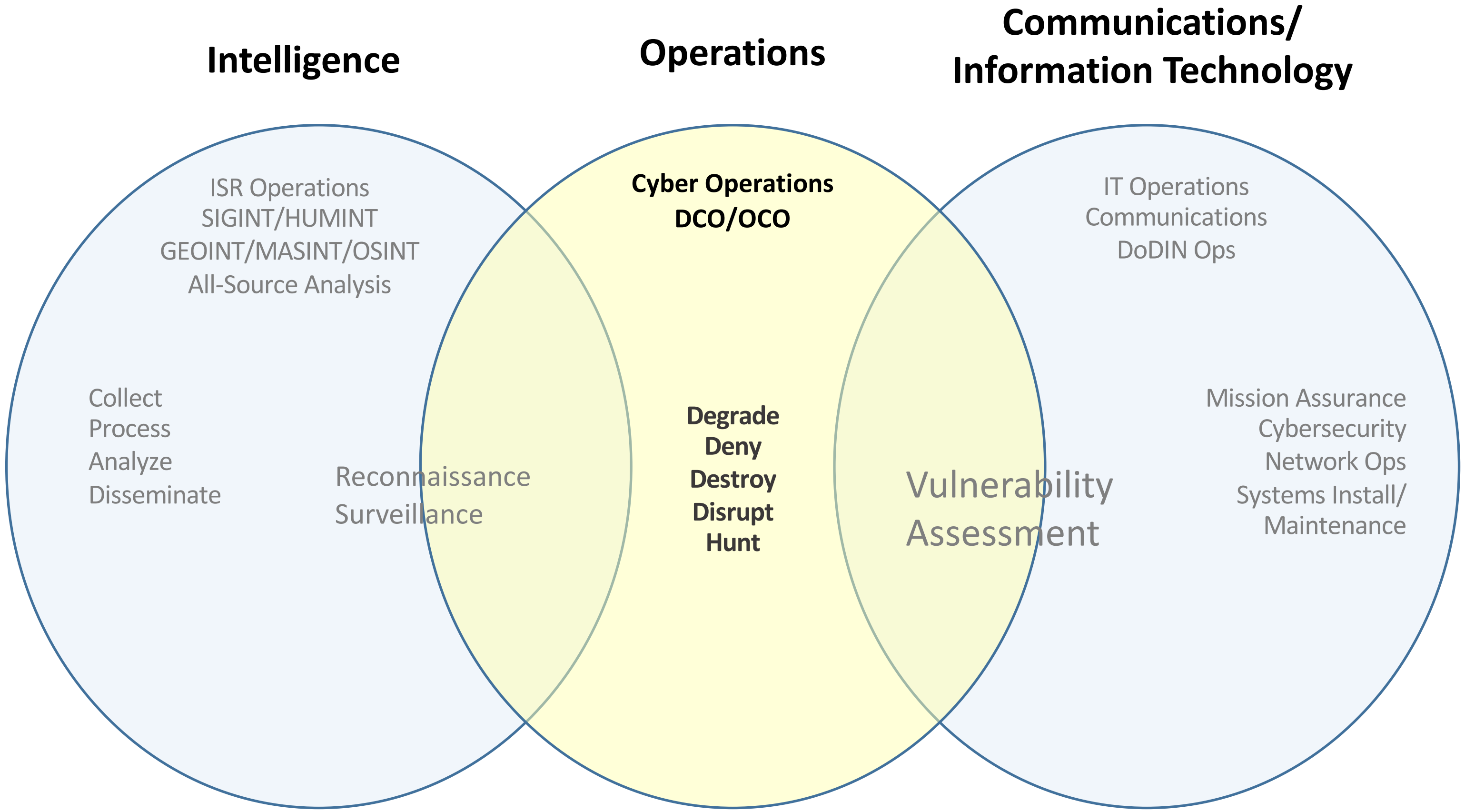
4. Is a Bureau with no command authority over State NG units or forces.

54 States, Territories, and the District of Columbia

"The NG has a unique dual mission that consists of both Federal and State roles: in peacetime, the governor of each respective state or territory commands the NG; when ordered to active duty for mobilization or called into federal service for emergencies, units of the Guard are under the control of the appropriate service secretary."

How do we conceptualize Cyber?

Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems, non-networked devices and associated physical infrastructures



Intelligence

ISR Operations
SIGINT/HUMINT
GEOINT/MASINT/OSINT
All-Source Analysis

Collect
Process
Analyze
Disseminate

Reconnaissance
Surveillance

Operations

Cyber Operations
DCO/OCO

Degrade
Deny
Destroy
Disrupt
Hunt

Communications/ Information Technology

IT Operations
Communications
DoDIN Ops

Mission Assurance
Cybersecurity
Network Ops
Systems Install/ Maintenance

Vulnerability Assessment

NG Cyber Forces Capability

PARTNERSHIPS

Total <u>66</u> National Guard Cyber Units
- 42 States with ~2800 Personnel

- States Mission Partner engagements domestically
- Asset for NGB State Partnership Program (SPP)
- Federal/interagency
- State, Local, Tribal and Territorial (SLTT)

WARFIGHT

ANG (1,819 pax):
- CMF: 2 x CPTs and 1 x NMT support
  - 16 COS supporting 2 x mobilized CPTs
  - 3 COS supporting part of 1 x mobilized NMT
- Other:
  - 3 COG Headquarters
  - 1 x COS Aggressor / Red Team
  - 1 x Operational Support Squadron

ARNG (985 pax):
- 1 x 91st Cyber BDE
  - 5 x Cyber BN Headquarters (1 BN+ mobilized)
  - 5 x Cyber Security Companies
  - 5 x Cyber Warfare Companies
  - 11 x CPTs incl 1 x T32 AGR CPT (MD) providing training support

*** War-fight capabilities can be used for Homeland missions**

HOMELAND

DCO-E: 54 x10 ARNG M-day teams (~540 pax)
- State cyber response for ARNG network
- Surge capacity to assist TAGs & mission partners in
- identifying/defending key cyber terrain

- **Mission Essential Tasks**
- Interface with mission partners (IRT, Exercises)
- Manage cyber incident response (SAD, EMAC, DSCA)
- Warfighting forces available for Homeland when not mobilized

THE NATIONAL GUARD OF THE U.S.
IN WAR
IN PEACE
THE OLDEST MILITARY ORGANIZATION IN THE US
3¢

<u>LEGEND</u>

CMF: Cyber Mission Force
COG: Cyber Operations Group
COS: Cyber Operations Squadron

CPT: Cyber Protection Team
DCOE: Defensive Cyberspace Operations Element
NMT: National Mission Team

Types of NG Cyber Units

Army National Guard

Defensive Cyber:

- **Cyber Protection Teams:** 11 Teams of 39 Soldiers (429 total)
  - defend the DODIN, protect priority missions, and prepare forces for combat
  - *Growth: **CPT-ME Initiative**
- **Cyber Security Companies:** 5 Companies of 22 Soldiers (165 Total)
  - vulnerability assessments, forensics analysis, USCYBERCOM Readiness Inspections, and cybersecurity support.
- **Defensive Cyber Operations Elements:** 54 Elements of 10 Soldiers (540 Total)
  - secure the National Guard portion of DODIN-A (NG) and respond to State cyberspace emergencies as directed by Governor or Adjutant General.

Offensive Cyber:

- **Cyber Warfare Companies:** 5 Companies of 33 Soldiers (165 Total)
  - full spectrum cyber operations support, OPFOR support to exercises, and penetration testing.

Air National Guard

Defensive Cyber

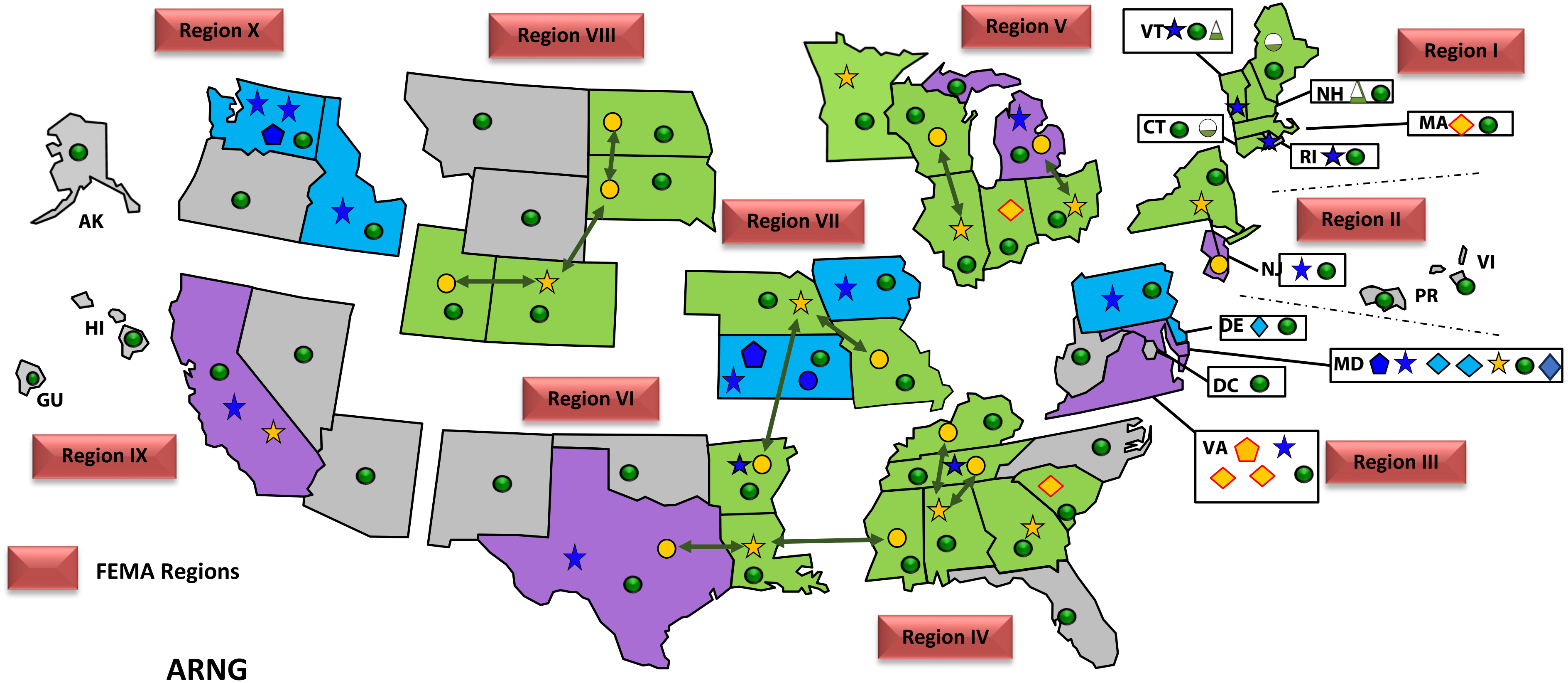
- **Cyber Protection Teams:** 2 Teams of 39 Airmen (78 Total)
  - defend the DODIN, protect priority missions, and prepare forces for combat
  - 16 Cyber Operation Squadrons support CPT Missions totaling 1,136 Airmen

Offensive Cyber

- **National Mission Teams:** 1 Team of 22 Airmen
  - intelligence driven cyber operations against nation-state actors in defense of the nation
  - 3 Cyber Operations Squadrons support NMT Missions totaling 220 Airmen
- **Red Team:** 1 Squadron of 69 Airmen (*Growth: **+ 3**, Pre-decisional)
  - vulnerability assessments of friendly networks in support of Combatant Command and Service requirements
- **Cyberspace Wing:** Cyber-Enabled Air Superiority (CEAS) in OH (Growth: +1 in MD, mission TBD)

Each provides domestic operations capabilities available to their respective States in Title 32 or State Active Duty

NG Cyber Force Layout



ARNG

- ⬟ 1 X ARNG Brigade Headquarters
- ◆ 5 X ARNG Battalion Headquarter
- 5 X Cyber Security Companies
- △ 2 X Cyber Security Company Dets
- 5 X Cyber Warfare Companies
- ◒ 2 X Cyber Warfare Company Dets
- ● 11 X Cyber Protection Teams (CPT)
- ★ 13 X CPT Detachments
- ● 54 X Defensive Cyberspace Operations Elements (DCOE)

Total Operations Force

- 2804 Total NG Cyber Warriors
  - 115 ARNG mobilized supporting USCYBERCOM & ARCYBER
  - 122 ANG mobilized supporting USCYBERCOM & AFCYBER
- ARNG Defensive Cyber Operations Elements in each of the 54

ANG

- ⬟ 3 X Cyber Ops Groups
- ★ 16 X Cyber Ops Squadrons (CPT)
- ◆ 3 X Cyber Ops Squadrons (National Mission Teams)
- ● 1 X Cyber Ops Squadron (Aggressor/Red Team)
- ◆ 1 X Operational Support Squadron

6 March 2024
Chief, NGB J3/4/7-I
703-607-0895

Domestic Operations Support Options

Innovative Readiness Training

- DoD military training opportunity, exclusive to the U.S. & territories
- Joint training opportunities to increase deployment readiness
- Provides key services (health care, construction, transportation, & cybersecurity) with lasting benefits for our communities
- Can be at no cost or OSD funded
- MD and Anne Arundel School District

Emergency Management Assistance Compact

- State-to-State mutual aid compact facilitates the sharing of resources

Defense Support of Civil Authorities

- Federal- agency requests reimbursable support from the DoD emergency or other events
- Potential for National Guard and Federal military equipment for State missions
- Has not been leveraged by Cyber yet

Homeland Defense Activities

- 32 U.S.C. Ch 9…protection of territory or domestic population or of infrastructure…critical to national security
- Three cyber-related HDA requests submitted; none approved by OSD

National Guard Cyber Support Capability

National Guard State Active Duty (SAD)

What is SAD:

- National Guard training or other duty, other than inactive (“drill”) duty, performed under the authority of the Governor of a State.

Cyber Missions performed by National Guard while on SAD:

- The National Guard’s operational mission in terms of cyberspace is to protect critical State infrastructure and respond to cyberspace emergencies as directed by the Governor or The Adjutant General. The National Guard performs this mission in either a *Proactive or Reactive* state.

- **Proactive**:
  1. Cyber Assessment: Environment/Culture/Vulnerability Assessment
  2. Penetration Testing: Ethical Hacking, Document Exploitable Vulnerabilities
  3. Information Sharing: Alerts, Early Warning Notifications
- **Reactive**:
  1. Incident Response: Threat Hunting, Restoration, Recovery
  2. Digital Forensics: Indicators of Compromise, Path of Attack

Contact:

State-specific agency responsible for coordinating cyber support.

Innovative Readiness Training (IRT)

<u>What is IRT:</u>

- A Department of Defense (DoD) military training opportunity, exclusive to the United States and its territories, that delivers joint training opportunities to increase deployment readiness.
- Provides key services (health care, construction, transportation, and cybersecurity) to communities.

<u>Who does IRT apply to:</u>

- Department of Defense (DoD) military & American Communities.

*****May be requested by entities (Federal, regional, state, local, state or federal recognized tribes, and youth & charitable organizations specified in law (32 U.S. Code §508)*****

<u>IRT is not for:</u>

- Missions with no training value to the military unit.
- Law Enforcement.
- Response to natural or manmade disasters.
- Commercial development.

<u>Contact:</u>

Learn more at: http://irt.defense.gov
Questions: osd.irt@mail.mil
Phone: 703-695-7060

6 March 2024
Chief, NGB J3/4/7-I
703-607-0895

Defense Support to Civil Authorities (DSCA)

What is DSCA:

- Federal to federal support and services.
- When a federal agency requests reimbursable support from the DoD for emergency or other events.
- Potential for National Guard and Federal military equipment for State missions.
- Can augment their response through the Emergency Management Assistance Compact (EMAC), which enables State-to-State sharing of Guard forces and equipment.

Approval Requirements:

The use of the National Guard for DSCA requires:

- Receipt of a reimbursable written request (in accordance with the Economy Act) from a federal department or agency or qualifying entity for DoD assistance.
- Selection of the National Guard as the sourcing solution to a Combatant Commander’s request for forces.
- Determination by the Secretary of Defense to approve the use of the National Guard for DSCA to respond to the approved request.

Contact:

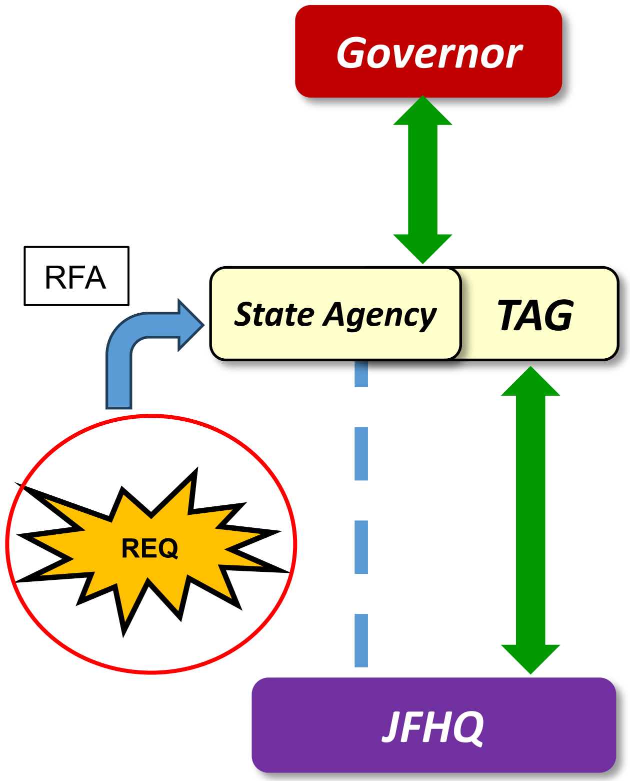
Respective federal agency corresponding to area or sector of concern.

National Guard Cyber Support Request Guide

Process Maps

National Guard State Active Duty (SAD)

**Non-reimbursable*

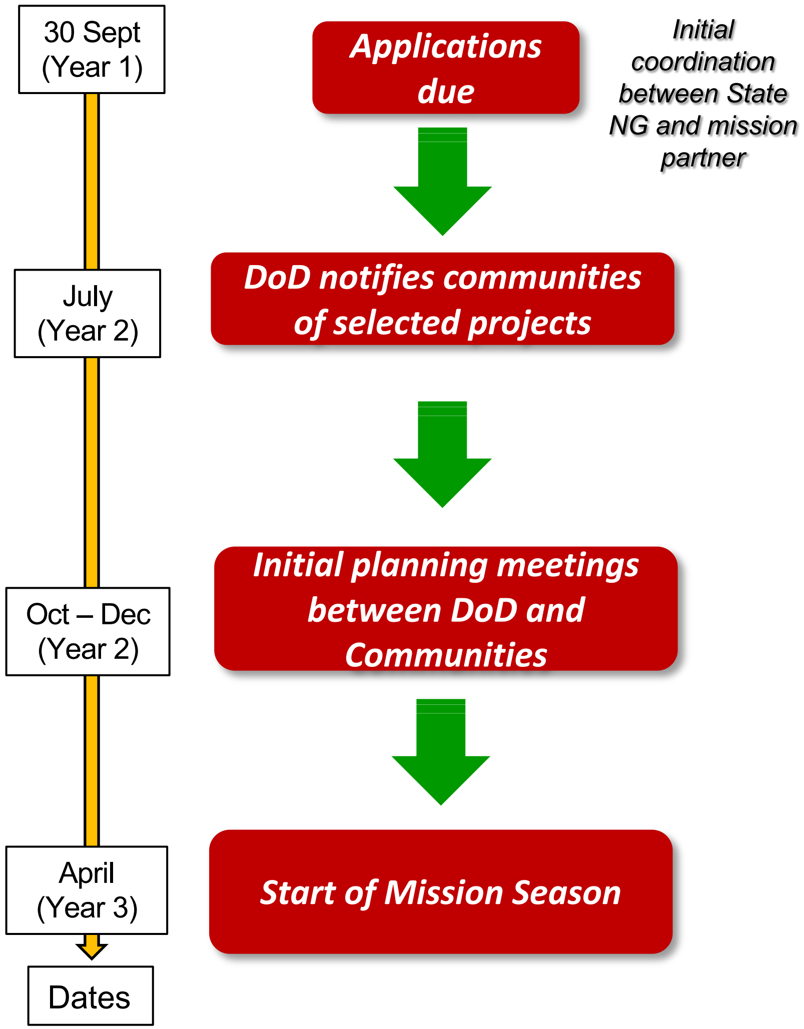


Legend

━ Support
━ Coordinate
╍ Conditional Request for Assistance

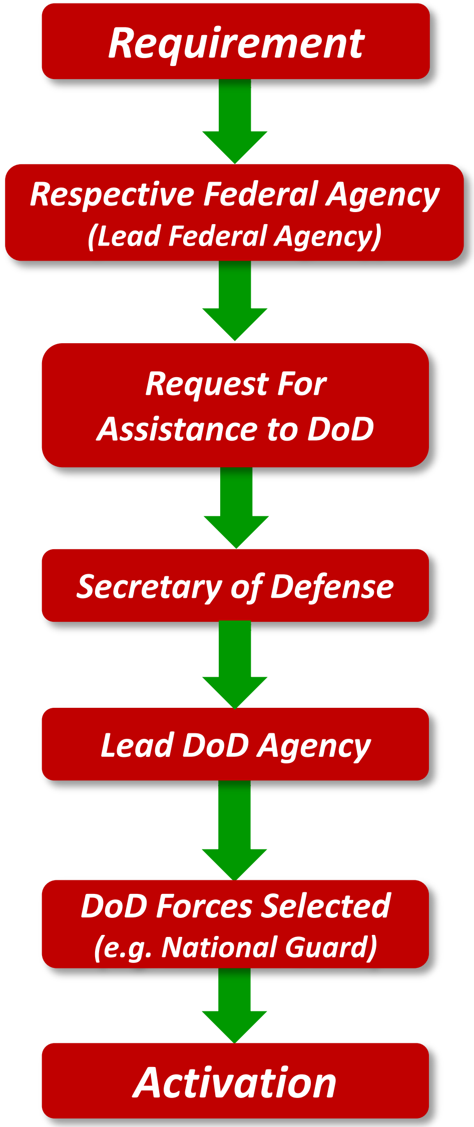
JFHQ = Joint Force Headquarters
RFA = Request for Assistance
REQ = Requirement
TAG = The Adjutant General

Innovative Readiness Training (IRT)


30 Sept (Year 1)
Applications due
Initial coordination between State NG and mission partner
July (Year 2)
DoD notifies communities of selected projects
Oct – Dec (Year 2)
Initial planning meetings between DoD and Communities
April (Year 3)
Start of Mission Season
Dates

For smaller community projects, Military Services may expedite the timeline if no DoD IRT funds are requested.

Defense Support to Civil Authorities (DSCA)


Requirement
Respective Federal Agency (Lead Federal Agency)
Request For Assistance to DoD
Secretary of Defense
Lead DoD Agency
DoD Forces Selected (e.g. National Guard)
Activation

Questions

For questions or concerns regarding anything in this brief, please contact the National Guard Bureau Cyber Operations Division:

ng.ncr.ngb-arng.mbx.j36-cyber-ops@army.mil