
U.S. DEPARTMENT OF HOMELAND SECURITY
STATE OF OREGON
1859
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
ARMY NATIONAL GUARD
AIR NATIONAL GUARD
DEPARTMENT OF DEFENSE
NATIONAL GUARD BUREAU
CYBEROREGON
UNITED STATES CYBER COMMAND
UNITED STATES
NORTHERN COMMAND
OREGON MILITARY DEPARTMENT
OEM
OFFICE OF EMERGENCY MANAGEMENT
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
TITAN FUSION CENTER
OREGON
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

National Guard Cyber Support

SSG Jason Adsit
Oregon Army National Guard

Mr. Courtney Ramsey
Oregon Titan Fusion Center

Cyber Initiatives in Oregon

- In September 2016, Governor Kate Brown issued Executive Order No. 16-13 entitled “Unifying Cyber Security in Oregon”
- In July 2017, Senate Bill 90 was enacted.
  - Unification of agency information technology security functions.
  - State agency coordination
  - Oregon Cybersecurity Advisory Council
  - Oregon Cybersecurity Center of Excellence
  - Authority of State Chief Information Officer to enter into agreements
  - Moneys from federal government and other sources
- In July 2018, the ORNG’s DCOE began working with the OTFC to improve the quality and timeliness of cyber intelligence sharing with SLTT partners.
- In fall 2018, the DCOE will coordinate with the Oregon Secretary of State’s security team with regard to cybersecurity of election infrastructure.

Traditional National Guard Missions

The Guard has a unique dual mission, with both federal and state responsibilities. During peacetime, Guard forces are commanded by the governor through a state adjutant general.

The governor can call the Guard into action during local or state-wide emergencies, such as storms, drought and civil disturbances.

Duty Statuses Applicable to the National Guard

	State Active Duty	Title 32	Title 10
Command and Control	Governor	Governor	President
Where	In State or State to State	United States	United States and Global
Pay	State	Federal	Federal
Discipline	State Military Code	State Military Code	UCMJ
Mission Types	State Domestic Operations Law Enforcement support in authority of state law	Federal Training & Missions Law Enforcement support in authority of state law	Overseas Training & Federal Missions Law Enforcement within the U.S. limited by *Posse Comitatus Act*

Cyber Mission Types

- Ongoing example: ORNG partnership with ESO and the OTFC to perform Cyber assessments for State customers (i.e. Counties, Cities, Schools, etc..), in order to increase their cyber posture.

- As Needed: State directed SAD and Title 32 missions to support CTAA. Guidance for these missions are dictated by DoD Policy Memo 16-002.

    - Title 32 Missions must not interfere with ORNG training requirements or unit readiness.

    - SAD Missions must be authorized by the Governor and pre-funded or reimbursed by the supported entity

Acronyms:
DCOE – Defensive Cyberspace Operations Element
CTAA – Coordinate, Train, Advise, and Assist
OEM – Office of Emergency Management
SAD – State Active Duty
DAS – Department of Administrative Services
NTOC – NSA/CSS Threat Operations Center
ESO – Enterprise Security Office
DSCA - Defense Support of Civil Authorities
OMD – Oregon Military Department
JRIC – Joint Regional Intelligence Center
OTFC – Oregon Titan Fusion Center
NCCIC – National Cybersecurity and Communications Integration Center

Mission Roles and Responsibilities

- During a large scale cyber event, the Governor will activate NG cyber teams to assist State, Local, Tribal, and Territorial governments with combating cyber-attacks and restoring critical Industrial Control Systems – Supervisory Control and Data Acquisition (ICS-SCADA) infrastructure (i.e. dams, power plants, mass transit) and services lost or damaged resulting from cyber-attacks.
- Deputy SECDEF Policy Memo 16-002: Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities.
- Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, signed June 2013, identified 16 critical infrastructure sectors:
  - Chemical
  - Commercial Facilities
  - Communications
  - Critical Manufacturing
  - Dams
  - Defense Industrial Base
  - Emergency Services
  - Energy
  - Financial Services
  - Food and Agriculture
  - Government Facilities
    - Includes Cybersecurity of Election Infrastructure
  - Healthcare and Public Health
  - Information Technology
  - Nuclear Reactors, Materials, and Waste
  - Transportation Systems
  - Water and Wastewater Systems

Additional Talking Points

- Cyber Incident Severity Schema
- Information Sharing and Analysis Organization
- NSA/DHS National Centers of Academic Excellence (CAE)
- Cyber Storm and Cyber Shield
- Cybersecurity of Election Infrastructure

Contact Information

SSG Jason Adsit

Cyber Operations NCO
Defensive Cyber Operations Element (DCOE)
Oregon Army National Guard
503-584-3945
jason.l.adsit.mil@mail.mil

Group Email:
ng.or.orarng.list.j6-dcoe@mail.mil

Mr. Courtney Ramsey

Intelligence Analyst
Urban Area Security Initiative (UASI)
Oregon Titan Fusion Center
503-934-2062
courtney.d.ramsey@doj.state.or.us

Group Email:
oregonfusioncenter@doj.state.or.us

References

National Cyber Incident Response Plan (NCIRP):
https://www.us-cert.gov/ncirp

SLTTGCC Cyber Resource Compendium:
https://www.dhs.gov/publication/slttgcc-cyber-resource-compendium

JP 3-12 - Cyberspace Operations:
http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Cyber Incident Severity Schema:
https://it.ojp.gov/GIST/178/File/Cyber%20Integration%20for%20Fusion%20Centers.pdf#page=29

NCCIC Cyber Incident Scoring System:
https://www.us-cert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf

National Guard Cyber Defense Teams:
http://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/NG%20Cyber%20Defense%20Team%20Fact%20Sheet%20(Dec.%202017).pdf

DTM 17-007 – Interim Policy and Guidance for Defense Support to Cyber Incident Response
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-17-007.pdf

CNGBI 3000.04 – National Guard Bureau Domestic Operations
http://www.ngbpdc.ngb.army.mil/pubs/CNGBI/CNGBI%203000.04_20180124.pdf

Cybersecurity Act of 2015
https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/jes%20for%20cybersecurity%20act%20of%202015.pdf

References (Continued)

Community College Cyber Summit (3CS)
https://www.my3cs.org

National Exercise Program - Principals' Objective # 1: Intelligence and Information Sharing
https://www.fema.gov/media-library-data/1531316812629-998bade9a8215eda367591b98963c0ec/NEP_PO1_Fact_Sheet_20180330.pdf

National Exercise Program - Principals' Objective # 4: Cyber Coordination
https://www.fema.gov/media-library-data/1531317306234-5d5135caa2604e6e8fea7f4f4f2cb2b6/NEP_PO4_Fact_Sheet_20180330.pdf

National Cyber League
https://www.nationalcyberleague.org

NSA/DHS National Centers of Academic Excellence (CAE) Requirements
https://www.iad.gov/NIETP/CAERequirements.cfm

Designation of Election Infrastructure as a Critical Infrastructure Subsector
https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

Example: California National Guard's Cyber Network Defense Team Reimbursement Authority
http://web1a.esd.dof.ca.gov/Documents/bcp/1819/FY1819_ORG8940_BCP1751.pdf

Example: California National Guard's Cyber Service Catalog
https://cdt.ca.gov/services/wp-content/uploads/sites/2/2017/02/CND-catalog.pdf

NG Cyber Capabilities Overview for Vigilant Guard 2018
https://wss.apan.org/ng/VGCTTX/Shared%20Documents/NG%20Cyber%20Capabilities%20Overview%20for%20VG18.pptx


U.S. DEPARTMENT OF HOMELAND SECURITY
STATE OF OREGON
1859
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
ARMY NATIONAL GUARD
AIR NATIONAL GUARD
DEPARTMENT OF DEFENSE
NATIONAL GUARD BUREAU
CYBEROREGON
UNITED STATES CYBER COMMAND
UNITED STATES
NORTHERN COMMAND
OREGON MILITARY DEPARTMENT
OEM
OFFICE OF EMERGENCY MANAGEMENT
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
TITAN FUSION CENTER
OREGON
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Backup Slides

DCOE Mission Execution

- Prior to the start of the mission, all DCOE team members are required to sign a Non-Disclosure Agreement (NDA) with the Customer.
- The DCOE Team Chief, along with the Customer, conduct a walk through of what is expected during the inspection prior to the mission being conducted.
- At the conclusion of the mission the Customer is provided with additional verification of, or updated information on, the Cyber Security posture of their network.
- All confidential materials are destroyed immediately after the tests, insofar as the information is not necessary for drafting the test reports. The remaining information is destroyed once the final report is submitted to the Customer.
- General trend information is collected from each mission and rolled into a final statewide, non-attributable report, providing feedback on the Cyber Security Assessment mission.
- DCOE Team deploys to assist organizations as “third party” SME’s in cooperation with DAS-ESO, ensuring the following:
  - Empower the customer with the knowledge and tools needed to improve their cyber posture.
  - Create an experience that will build good relationships and provide a valued service for the customer.

Cyber Incident Severity Schema

Incident Level and Coordination

	General Definition	Handling Precedence	
		Interagency Coordination	Targeted Entity Contact[iii]
Level 5 Emergency (Black)[vi]	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.	Immediate. An appropriate agency will initiate ECAP conferencing procedures.	If relevant and as needed.
Level 4 Severe (Red)	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Immediate. Elevate to the CRG[ix] for rapid consultation; possible initiation of ECAP.[x] Convene UCG[xi] and C- CAR,[xii] as appropriate.	Immediate
Level 3 High (Orange)	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.[xiii]	Begin coordination within 1 hour. Elevate to the CRG for its awareness and deliberation. Convene UCG and C-CAR, as appropriate.	Initiate contact within 8 hours; in-person response within 24 hours.
Level 2 Medium (Yellow)	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Begin coordination within 4 hours.	Initiate contact within 24 hours; in-person response within 5 days.
Level 1 Low (Green)	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Discretionary	Discretionary[xiv]
Level 0 Baseline (White)	Unsubstantiated or inconsequential event.	Not warranted	Not warranted

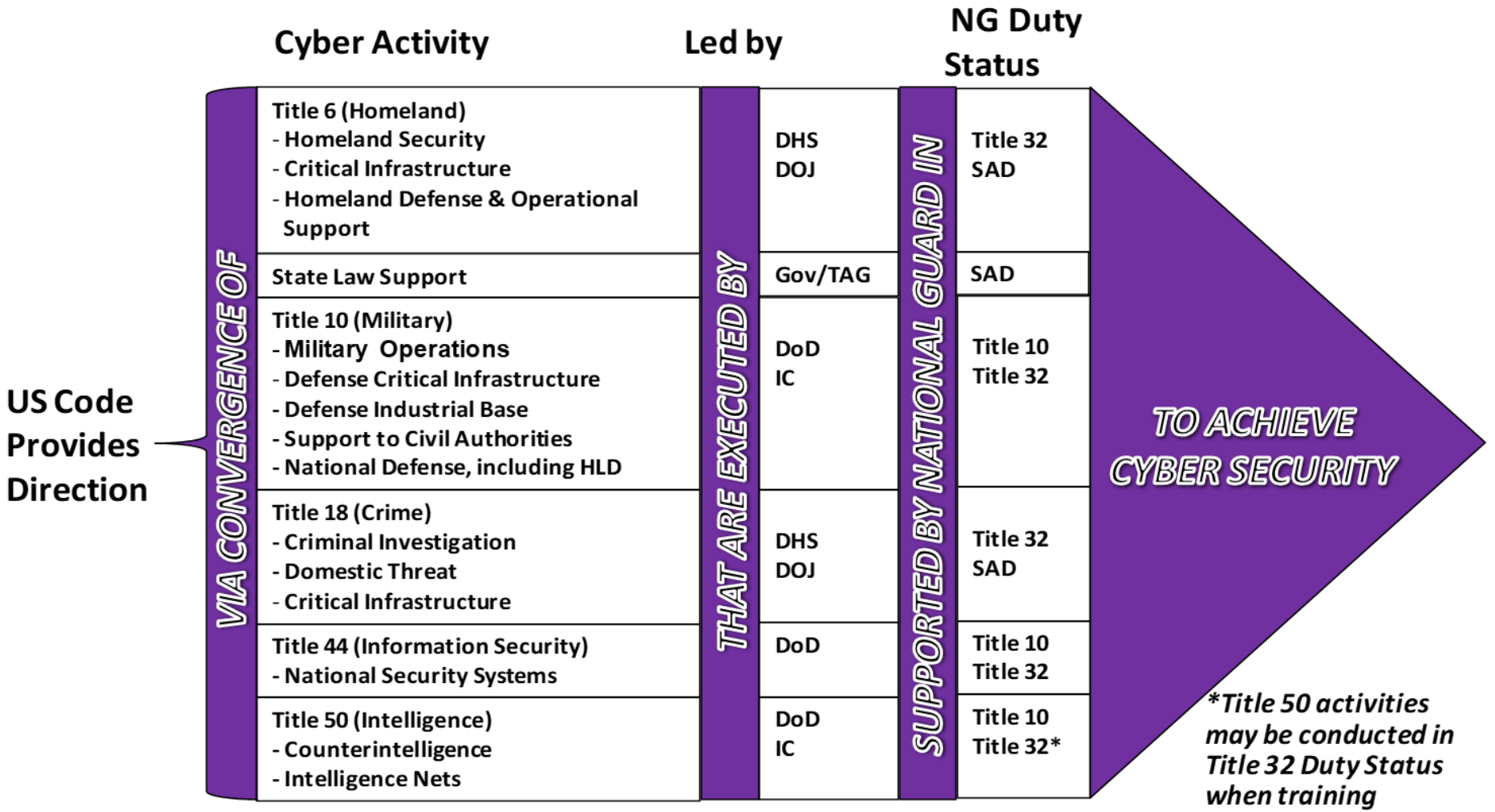
Significant Incidents

Skillsets and Capabilities

Skillsets	Capabilities

• Operating System environments
• Networking concepts and technologies
• Network security assessment techniques and procedures
• Industry standard security certifications include
  • Net +
  • Sec+
  • Linux+
  • CEH
  • CCNA
  • CISSP
  • GCFA
  • GCIH
  • GCED
	• **Shared Situational Awareness** – share, receive, filter/tearline, and broker cyber threat intelligence reports to/from the Customer, OTFC, ORNG JOC, DAS-ESO SOC, JRIC, NGCC, DHS NCCIC, NSA NTOC, and others
	• **Network Scanning and Mapping** - generate an independent, third-party perspective on the number, and types, of assets on the Customer's network
	• **Network Information Assurance Vulnerability Assessment (IAVA) Scan** - scan the Customer systems for known vulnerabilities and common misconfigurations
	• **Wireless Network Scan** - ensure that all wireless hardware and networks are properly configured and secured using current best practices
	• **Audit Log Review** - ensure that proper logs are kept on activity within the network
	• **Firewall Review** - verify firewall configurations, status of ports and the authorization of services/data flow running through the ports
	• **Network Security Procedural Review** - consult with the Customer on the current Security Management Posture of the network; identify security managers, security management procedures, limitations in management of the network (training, Hardware /software deficiencies, personnel); provide recommendations to enhance network security management posture
	• **Physical Security Review** - a non-invasive, comprehensive examination of the physical security controls
	• **Network Security Education** - consult with the Customer on any additional training that is needed to enhance security posture of the network
	• **Website Vulnerability Assessment (UPON REQUEST)** - provide Customer with a passive scan of hosted websites in order to validate the security of web applications utilizing open source tools.

Cyber Activities and Authorities



**Title 50 activities may be conducted in Title 32 Duty Status when training*

National Guard can support cyber operations across the entire cyber spectrum under Title 32, Title 10, and State Active Duty (SAD) statuses

Funding

Duty Status	State Active Duty	Title 32 502(a)	Title 32 502(f)(1)	Title 32 502(f)(2)	Immediate Response Authority
Description	Activation of NG by the Governor.	Planned NG Training. (One weekend a month, two weeks a year.) Additional training can be conducted pending availability of funds.	Planned NG Training with incidental benefit to an event. (Can be in addition to annual training requirements.)	NG operations with no other purposed than to conduct a specified mission	CDR's authority, in emergency circumstances where prior authorization is impossible, to engage temporarily in activities.
Funding	State Funded.	Federally appropriated training funds.	Federally appropriated training funds.	DoD funded or reprogrammed training funds.	Based on current duty status.
Considerations	Used at the discretion of the state at the cost of the state. No DoD funds are given.	Annually appropriated training funds. Statutorily mandated. Used for training purposes. Can be used to provide incidental support to an event.	Allows training with incidental benefit to an event. Requested by TAG. Approved by CNGB. Can also be additional training.	Used for activities that have a federal nexus. Can be in the form of authority only. Appropriateness, resource dislocation, Availability, Cost	(1) such activities are necessary to prevent significant loss of life or destruction of property (2) Authorities are unable or decline to provide protection for property gov functions.
References	As applicable to the respective state's laws	32 USC 502, SECDEF memo dated 16 DEC 2013 Leveraging Military Training	32 USC 502, DODD 3025.18, DODI 3025.20	32 USC 502, DODD 3025.18, DODI 3025.20	32 CFR 185.3, DODD 3025.18
Historic Events	Boston Marathon, Kentucky Derby, Illinois' floooding, ect ect.	RNC/DNC, NATO	Presidential Inauguration, NSJ, RNC/DNC, NATO Summit	Presidential inauguration, funerals, FEMA MAF sourced NG	California wild fires


U.S. DEPARTMENT OF HOMELAND SECURITY
STATE OF OREGON
1859
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
ARMY NATIONAL GUARD
AIR NATIONAL GUARD
DEPARTMENT OF DEFENSE
NATIONAL GUARD BUREAU
CYBEROREGON
UNITED STATES CYBER COMMAND
UNITED STATES
NORTHERN COMMAND
OREGON MILITARY DEPARTMENT
OEM
OFFICE OF EMERGENCY MANAGEMENT
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
TITAN FUSION CENTER
OREGON
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA