National Guard Cyber Support

CW2 Krispin Chairet

Oregon Army National Guard

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.

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:
ORNG – Oregon National Guard
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
SLTT – State, Local, Tribal, and Territorial
ESO – Enterprise Security Office
DSCA – Defense Support of Civil Authorities
OMD – Oregon Military Department
JRIC – Joint Regional Intelligence Center
OTFC – Oregon Titan Fusion Center

Current Trends

Threats

- SPAM
- Spear Phishing
- Scareware
- Ransomware
- Cryptojacking

Risks

- Email
- Websites
- Mobile devices
- Exposed ports
- Default or weak passwords

Contact Information

CW2 Krispin Chairet

Defensive Cyber Operations Element Leader
Oregon Army National Guard
503-584-3838
krispin.z.chairet.mil@mail.mil

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

Backup Slides

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 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

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

Implementation of E.O. 16-13, "Unifying Cyber Security in Oregon“:
https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/96166

References (Continued)

Oregon Emergency Operations Plan, Incident Annex 10 – Cyber Security
https://www.oregon.gov/oem/Documents/2015_OR_eop_ia_10_cyber.pdf

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 Strategy
https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

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#page=2

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

PSU Research to Support the Drafting of the Oregon Cybersecurity Center of Excellence Proposal:
https://olis.leg.state.or.us/liz/2018R1/Downloads/CommitteeMeetingDocument/141288

References (Continued)

Oregon OEM Overview:
https://olis.leg.state.or.us/liz/2015R1/Downloads/CommitteeMeetingDocument/47426

Oregon Public Safety Information Resource Management Strategic Plan 2017-2019:
https://olis.leg.state.or.us/liz/2017R1/Downloads/CommitteeMeetingDocument/99012

2017-2019 Governor's Budget, Oregon Military Department (Policy Package 106 & 107):
https://www.oregon.gov/OMD/AGC/Documents/2017-19_Governors_Budget.pdf#page=135

2018 Office of the State Chief Information Officer (OSCIO) Update:
https://olis.leg.state.or.us/liz/2018R1/Downloads/CommitteeMeetingDocument/142857#page=33

Domestic Operational Law – 2018 Handbook for Judge Advocates
https://tjaglcspublic.army.mil/documents/27431/38018/2018+DOMOPs+Handbook#page=288

Operational Law Handbook – 2018:
https://tjaglcspublic.army.mil/documents/27431/37173/Operational+Law+Handbook+18th+Edition.pdf#page=134

ISAO 300-2 - Automating Cyber Threat Intelligence Sharing:
https://www.isao.org/wp-content/uploads/2018/07/ISAO-300-2-Automating-Cyber-Threat-Intelligence-Sharing-v0.1.pdf

ISAO 600-2 - U.S. Government Relations, Programs, and Services:
https://www.isao.org/wp-content/uploads/2016/10/ISAO-600-2-US-Government-Relations-Programs-and-Services-v1-01_Final.pdf

Oregon Civil Defense Force:
https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB1000

State of Oregon Information Security Incident Response Plan:
https://www.oregon.gov/das/OSCIO/Documents/InformationSecurityIncidentResponsePlan.pdf#page=16


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
UNITED STATES CYBER COMMAND
CYBEROREGON
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