California Military Department
NCSL Legislative Summit Briefing

July 30, 2018
California Military Department
Joint Task Force Cyber
Force Structure and Training

MAJ Edward L Bombita
Agenda

- Joint Task Force Cyber Unit Structure
- Unit Locations
- Unit Missions and Manning
- Personnel Training
- Deployments
Joint Task Force Cyber Unit Structure

- JFHQ
- 195th AW O6
- 100th TC O6
- J2
- CSMR Cyber
- 149 C-ISR
- CND
- CPT 171
- 261st COS

SAD PERSONNEL

Army
Air Force
State
Joint
Unit Locations

Mather Airfield:
- Computer Network Defense Team
- 149th Intelligence Squadron
- JFLIC SCIF

Camp Parks:
Western Army Reserve Support Intelligence Center SCIF

Los Alamitos:
- Joint Forces Training Base SCIF
- Joint Regional Intelligence Center SCIF

Van Nuys:
261st Cyber Operations Squadron

Camp San Luis Obispo:
Cyber Protection Team 171

Silicon Valley

Silicon Beach
Mission: Conduct Defensive Cyberspace Operations – Internal Defensive Measures to secure the state’s portion of GuardNet, the ARNG contribution to the Department of Defense Information Network (DODIN). On order, CND-Ts protect critical state infrastructure and respond to state cyberspace emergencies as directed by TAG or Governor.

Manning: 18 total personnel from CAARNG, CANG and CSMR.

- Full time state active Duty (SAD): 9
- Traditional guard personnel: 9
261st Cyberspace Operations Squadron 261st COS


Manning: 39 total personnel on title 32 status.
- Full time technicians: 1
- Traditional guard personnel: 37
Cyber Protection Team 171 (CPT 171)

Mission: Conduct defensive cyberspace operations on military networks to support mission requirements as identified by DOD or state leadership. Primary support is support of federal cyber forces. Secondary focus is state support, mainly as incident response forces.

Manning: 39 total personnel on title 32 status.
- Full time personnel: 2
- Traditional guard personnel: 37
149th Intelligence Squadron

**Mission:** produce tailored all-source intelligence products for AFCYBER, the National Intelligence Community, and enable the Cyber Mission Force (CMF) operations. The analytic work-roles are Target Digital Network Analysts (TDNA) and All-source Intelligence Analysts (ASIA). The ISR operators provide SIGINT-based, all-source analysis in the Cyber domain.

**Manning:** 71 CANG personnel on title 32 status:
- Full time technicians: 18
- Traditional guard personnel: 53
California State Military Reserve - Cyber

**Mission**: Provide support to cyber forces in specific areas of expertise. Currently CSMR-Cyber is providing legal support and will soon be providing Cyber SMEs to the other JTF elements. These SMEs will be recruited from major IT and Cyber companies and will help training and keep our cyber forces current.
Personnel Training

• **Job qualification Training**
  • Initial training for cyber personnel
  • Based on military occupation title
  • Same no matter where service member is assigned

• **US Cyber Command (USCC) Training**
  • Training USCC requires if assigned to a cyber unit
  • Based on work role
  • Two training tracks:
    • Intelligence
    • Technical (IA, Intermediate/Advanced cyber training, Methodologies)

• **Additional Training**
  • Certifications (e.g. CISSP, CEH)
  • Tools training (e.g. Security Onion)
Deployments

261st COS
  • Joint Base Lewis-McChord Rotation (2017)

CPT 171
  • FT Meade, MD (2017-18)
So What?

- Large breadth of experience
- Low cost to train
- Clearances
California Military Department
Cyber Network Defense Team
Operational Overview
LTC James Parsons
Agenda

• Purpose
• Typical Situation
• Independent Security Assessments
• Risk Identification
• Intended Outcomes
• California National Guard
  • Cyber Network Defense Team
Purpose

• Increase the security of state agency networks and systems in order to protect the data and livelihood of California Citizens
Typical Situation

- An Enterprise of Enterprises
- Little Centralized Control of IT Systems
- Little Standardization of IT Systems
Independent Security Assessment

• There are many cybersecurity initiatives underway in California State Government

• The Core$^4$ Cybersecurity Partnership
Independent Security Assessment

• An Independent Security Assessment (ISA) is:
  • Third party objective look at the cybersecurity of an agency
  • Conducted with established criteria
  • Provides an indicator of Entity’s Cybersecurity Maturity

• An ISA is a California Policy that was moved into state law 1 January 2016
  • [Link](https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=11549.3.&lawCode=GOV)
    • “The Military Department may perform an independent security assessment of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed.”
Risk Identification

• Criteria
  • National Institute of Standards and Technology (NIST) Based Analysis
  • Includes State of CA Specific Enhanced Guidance
  • Metrics-based Scoring

• Two Phases
  • External
  • Internal

• Two Teams
  • Blue – Defensive Resistance and Measures Analysis
  • Red – Threat-Actor Simulated Attacks / Measurements
ISA Outcome

• ISA Overall Score
  • The ISA evaluates 29 areas across 9 NIST and State Administrative Manual (SAM) Control families

• Score Impacts
  • CISO’s Cybersecurity Maturity Metric
  • Will impact future Audit requirements

• Key Take-Aways
  • Management awareness of cybersecurity status
  • Prior analysis at this level of detail is uncommon for most Gov’t organizations
  • Analysis and recommendations help inform future IT security spending
Criteria Sample

Task ID: 2.04.1 - Detection and Mitigation of Network Rogue Devices  NIST Ctrl: SI-4

Foundational Framework Category: Network Security
Prime Objective: Network Admission Control

Artifact Requirements: Required: No  * If Yes, see required artifact for description

Required Artifact: n/a
Condition:
Entity deploys controls and monitors for signs of Rogue Network Devices; reacts to detected potentially unauthorized devices on the network:
- Entity deploys controls for the detection and alerting of unauthorized / rogue devices upon connection
- Network security team receives rogue devices alerts and opens event for remediation
- Network team reports incident to ISO / Security team
- Required Logical test: Assessment team connects to random port not provided for the assessment with rogue device; waits 60 minutes to determine if connection is detected / investigated

Scoring Criteria:
I – Entity detects, alerts, reports security incident, and locates potentially unauthorized device within 60 minutes of connection
P – Entity detects, alerts, but does not report occurrence or locate device within 60 minutes of connection
N – Entity does not detect, alert or fails to identify location of suspect device

Findings / Comments:
California National Guard
  - Cyber Network Defense Team

• Discussions with the CISO revealed the need for cybersecurity support to state agencies

• Cyber Network Defense (CND) Team Established April 2013
  • Initially staff taken out of hide and team augmented with grant funding
  • Staffed with State Civil Service and State Active Duty Service members
  • Currently funded entirely by reimbursements from services provided

• CND Qualifications – What is the Guard qualified to offer
  • Experience in Enterprise IT and Cybersecurity
  • DoD Experience in Information Assurance/Inspections
  • Industry Standard Certifications
California National Guard
- Cyber Network Defense Team

• Services Provided:
  • Vulnerability Assessments
  • Penetration Tests
  • Phishing Testing
  • System Hardening Analysis
  • Web Site Assessments
  • Firewall Assessments
  • Incident Response
  • General Consulting where expertise exists

• Statistics For Fiscal Year 2017 - 2018:
  • Hosts Analyzed: 58,347
  • Total ISAs: 41
Typical Discoveries

• Cybersecurity needs Executive Level Buy-in

• Patching is Resource Intensive

• Cyber requires qualified and dedicated staff

• Current technology for cybersecurity is important
  • Next Generation Firewalls
  • Next Generation Anti-Virus

• Inspect What You Expect
  • If you don’t look, you don’t know
California Military Department
Joint Task Force Cyber
Cyber Law
BG Jay Coggan
Discussion / Questions

Major Edward Bombita
CPT 171 Commander, CA Military Department
edward.l.bombita.mil@mail.mil

Lieutenant Colonel James Parsons
CND Chief, CA Military Department
James.L.Parsons@cnd.ca.gov

Brigadier General Jay Coggan
CSMR Commander, CA Military Department
jay.m.coggan.nfg@mail.mil