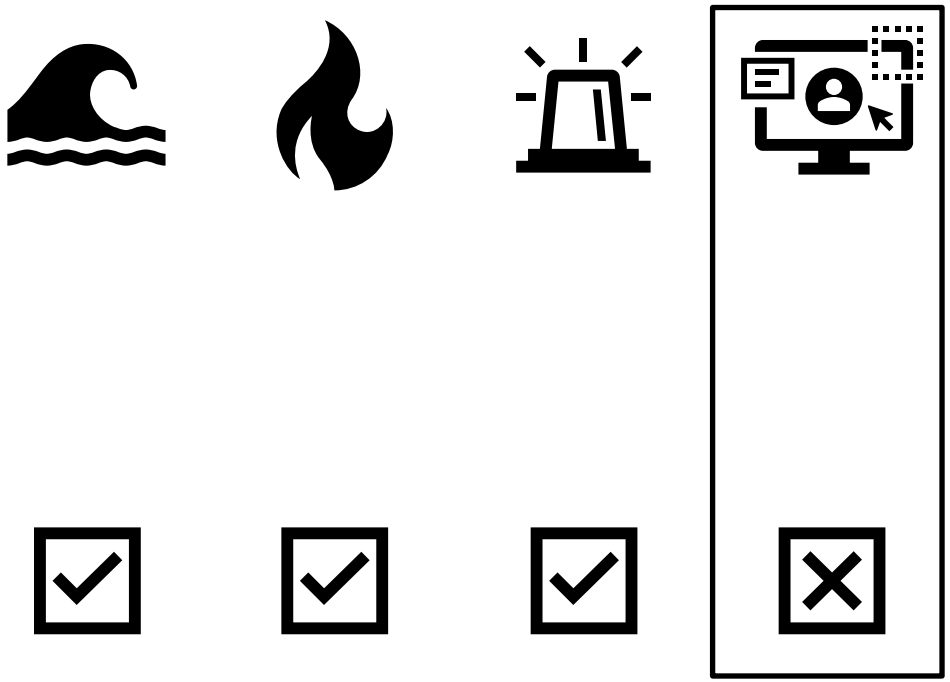
Nevada National Guard JTF Cyber Implementation Plan
9 Jan 2023

Purpose

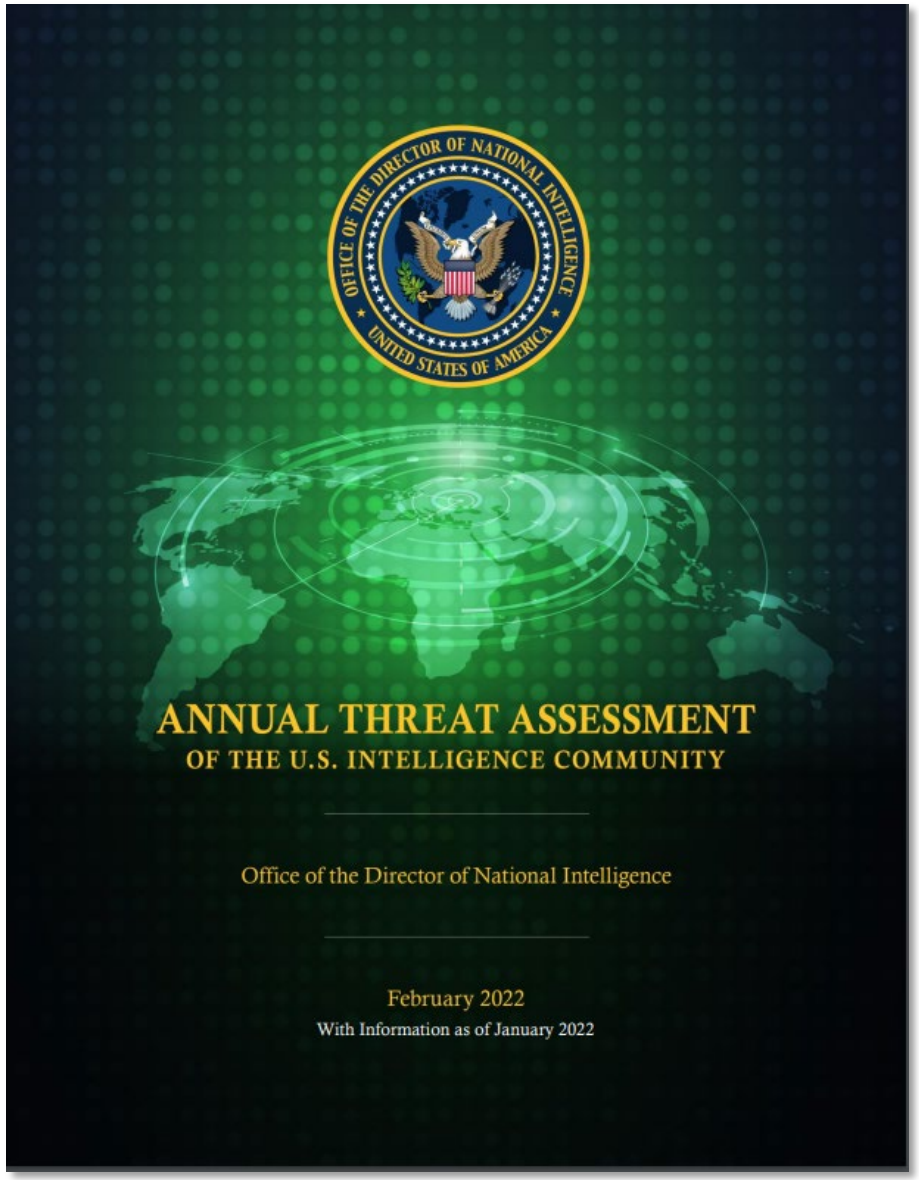
- **Brief on the Nevada National Guard's JTF Cyber, its Concept of Operations, Implementation Timeline, and the supporting intelligence.**



Intelligence Estimate of Cyber Threats: National

Nation States

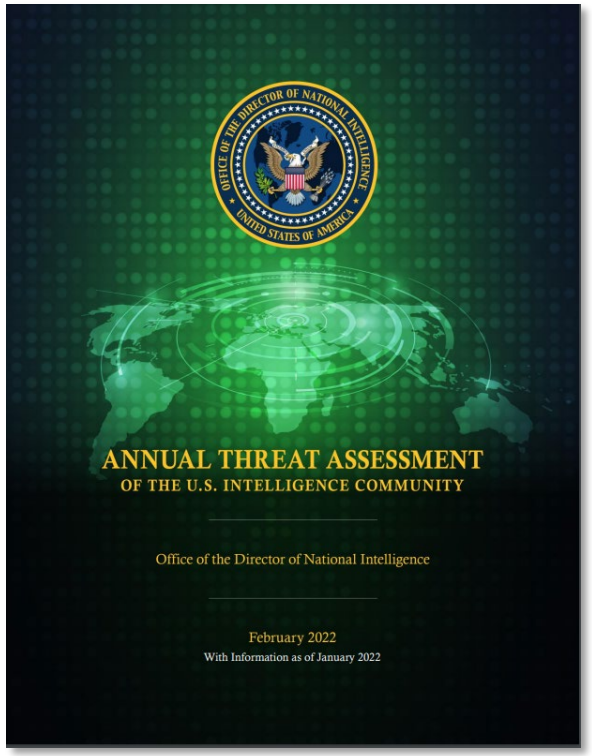
- ***China*** *- broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks.*
- ***Russia*** *- employs its espionage, influence, and attack capabilities…. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions, as well as a deterrence and military tool.*
- ***Iran*** *- believes it must demonstrate that it can push back against the US. Recent attacks show that Iran is more willing to target countries with stronger capabilities.*
- ***DPRK*** *- probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the US.*

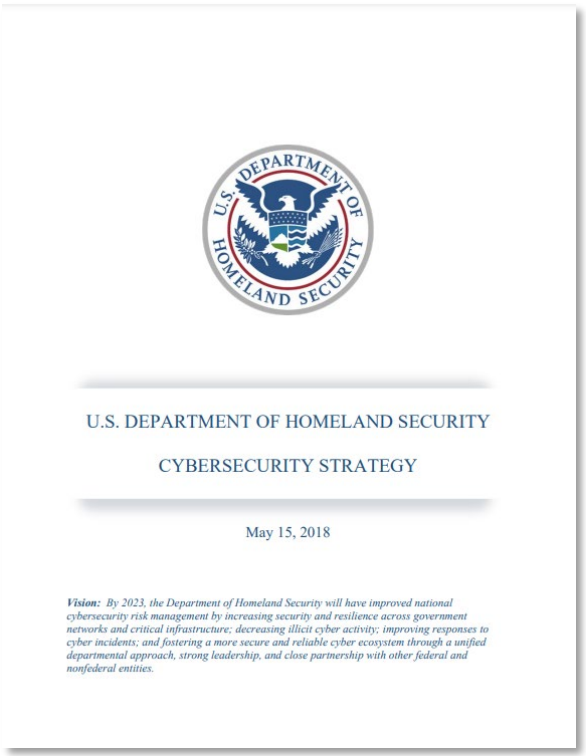


Intelligence Estimate of Cyber Threats: National

Transnational cyber criminals

- *Increasing the number, scale, and sophistication of ransomware attacks*
- *Fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide*
- *Driven by the promise of large profits, reliable safe havens from which to operate, and a decreasing technical barrier to entry for new actors.*
- *Increasingly collaborate through cyberspace*
- *Increasingly used as proxies to blur the distinction between state and non-state cyber activities*
- *In several cases, malicious actors engaged in significant criminal cyber activity appear to have both criminal and nation-state affiliations*





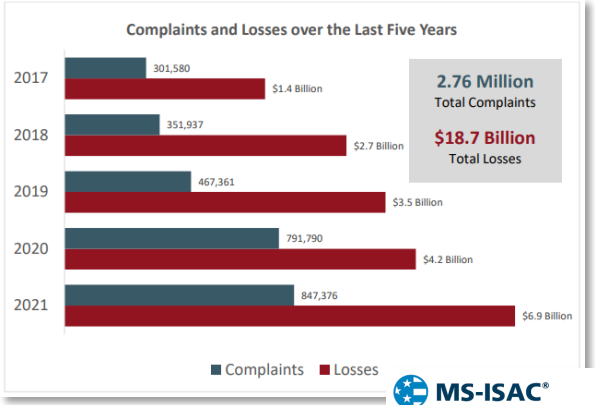
UNCLASSIFIED

Intelligence Estimate: Nevada

Most Likely COA:

Organized Cybercrime Actors continue to *opportunistically and indiscriminately* target Nevada State Agencies, Municipalities, and Businesses for financial gain *as part of broad-based international campaigns.*

FEDERAL BUREAU of INVESTIGATION
Internet Crime Report



MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Cyber Threat Intelligence

BlackCat: A Bad Omen Plaguing SLTTs

August 2022 • SFAR-2022-3
TLP: AMBER

Most Dangerous COA:

Nation State Actors *deliberately* target Nevada Critical Infrastructure with *Disruptive / Destructive Effects.*

April 20, 2022

ACSC Australian Cyber Security Centre
Communications Security Establishment Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité
GOVERNMENT COMMUNICATIONS SECURITY BUREAU TE TIRA TIAKI
National Cyber Security Centre
NCA National Crime Agency

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

ADVANCED PERSISTENT THREAT FROM TEHRAN —

Hackers backed by Iran are targeting US critical infrastructure, US warns

Vulnerabilities already patched by Microsoft and Fortinet are being exploited en masse.

July 6, 2022

North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

NIST Cybersecurity Framework vs Adversary Cyber Kill Chain

- **Identify**
  - Identify Physical / software assets
  - Identify Mission / Business Dependencies
  - Identify Vulnerabilities
  - Identify Risk Management Strategy
- **Protect**
  - Protect the confidentiality, integrity, and availability
  - Manage Protective Technology
  - Conduct Awareness and Training
- **Detect**
  - Monitor Cybersecurity Events
  - Ensure Anomalies and Events are Detected
- **Respond**
  - Execute Incident Response
- **Recover**
  - Restore Impaired Services
  - Implement Lessons Learned to Ensure Resilience Against Future Attacks

Incident-to-Deployment: Notional JTF Cyber Tasking Cycle

1. Municipality or State Agency is Alerted to Malicious Activity

Alert

2. Conducts Analysis / Organic Mitigations, if able

3. Reaches Internal Resource Exhaustion / Escalates Higher (OCDC, EITS)

4. DEM Conducts Intel-informed Risk Assessment

High Risk

5. Requests JTF Cyber Deployment from the Governor

6. Governor Concurs

7. DEM Deploys JTF Cyber

8. JTF Cyber Conducts Timely, Effective Defensive Cyber Ops on Objective

Texas and Louisiana Case Studies Lessons Learned

- **A proactive assessment of security policies and their implementation would have highlighted the vulnerable "low hanging fruit"**
  - **Misconfigurations**
  - **Unpatched vulnerabilities exploited elsewhere**

- **Visibility and timely actions in response to suspicious actions would have denied the wide-spread lateral movement to adversary**

- **An all-hazards JTF Cyber deployment after adversary's actions on objective will likely be a *"recover" recovery mission, not an adversary interdiction – "detect, respond"***
  - **Current NV NG skillsets already available for recovery tasks**

Initial JTF Cyber Commander's Intent

Purpose

- JTF Cyber conducts intelligence-informed cyber operations on Nevada State, County, Municipal, and critical infrastructure networks and systems to reduce the risk of service disruptions, sensitive data theft, or other instances of material loss from malicious cyber activity.

Method

- NV ARNG and NV ANG organize, train, and equip qualified JTF Cyber personnel to preemptively assess the security posture of Nevada networks and deploy in a post-breach incident response capacity.

End State

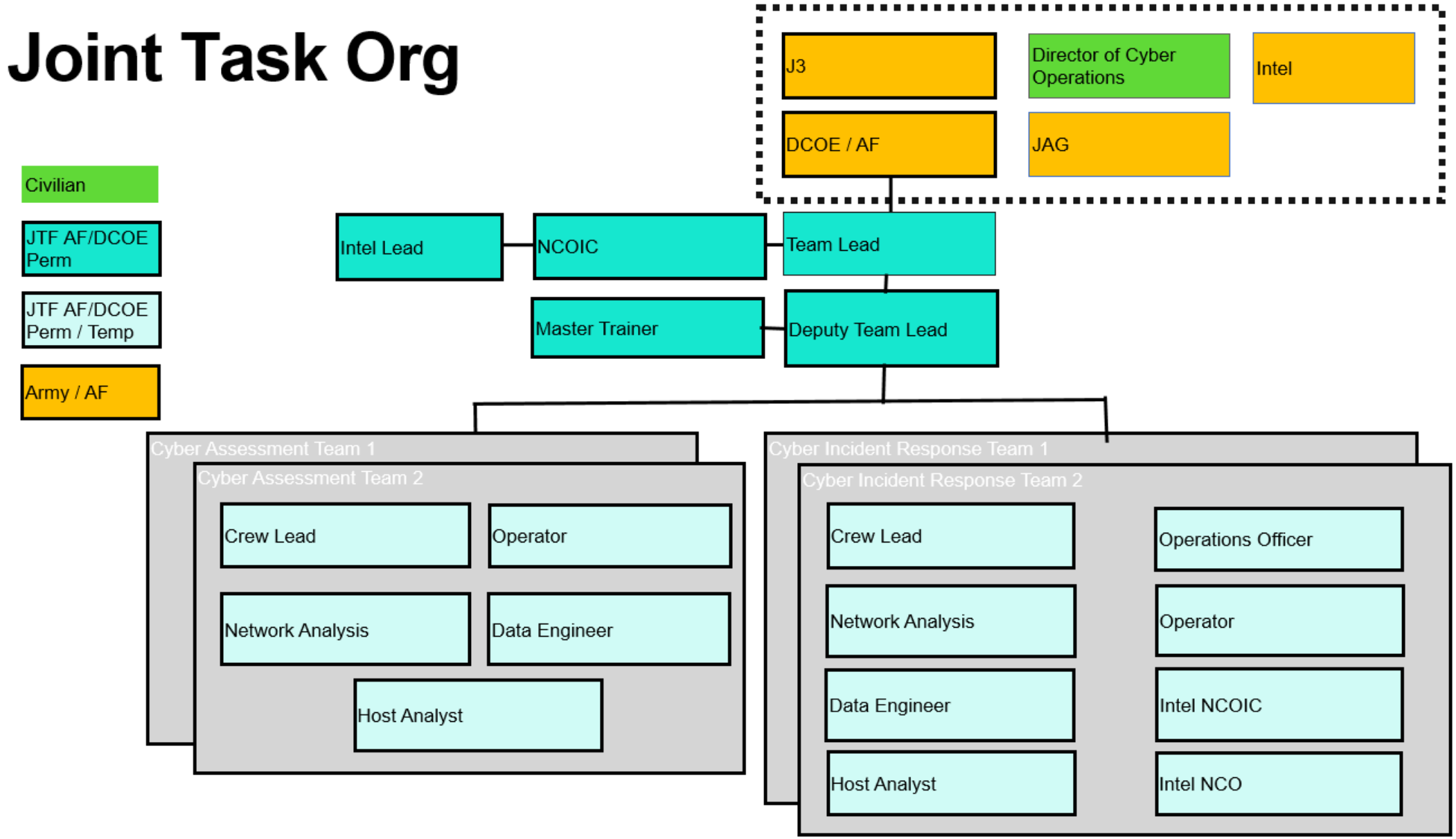
- JTF Cyber readiness results in effective and timely operations to shrink the attack surface of friendly networks and reduce the risk of malicious cyber activity in post-breach incident response capacity.

Lines of Effort

- ***LOE 1 – Component Responsibilities***
  - ***Task 1.1*** OT&E most-qualified DCOE and 152 CF personnel for JTF Cyber (Planning/Execution: Immediately)
  - ***Task 1.2*** Long-term CMF alignment to expand JTF Cyber capability and capacity (Planning: Immediately; Execution: in 12-18 months)
- ***LOE 2 – JTF Responsibilities for Mission Execution***
  - ***Task 2.1*** Collect and analyze intel to refine IE (Planning/Execution: Immediately)
  - ***Task 2.2*** Establish JQS (Planning/Execution: Immediately)
  - ***Task 2.3*** Shrink friendly attack surface and increase readiness for all-hazards cyber incident response (Planning/Execution: Immediately)
- ***LOE 3 – JTF Responsibilities for External Engagement and Partnership Building***
  - ***Task 3.1*** Engage with the State and Federal key stakeholders to develop and implement a Cybersecurity Strategy for *intel-informed defensive cyber ops* (Planning/Execution: Immediately)
  - ***Task 3.2*** Advocacy for State Active Duty / State Employee funding to conduct technical assessments and incident response

Friendly Forces

Joint Task Org



State Active Duty Team: Mission

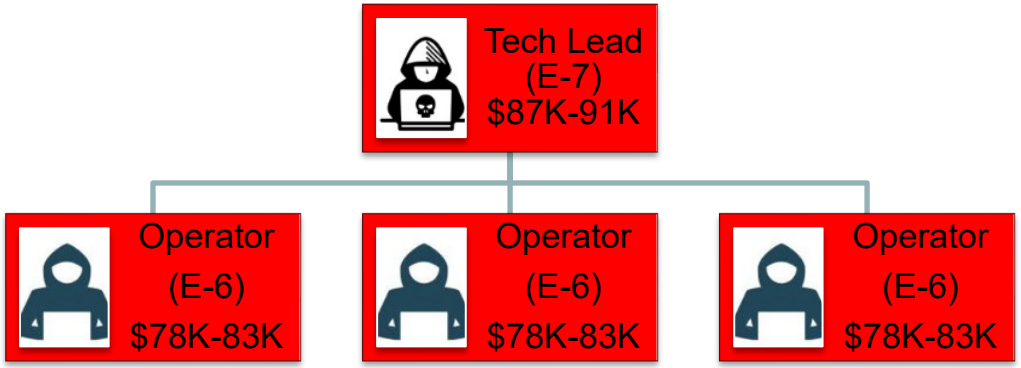
Mission

- **Independent Assessment Team conducts penetration assessments and red team missions in order to provide supported Nevada State, municipal, and critical infrastructure organizations an intelligence-informed, threat-representative context of risk posed by a potential cyber adversary.**
- **Provide technical expertise in an all-hazards cyber incident response event.**

State Active Duty Team: Manpower (4 positions)

4-position Team

- One mission-at-a-time construct
- 6 week mission planning horizon
  - 1 week planning
  - 2-week execution
  - 2 week report writing
  - 1 week personnel/tool reconstitution
- Legal consideration would be planned out via general support JA, which may incur short-term legal risks
- Mission capacity reduced from 2 to 1 mission at a time due to operator reduction
- Without Team Chief, Tech Lead takes on leadership and technical oversight roles for operators, which extends out the report writing windows and reduces leadership engagement with support organization
- $321K/year if all personnel w/o dependents
- $340K/year if all personnel w/ dependents



Objectives: LOE 3 (JTF & Joint Staff)

- 3.1 Engage with the State's key stakeholders to develop and implement a Cybersecurity Strategy for *intel-informed defensive cyber ops*
  - Grow capacity for comprehensive coverage along the NIST Cybersecurity Framework
    - Federal Partnerships
    - Deliberate Talent Recruiting, Retention, and Development
      - CyberCorps Scholarships
    - Partnership with Academia
      - Research & Innovation
    - Partnership with Industry
      - Capability procurement
      - Bilateral career broadening
    - JTF Cyber Integration - optimize the tasking process to ensure timely and effective response.
  - Hardware / software integrity
    - State IT modernization
    - Supply chain security