Nevada Department of Public Safety
Office of Cyber Defense Coordination
2020-2022 Strategic Plan

Mission Statement

The Office of Cyber Defense Coordination serves as the primary focal point for cybersecurity strategy, policy, planning and coordination for the State of Nevada.

Primer

A healthy cyber community depends on an open, robust, thought provoking, and thought-provoking dialog between community members at all levels. Public and private partners each bring their own diverse perspective and strengths to the table. OCDC, in our role as a focal point for enhancing cybersecurity for all partners, will continue to expand and leverage relationships throughout the State.

Current and future relationships with public and private partners will pay dividends as OCDC assumes its role in prescribing and reviewing cyber-incident response plans for all political subdivisions. The subsequent establishment, review, adoption, and exercise of flexible and adaptable cyber-incident response plans by partner organizations will prepare the community as a whole to prevent, counteract, and successfully respond to future cyber-incidents.

Guiding Principles

The Nevada Office of Cyber Defense Coordination is guided by Nevada Revised Statute (NRS) 480.900-480.950. Specifically, OCDC is charged with meeting the following:

1. **Prevent** adverse cyber-incidents throughout the State of Nevada by acting as a conduit for best practices and lessons learned to flow through to partnering organizations.
2. Enable the **response** process by prescribing relevant incident response plan requirements, auditing plans for compliance and conducting exercises to strengthen those plans.
3. Enable organization's ability to counteract malicious cyber-actors by **coordinating** resources and technical experts to organizations.

Based on guidance set forth in NRS 480.930 OCDC has outlined the following **strategic pillars** for the 2020-2022 biennium.

Threat Identification / Prevention – OCDC will work with community partners to share cyber lessons learned, cyber threat intelligence, and current threat mitigation techniques to better identify and prevent threats to and attacks on the security of information systems in the State of Nevada.

Incident Response - OCDC is at the forefront of helping Nevada's political subdivisions prepare and complete dynamic, flexible, cyber-incident response plans. These living documents will better prepare State entities to contain, eradicate, and recover from a cyber incident.

Partner Collaboration - OCDC will continue to coordinate information, intelligence, and resource sharing throughout the State by leveraging ever-evolving partner relationships. This will enhance the voluntary sharing of information and collaboration amongst appropriate state, local, and federal entities.

Cybersecurity Investment – OCDC will ease the confusion and frustration associated with cybersecurity investing by identifying cost effective alternatives which provide comparable security, aid in the identification of shortfalls, and help partners find the most appropriate means to protect critical infrastructure, their assets, and maintain their bottom line.

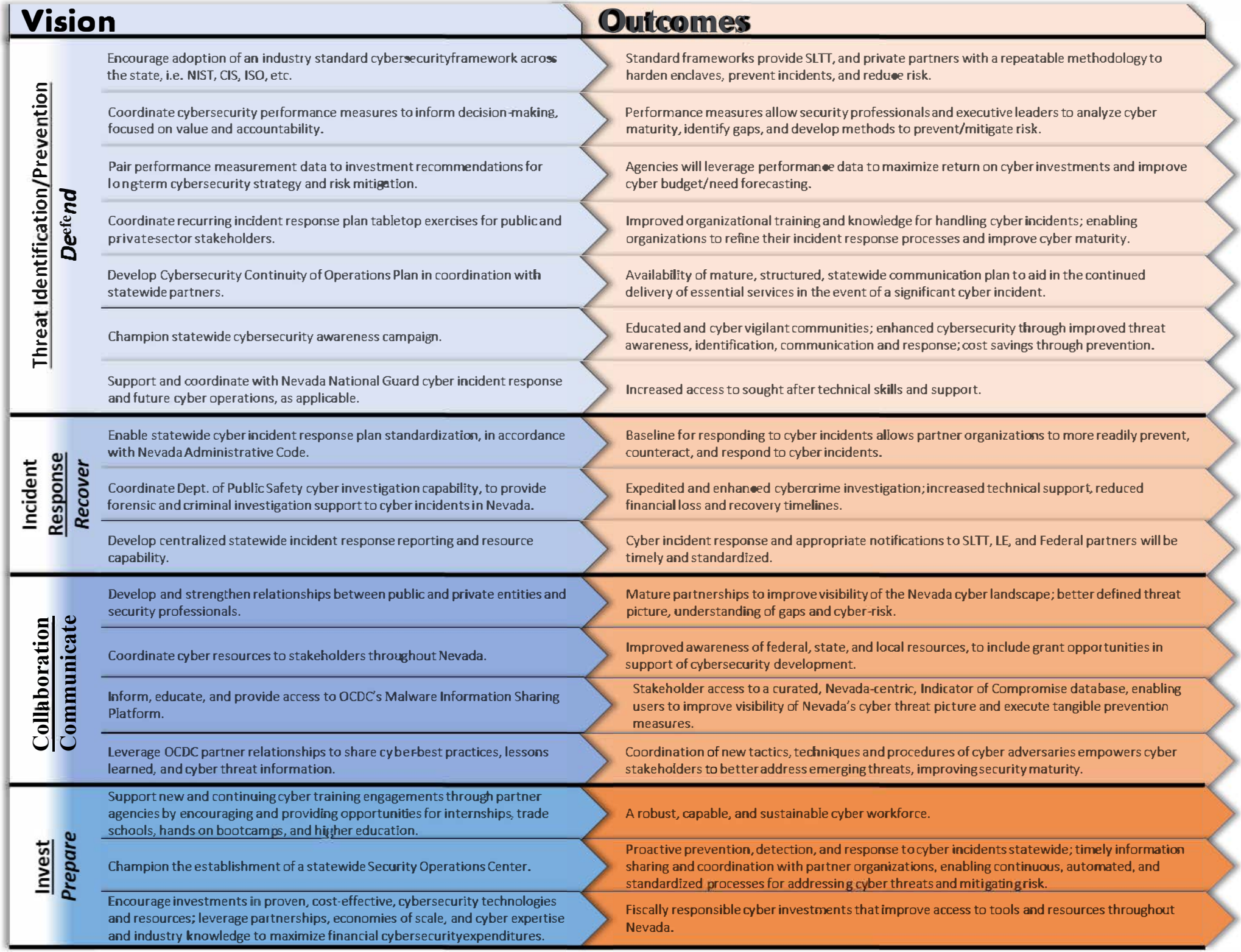
Milestones and Challenges

Milestones

- Establish an incident response plan baseline which partners can utilize to create their own custom plans.
- Provide clear, obtainable, guidance for the creation, review, implementation, and exercise of incident response plans.
- Track and report progress on compliance with NRS 603A, which identifies the CIS top 20 controls as a baseline security framework for the Executive Branch.

Challenges

- Cybercrime is evolving daily and there is literally no end in sight, as the threat evolves our partners and OCDC will need to remain nimble and work toward a greater ability to be more proactive than reactive.
- Cybercrime pays and is starting to pay more often and in larger amounts. There are multiple accounts of organizations paying ransoms, or Business Email Compromise, and similar cybercrimes that result in big paydays.
- Collaboration between state, local, public, and private partners. Tearing down silos and getting organizations to share cybersecurity intelligence and information will prove to be key in protecting the State of Nevada and its interest.


Vision
Outcomes
Threat Identification/Prevention
Defend
Encourage adoption of an industry standard cybersecurityframework across the state, i.e. NIST, CIS, ISO, etc.
Standard frameworks provide SLTT, and private partners with a repeatable methodology to harden enclaves, prevent incidents, and reduce risk.
Coordinate cybersecurity performance measures to inform decision-making, focused on value and accountability.
Performance measures allow security professionals and executive leaders to analyze cyber maturity, identify gaps, and develop methods to prevent/mitigate risk.
Pair performance measurement data to investment recommendations for long-term cybersecurity strategy and risk mitigation.
Agencies will leverage performance data to maximize return on cyber investments and improve cyber budget/need forecasting.
Coordinate recurring incident response plan tabletop exercises for public and private-sector stakeholders.
Improved organizational training and knowledge for handling cyber incidents; enabling organizations to refine their incident response processes and improve cyber maturity.
Develop Cybersecurity Continuity of Operations Plan in coordination with statewide partners.
Availability of mature, structured, statewide communication plan to aid in the continued delivery of essential services in the event of a significant cyber incident.
Champion statewide cybersecurity awareness campaign.
Educated and cyber vigilant communities; enhanced cybersecurity through improved threat awareness, identification, communication and response; cost savings through prevention.
Support and coordinate with Nevada National Guard cyber incident response and future cyber operations, as applicable.
Increased access to sought after technical skills and support.
Incident Response
Recover
Enable statewide cyber incident response plan standardization, in accordance with Nevada Administrative Code.
Baseline for responding to cyber incidents allows partner organizations to more readily prevent, counteract, and respond to cyber incidents.
Coordinate Dept. of Public Safety cyber investigation capability, to provide forensic and criminal investigation support to cyber incidents in Nevada.
Expedited and enhanced cybercrime investigation; increased technical support, reduced financial loss and recovery timelines.
Develop centralized statewide incident response reporting and resource capability.
Cyber incident response and appropriate notifications to SLTT, LE, and Federal partners will be timely and standardized.
Collaboration
Communicate
Develop and strengthen relationships between public and private entities and security professionals.
Mature partnerships to improve visibility of the Nevada cyber landscape; better defined threat picture, understanding of gaps and cyber-risk.
Coordinate cyber resources to stakeholders throughout Nevada.
Improved awareness of federal, state, and local resources, to include grant opportunities in support of cybersecurity development.
Inform, educate, and provide access to OCDC's Malware Information Sharing Platform.
Stakeholder access to a curated, Nevada-centric, Indicator of Compromise database, enabling users to improve visibility of Nevada's cyber threat picture and execute tangible prevention measures.
Leverage OCDC partner relationships to share cyber-best practices, lessons learned, and cyber threat information.
Coordination of new tactics, techniques and procedures of cyber adversaries empowers cyber stakeholders to better address emerging threats, improving security maturity.
Invest
Prepare
Support new and continuing cyber training engagements through partner agencies by encouraging and providing opportunities for internships, trade schools, hands on bootcamps, and higher education.
A robust, capable, and sustainable cyber workforce.
Champion the establishment of a statewide Security Operations Center.
Proactive prevention, detection, and response to cyber incidents statewide; timely information sharing and coordination with partner organizations, enabling continuous, automated, and standardized processes for addressing cyber threats and mitigating risk.
Encourage investments in proven, cost-effective, cybersecurity technologies and resources; leverage partnerships, economies of scale, and cyber expertise and industry knowledge to maximize financial cybersecurityexpenditures.
Fiscally responsible cyber investments that improve access to tools and resources throughout Nevada.