# 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

To address the growing cyber threat environment, the Office of Cyber Defense Coordination will manage a statewide cyber strategy to deter malicious cyber actors from conducting cyber-attacks against the State of Nevada and its interests. As part of this effort, the Office of Cyber Defense Coordination will champion an interconnected framework of initiatives to enable the State of Nevada to work with public and private stakeholders to effectively prevent, respond to, and mitigate the impact of cyber-attacks in Nevada.

The specific goals outlined in this strategy represent new and ongoing efforts to realize an improved cyber security posture across the State of Nevada. This document identifies essential and achievable goals to enable and empower entities across the State of Nevada to improve their unique cyber security posture. Further, this strategy contains goals for improving cyber security education, training, and bolstering the cyber security workforce in Nevada.

## 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 incident **response** process by prescribing relevant incident response plan criteria, standardization, and conducting exercises to strengthen those plans.
3. Enable organization's ability to counteract malicious cyber-actors by **coordinating** information, 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 current cyber resources, threat intelligence, mitigation techniques, and lessons learned to better identify risk and prevent attacks on the information systems in the State of Nevada.

**Incident Response –** OCDC will continue to build statewide cyber incident response capacity. Standardization across political subdivisions, improved response capabilities, robust partnerships all contribute to mature cyber incident response, which OCDC will lead.

**Partner Collaboration -** OCDC will continue to coordinate information, intelligence, and resource sharing throughout the State by leveraging continuously evolving partnerships. These efforts will enhance the sharing of information and collaboration among appropriate state, local, and federal entities.

**Cybersecurity Investment –** OCDC will continue to provide awareness and best practices regarding investments in technology, infrastructure, and personnel to address cybersecurity in the protection of information systems throughout Nevada. Leveraging economies of scale, improving access to tools, resources, and training will be critical to combat the significant and dynamic cyber threat.

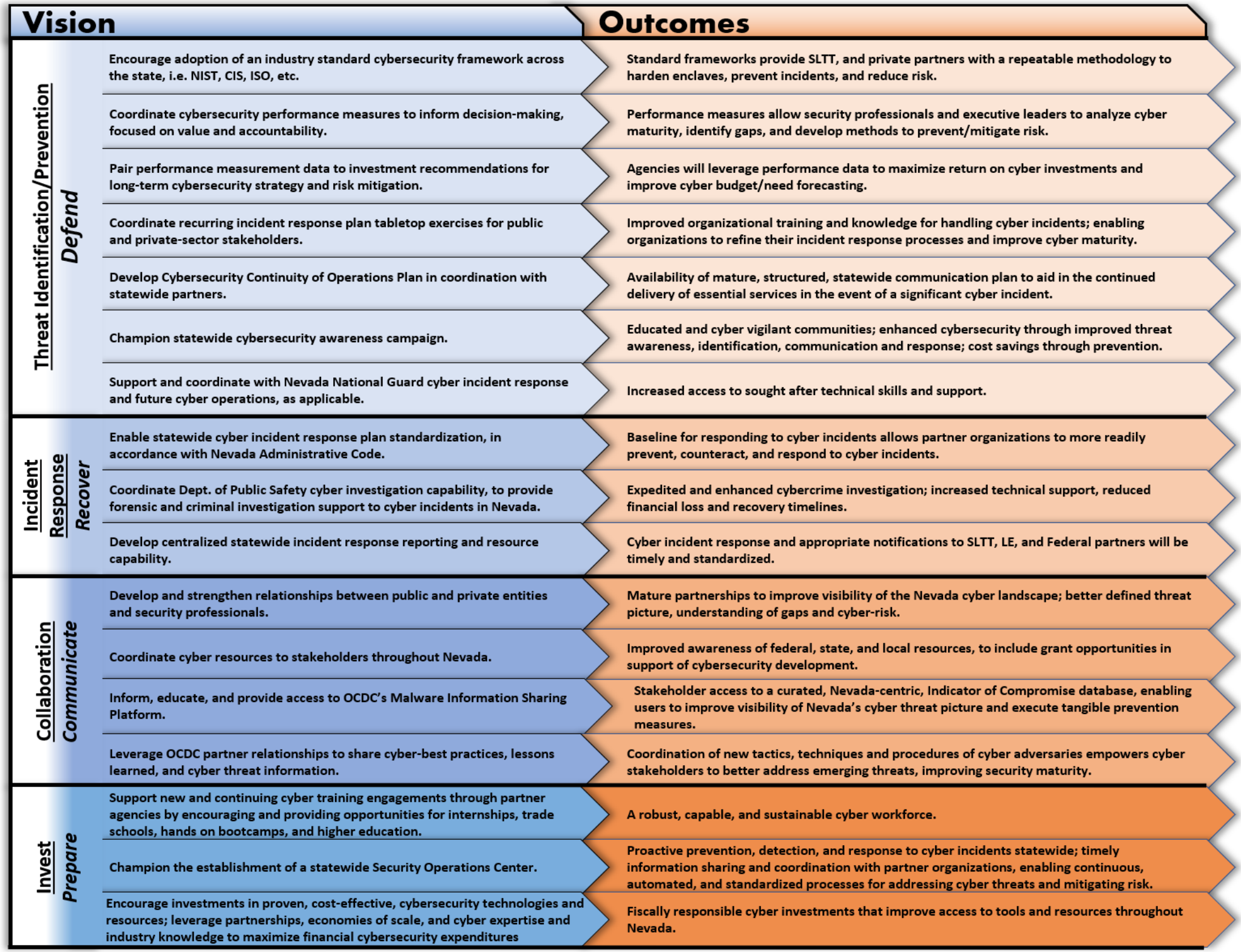
## Recent Milestones and Continuing Challenges

### Recent Milestones

- In the 80th Legislative Session, OCDC was directed by the Nevada Legislature to develop regulation for the development, management, and retention of cybersecurity incident response plans for all Nevada Cities and Counties.
- OCDC, in partnership with Nevada-based not-for-profit organization, CyberSmartNV, created a public web-based focal point for cybersecurity resources, information, events, and collaboration for all Nevadans.
- OCDC, in partnership with the Dept. of Public Safety – Division of Investigation and the Federal Bureau of Investigation, created two cybersecurity investigator positions to serve on the FBI Cybercrimes Task Force –increasing the State's role in cyber investigation and response.

### Continuing Challenges

- "Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. Cyberattacks are the fastest growing crime globally, and they are increasing in size, sophistication and cost." – Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac
- The cyber threat landscape continues to transform, and with a limited number of mature cybersecurity programs in Nevada – whether government or private sector – the need for organizations to increase investments in agile and resilient security is paramount.


Vision
Outcomes
Threat Identification/Prevention
Defend
Encourage adoption of an industry standard cybersecurity framework 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 cybersecurity expenditures
Fiscally responsible cyber investments that improve access to tools and resources throughout Nevada.