Nevada Office of Cyber Defense Coordination

Strategic Plan 2018 - 2020

Nevada Department of Public Safety

Table of Contents

Executive Summary

"The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United State and abroad." Presidential Policy Directive/PPD-41.

Malicious cyber activities are conducted for a variety of reasons including: financial gain, information/intellectual property theft, activist causes, to disable computer systems or to disrupt critical infrastructure and vital resources of a government or organization.

To address the increasingly diverse cyber threat environment, the Nevada Office of Cyber Defense Coordination will implement a comprehensive cyber strategy to deter state and non-state actors from conducting malicious cyber activity against the State of Nevada and its interests.

The Nevada Office of Cyber Defense Coordination will invest in a framework to enable the State of Nevada to work with public and private stakeholders to effectively respond to and mitigate the impact of cyber attacks in Nevada.

The specific goals outlined in this strategy represent the first step to realizing 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.

"Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the U.S. and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. The threats are amplified by our ongoing delegation of decision making, sensing, and authentication roles to potentially vulnerable automated systems. This delegation increases the likely physical, economic, and psychological consequences of cyber attack and exploitation events when they do occur." Daniel R. Coats, Director of National Intelligence, 2017

Introduction

> *"At the end of the day, cyber security is not about technology, it's about managing risk." Brigadier General (retired) Gregory J. Touhill – the first Chief Information Security Officer (CISO) of the United States*

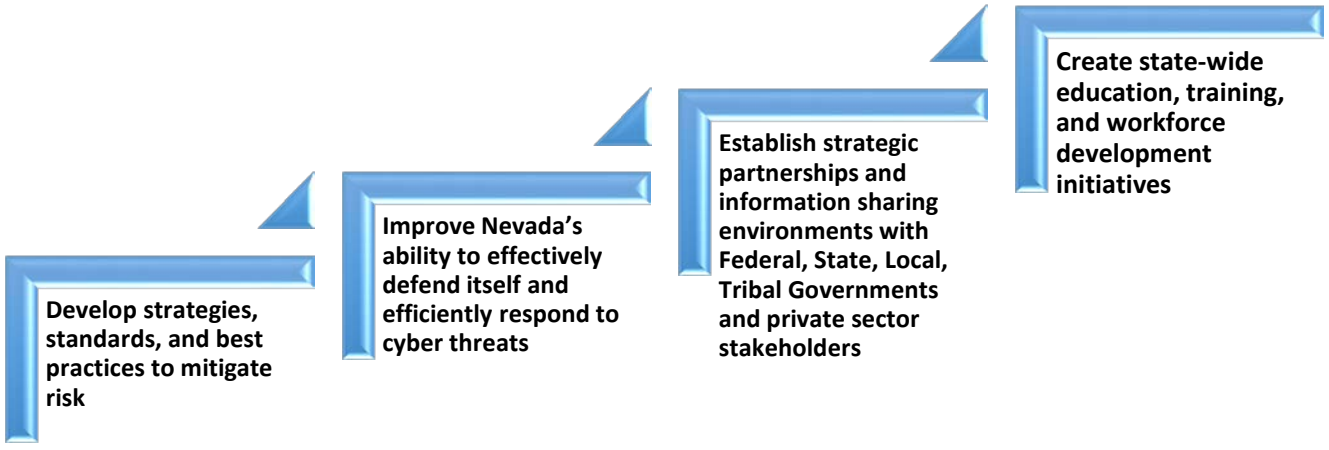
The inception of the Nevada Office of Cyber Defense Coordination (OCDC) stems from Nevada Governor Brian Sandoval's initiative to champion cyber security across the State of Nevada. Announced as a leading priority during the Governor's 2017 State of the State address, OCDC gained traction as Assembly Bill 471 and received a wealth of support from myriad government and non-government organizations across the state. On June 2, 2017, Assembly Bill 471 was passed into law, establishing the Nevada Office of Cyber Defense Coordination. OCDC is housed under the Nevada Department of Public Safety, allowing for simplified coordination of support resources.

The Office of Cyber Defense Coordination will work with state and partner components for the synchronization and coordination of strategic cyber security initiatives within Nevada. The Office of Cyber Defense Coordination will not replicate existing programmatic or budgetary mechanisms, or interfere with previously defined cyber security roles; rather, it will provide a single platform to integrate cyber security initiatives, manage strategic policy and planning, and streamline cyber security governance structures. Further, OCDC will provide senior-level advice and recommendations on key cyber issues to the Governor's Office, Nevada State Legislature, state agencies, political subdivisions, tribal governments, private-sector entities, and the Nevada Commission on Homeland Security.

Mission and Vision

OCDC Mission: The Nevada Office of Cyber Defense Coordination serves as the primary focal point for cyber security strategy, policy, planning, and coordination for the State of Nevada.

OCDC Vision: To become a State leader in cyber security information management, by coordinating information, enabling effective risk management decisions, addressing cyber threats and advancing cyber security education and training. Key objectives include:



2018 – 2020 Strategic Goals

Strategic Goal 1: Adopt Information Management Policies, Guidance, and Best Practices

Current governance mechanisms require modernization and enhancement to meet the dynamic cyber threat landscape. As an example, recent data breaches across the United States highlight the need for improved governance structures and the elimination of silos. OCDC will develop methodologies to standardize cyber security practices by investing in appropriate policy, regulation, emerging technologies, and best practices.

- **Goal 1.1:** The OCDC will develop a framework to complement existing business and cyber security operations in a holistic effort to identify, assess, and manage cyber security strategy and risk for the State of Nevada and its interests.
- **Goal 1.2:** Develop cyber security performance measures to inform decision-making, highlight value, and ensure accountability.
    - As stewards of public funds, it is the responsibility of this office to establish clear and tangible cyber security objectives with measured outcomes, as able.
- **Goal 1.3:** Develop, in coordination with stakeholders, recommendations regarding State of Nevada cyber security funding appropriations. Additionally, OCDC will ensure state investments are aligned to support a whole-of-government approach to effective cyber security.
- **Goal 1.4:** Craft or enhance continuity of operations plans and procedures to enable the State of Nevada to conduct business activities within a degraded or disrupted cyber environment, in the event of a successful cyber attack.
- **Goal 1.5:** OCDC will leverage private sector cyber security subject matter experts for input on trending cyber threats, best practices and guidance, and to perform unique ad hoc support and enhance the limited cyber security workforce, as necessary.

Strategic Goal 2: Safeguard Information Systems against Cyber Threats

Protection of Nevada's critical information resources is paramount to Nevada's growing economy, health, and public safety. As part of this strategy, OCDC will work with key allies and partners to build networked cyber security capacity in an effort to secure critical infrastructure and key resources which Nevada depends on for the continued delivery of essential services.

"The evolution of ransomware in 2017 should remind us of how aggressively a threat can reinvent itself as attackers dramatically innovate and adjust to the successful efforts of defenders," Steve Grobman, Chief Technology Officer, McAfee, LLC

- **Goal 2.1:** OCDC will develop methodologies to efficiently evaluate State of Nevada information systems, in addition to associated policies, procedures, identified gaps, overlaps, conflicts, and areas in need of modernization. As part of this goal, OCDC will:
    - Assess the cyber security posture of individual state agencies and associated strategies and assess the State of Nevada's ability to deter state and non-state actors from conducting successful cyber attacks against Nevada and its interests.
- **Goal 2.2:** Understanding the wealth of unique state business operations/objectives, legal and regulatory requirements, and organizational constraints, OCDC will establish risk-based assessments of information systems operated and maintained by state agencies.
    - Through identification and prioritization, OCDC will develop strategies to mitigate identified security gaps and risk to critical and non-critical assets.
- **Goal 2.3:** Develop a cyber threat intelligence sharing platform to aid in situational awareness, risk management, system readiness, and identification of appropriate controls, as funding permits.
- **Goal 2.4:** Develop processes to accelerate notification of cyber security incidents to state and partnering entities.

Strategic Goal 3: Develop Incident Response, Triage, and Recovery Teams

In an effort to address and respond to identified cyber attacks, OCDC will mitigate the impact of cyber incidents through the creation of cyber response teams, with a focus to expand continuity of operations, reduce impact time, and increase resiliency. Cyber attacks are more dynamic than traditional threats and require timely response. Development of a response governance structure to adequately prepare and secure the state in an evolving threat landscape is paramount.

- **Goal 3.1:** Create cyber incident response teams with elements of Department of Public Safety Division of Emergency Management, Division of Investigation, and Department of Administration Enterprise IT Services; additional team participation from federal, state, local, tribal governments and private-sector elements, as appropriate.
- **Goal 3.2:** Ensure recovery elements have clear understanding of organizational key assets, risk assessments, threat landscape, potential impact, and current controls in place to protect assets.

- **Goal 3.3:** Develop defined protocols and responsibilities for responding to cyber incidents/attacks.
- **Goal 3.4:** Develop and coordinate cyber security incident response training exercises with state and non-state partners to mature cyber response capabilities and readiness.

Strategic Goal 4: Foster Partnerships to Strengthen Cyber Ecosystem

The cyber ecosystem encompasses a variety of diverse contributors – federal, state, local, tribal government, and private-sector partners. Achieving a successful cyber security ecosystem relies, in part, on extensive and resilient partnerships that cultivate innovation, information sharing, and best practices.

OCDC will initiate a series of programs to create a healthy cyber ecosystem with a focus on collaboration in real-time to anticipate and prevent cyber-attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a normal environment.

- **Goal 4.1:** OCDC will develop a framework through integrated capabilities and robust partnerships with federal, state, local, tribal government, and private-sector entities to strengthen and defend Nevada from cyber attacks.
- **Goal 4.2:** To improve Nevada's defensive posture, OCDC will generate partnerships and strategies with stakeholders to develop intelligence information sharing methodologies to disrupt or deter cyber attacks before they impact Nevada.
    - OCDC will further develop partnerships for the management and exploitation of cyber threat information aggregated through information sharing relationships.
- **Goal 4.3:** To improve cyber threat situational awareness, OCDC will develop strategies to leverage continuous, automated, and standardized mechanisms for sharing critical information with stakeholders across the State of Nevada.

Strategic Goal 5: Champion Cyber security Education and Training

To overcome the global cyber security skills shortage, Nevada must rely on the development of an effective local cyber security workforce. OCDC will champion programs which help Nevadans find the education and training they need to advance their careers and close the skills gap in the field of cyber security. Specifically, OCDC will promote robust cyber security education, training, and workforce development initiatives through comprehensive partnerships in academia, local government, and private sector entities to cultivate a highly capable cyber workforce.

"Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats." Robert Herjavec, founder and CEO at Herjavec Group

- **Goal 5.1:** OCDC will develop cyber education initiatives with Nevada colleges and universities to aid in the development of a robust cyber workforce.
- **Goal 5.2:** Research long-term cyber workforce needs for Nevada, and develop initiatives with government and not-for-profit workforce development agencies to encourage and strengthen advancement of cyber security careers.
- **Goal 5.3:** Create programs to inspire cyber security career awareness with students in elementary schools, stimulate cyber security career exploration in middle schools, and enable cyber security career preparedness in high schools.
- **Goal 5.4:** OCDC will raise awareness of the National Cyber Security Workforce Framework and encourage adoption.
- **Goal 5.5:** In collaboration with partner organization, OCDC will develop a training environment to conduct cyber attack exercises, experimentation, forensics, and assessment of cyber tactics, techniques, and procedures.

Conclusion

Legacy governance structures and policies will continue to prove ineffective in a dynamic cyber threat environment. Greater reliance on mobile devices, advances in artificial intelligence, expanded use of internet-of-things (IoT) connected devices, and the digital-physical world will further stress cyber security policy frameworks.

The development of a common language for internal and external communication of cyber security issues, efficient sharing of cyber threat information between stakeholders, improved situational awareness, and execution of best practices will be paramount for the successful strengthening of cyber security in Nevada.

The goals outlined in this strategy represent the first step to realizing an improved cyber security posture across the State of Nevada. For the Nevada Office of Cyber Defense Coordination to succeed in meeting these goals, leaders from across the state must take action to achieve the objectives outlined in this document. Collaboration, execution, and accountability will prove vital for the success of these initiatives. The cyber threat environment can change rapidly. We must remain dynamic, adaptable, and tenacious to enhance and drive the cyber security paradigm forward.