2017

Initial Report of the Cyber Security Committee

Nevada Commission on Homeland Security
November 20, 2017

Nevada Department of Public Safety
Division of Emergency Management and Office of Homeland Security

State Capitol Building
101 N. Carson St., Ste.2
Carson City, NV 89701
775.684.7111

Grant Sawyer Building
555 E. Washington Ave., Ste. 5500
Las Vegas, NV 89101
702.456.2400

OFFICE OF THE LIEUTENANT GOVERNOR
Mark A. Hutchison

November 20, 2017

Dear Colleagues:

As Chair of the Nevada Cyber Security Committee, Nevada takes very seriously the considerable cyber threats that our state faces at any given time. Recognizing these threats, Nevada has worked to coordinate existing efforts, determine best practices, and encourage strategic efforts to build upon the successes of our work in recent years. The following report aims to document much of these efforts to ensure that Nevada's future work in cyber security can build upon our existing foundation.

Under the chairmanship of Governor Brian Sandoval, the Nevada Commission on Homeland Security serves as a key leader in cyber security administration for Nevada. In recent years, the Commission has selected cyber security as a priority for grants funding and during the Commission's annual Threat and Hazard Identification and Risk Assessment [THIRA] survey. The Commission's prioritization of cyber security in recent years led to the establishment of the Cyber Security Committee as a subcommittee of the Commission, as well as the passage of Assembly Bill 471 during the 2017 Legislative Session, which created the Office of Cyber Defense Coordination within the Nevada Department of Public Safety.

Since April 2017, the Cyber Security Committee has deliberated on various aspects of Nevada cyber security capabilities, including the drafting and consideration of the following report. It is the Committee's hope that this report serves as a culminating document for the previous years of work and investment to date, and also as a foundational document for the Administrator of the newly created Office of Cyber Defense Coordination. Furthermore, to better illuminate the work on a statewide level, the Cyber Security Committee hopes this report will contribute to a broader understanding of Nevada's ongoing cyber security efforts.

This following report serves as an initial effort, with the continual investments to be made over time to grow Nevada's cyber capabilities into increasingly robust and resilient efforts in the future. Through the Governor's leadership, the Commission's input, and the Committee's focus, we have accomplished much, but more must be done to ensure that Nevada is able to prepare against, respond to, and recover from cyber attack.

Best regards,

Mark A. Hutchison
Lieutenant Governor
State of Nevada

101 N. Carson Street, Suite 2
Carson City, NV 89701
Phone: 775.684.7111 Fax: 775.684.7110

555 E. Washington Avenue, Suite 5500
Las Vegas, NV 89101
702.486.2400 Fax 702.486.2404

TABLE OF CONTENTS

Initial Report of the Cyber Security Committee
Nevada Commission on Homeland Security
November 20, 2017

1. Executive Summary

This report serves as the initial report of the Cyber Security Committee (CSC), a committee of the Nevada Commission on Homeland Security (NCHS). It is intended to capture much of the great effort that has been made to protect Nevada's information technology infrastructure, its economy, and its residents and visitors to date. In doing so, it is also intended to serve as the foundation for future efforts to continue in this same effort. As this is the initial report of the CSC, the final report will be completed and available to the public in April of 2018, following the completion of the state's cyber security strategic plan by the Department of Public Safety's Office of Cyber Defense Coordination (OCDC).

In order to provide a relevant initial report, the CSC endeavored to accomplish two general goals. The first general goal of the CSC was to provide an overview of the background of efforts to date. The second general goal of the CSC was to develop findings and recommendations from that overview. Both of these goals combine to allow the CSC's initial report to not only solidify the successes from statewide efforts of the recent past but to also shape the future of cyber security success in the state. The final report of the CSC in 2018 will continue in this same effort.

This report begins with the CSC's effort to provide an overview of recent activities. This includes a history of the CSC, the makeup of its membership, an overview of its meetings to date, and the mission and purpose the CSC developed to guide its efforts. Also included is an overview of the CSC's role in vetting and refining cyber security grant proposals for the Homeland Security Working Group, the Urban Area Working Group, the Nevada Commission on Homeland Security, and its Finance Committee. The oversight of the Homeland Security Grant Program entails a lengthy process, but it has remained a deliberate effort that has resulted in identifying quality cyber security projects for funding, which have in turn been supported by state and local cyber security investments as well.

Based on findings from the overview of this background, this report also makes recommendations for future cyber security efforts. There are few recommendations included here, and to be clear, they are intended to be very general in nature. This is at least in part due to the CSC's decision to develop this report as an initial report in 2017 and as a final report in 2018, where the findings and recommendations will be more robust. In the meantime, the recommendations included here cover budgetary, policy, and operational considerations for the CSC, OCDC, Nevada's Enterprise Information Technology Services (EITS), as well as other contributors to the statewide cyber security effort. The centerpiece of both of the

goals described above is the newly-established OCDC within Nevada's Department of Public Safety. This office, which was envisioned and championed by Governor Sandoval and his staff, was approved through the 2017 Legislative Session and signed by Governor Sandoval. Described in detail within this report, the OCDC will serve a strategic and coordinating role for cyber security within the state. Not only will it be able to build off many of the successes to date, but it is the CSC's hope that the recommendations provided here are included in the OCDC Administrator's strategic planning, partnership, and collaboration efforts.

This report captures a great deal of work that has taken place to date, but it also necessarily serves as a roadmap for the way ahead. Although the cyber threat is constantly evolving, through efforts like this, the NCHS's emphasis on cyber security, the OCDC, and the ongoing investment of federal and state dollars in cyber security and cyber defense, Nevada will be better able to evolve with and respond to that threat. That is in line with the CSC's mission, and with the best interests of the people of Nevada.

2. History of the Cyber Security Committee

Following the attacks on September 11, 2001, and the creation of the Department of Homeland Security (DHS), Chapter 239C was added to the Nevada Revised Statutes (NRS) which created the Nevada Commission on Homeland Security (Commission). This chapter of NRS provided the specific duties and makeup of the Commission and established the legal framework for its work. Since it was first established, the Commission has remained the central strategic and guiding force of Nevada's Homeland Security efforts which has only increased in stature since Governor Brian Sandoval chose to serve as the Commission's Chair.

The duties outlined in NRS 239C include overseeing the grants process, advising on homeland security related issues, ensuring coordination of emergency response capabilities, and several other important functions. Additionally, NRS 239C.170 authorizes the Chair of the Commission to create a Committee on Finance, as well as "any other committees deemed necessary by the Chair to assist in carrying out the duties of the Commission." On September 24, 2014, the Commission authorized the creation of the Cyber Security Committee (CSC) to address the protection and resiliency of statewide technology.

In general, the CSC was formed to provide input for the grants process as well as to provide subject matter expertise on matters related to cyber security. To accomplish this, cyber security expertise was sought on a statewide basis to represent the CSC membership, including cyber security, information technology,

and critical infrastructure at a federal, state, county, city, and private sector level. A list of the current members of the CSC is provided below:

Nevada Commission on Homeland Security		
Cyber Security Committee Membership		
Name	**Title/Organization**	**Committee Status**
Mark Hutchison	Lieutenant Governor, Nevada	Chair - Voting
Terry Daus	Information Security Manager, City of Henderson	Vice Chair - Voting
Randall Bolelli	Assistant Special Agent in Charge, Federal Bureau of Investigation	Voting Member
Caleb Cage	Chief, Nevada Division of Emergency Management and Homeland Security and Homeland Security Advisor (HSA)	Voting Member
Dennis Carry	Sergeant, Cyber Crimes, Washoe County Sheriff's Office	Voting Member
Bob Dehnhardt	Chief Information Security Officer, Nevada Department of Administration	Voting Member
Mehmet Gunes	Associate Professor, Department of Computer Science and Engineering, University of Nevada Reno	Voting Member
Greg Hearn	Senior Manager, Administration and Infrastructure, Las Vegas Valley Water District	Voting Member
Robin Heck	Manager, IT Security and Compliance, City of Las Vegas	Voting Member
Scott Howitt	Senior Vice President and Chief Security Officer, MGM Resorts, International	Voting Member
Joe McDonald	Chief Security Officer, Switch, Ltd.	Voting Member
Deron McElroy	Chief of Operations-West, Stakeholder Risk Assessment and Mitigation/Office of Cybersecurity and Communications, Department of Homeland Security	Voting Member
William Olsen	Vice President, Information Technology/Chief Information Officer	Voting Member
Shannon Rahming	Chief Information Officer, State of Nevada Enterprise IT Systems	Voting Member
Randy Robison	Director, State Legislative Affairs, CenturyLink	Voting Member
Cory Schulz	Colonel, Nevada National Guard	Voting Member
Rachel Skidmore	Emergency Manager, Las Vegas Metropolitan Police Department (LVMPD) (Chair of CIC)	Voting Member
Mike Smith	Chief Information Security Officer, Clark County	Voting Member
Justin Zhan	Associate Professor, Department of Computer Science, University of Nevada Las Vegas	Voting Member

The CSC met a total of three times in 2016. On March 8, 2016, the CSC was briefed with a complete overview of the Homeland Security Grant Program (HSGP) process and tasked with the development of priorities and objectives as a tool for reviewing and rank-prioritizing HSGP projects with a cyber security component. The establishment of priorities to which all cyber-related projects would be vetted was adopted by the CSC including:

- Alignment with the Department of Homeland Security (DHS) Cybersecurity Framework;
- Avoidance of conflict with Improving Critical Infrastructure Cybersecurity under Presidential Executive Order 13636;
- Review and ranking of HSGP projects for regional and/or statewide impact;
- 100% completion of project(s) within the allotted performance period of the grant;
- Sustainability of the project long-term;
- Compliance with the Commission's priorities and direction; and
- Compliance with Federal and State grant guidance.

Using this matrix, the CSC reviewed a total of 12 FFY 2016 HSGP project proposals totaling $2,823,853.00. Of these projects, only six were deemed to meet the established priority criteria. Those six projects were rank-prioritized, per funding stream, for further review and consideration by the Nevada Homeland Security Working Group (HSWG). Pursuant to NRS 239C.170[1], the CSC voted to approve Lieutenant Governor Mark Hutchison as the Chair of the CSC, and Joe McDonald, Chief Security Officer, Switch, Ltd., as Vice-Chair.

On September 7, 2016, the CSC was briefed on Presidential Policy Directive 41 (PPD-41) released on July 26, 2016, that set forth guiding principles to govern the federal government's response to a cyber incident effecting government or private sector entities. Of significance was the establishment of lead federal agencies and architecture for broader coordination in Federal response, and guiding principles including shared responsibility, risk-based response, respecting affected entities, unity of governmental effort, and enabling restoration and recovery. The CSC made the determination that PPD-41 may be considered in the examination of future projects for Nevada. Additional emphasis was placed on development of Nevada's cyber posture in reducing risk and utilizing the CSC not only as a grants project review body to develop unity with regard to cyber efforts across the state, but also to coordinate a baseline approach using best practices to address cyber security issues facing the state.

On December 13, 2016, the CSC was briefed on the current HSGP status in addition to the upcoming FFY 2017 HSGP process as it relates to cyber-related projects. With the prior approval by the Commission on September 22, 2016, and pursuant to NRS 239C.140, the CSC voted to hold a closed session to receive a cyber security briefing.

So far in 2017, the CSC has met three times. On March 29, 2017, the CSC reviewed and amended a baseline draft of the Nevada Cyber Security Committee Objectives and Recommendation report aimed at defining the long-term role of the

CSC's purpose with objectives and recommendations to include workforce, education, incident response and recovery, legal changes, and public information and awareness. Pursuant to NRS 239C.170 [1], the CSC voted to approve Nevada Lieutenant Governor Mark Hutchison, as the elected Chair of the CSC, and Terry Daus, Information Security Manager, City of Henderson, as the elected Vice-Chair. The CSC unanimously approved the use of established grant requirement objectives with the addition of requiring projects be in alignment with Presidential Policy Directive (PPD) 41 for the FFY 2017 grant process.

On May 2, 2017, using the approved grant requirement matrix, the CSC reviewed a total of five FFY 2017 HSGP project proposals totaling $917,040.00. All five projects were deemed to meet the established priority criteria, and were rank-prioritized, per funding stream, for further review and consideration by the Nevada Homeland Security Working Group (HSWG).

On October 31, 2017, the CSC met again with the primary intention of reviewing and approving this report and agreeing upon the course of action for completing and presenting it. During the meeting, the CSC reviewed various aspects of the report, developed several recommendations, and voted to allow the Division of Emergency Management to finalize the initial report ahead of the December NCHS meeting. Additionally, the chair established a subcommittee of CSC members to collaborate to develop the next round of recommendations to be included in the final report of the CSC in 2018.

In addition to the activities and efforts of the CSC, Governor Sandoval also introduced legislation that would greatly increase Nevada's cybersecurity capability while providing an additional opportunity for the CSC to provide input. Assembly Bill 471 (AB471) was passed during the 79th Session of the Legislature and signed by the Governor on June 2, 2017. The bill became effective on July 1, 2017.

AB471 established the Office of Cyber Defense Coordination (OCDC) within the Nevada Department of Public Safety (DPS) and outlined the office's duties and responsibilities. OCDC will be headed by an administrator appointed by the DPS Director, and who will also serve as an *ex officio*, non-voting member of the Commission. The primary function of OCDC will be to periodically review the information systems that are currently operating or being maintained by state agencies, including conducting performance audits and assessments of the systems to determine adherence to regulations and policies set up by the Division of Enterprise Information Technology Systems (EITS). OCDC will also serve as "the strategic planning, facilitating and coordinating office for cybersecurity policy and planning in this state," which will be done by coordinating statewide trainings to teach awareness and educate regarding risks to the security of the information systems used by State agencies.

To achieve these goals, OCDC will establish partnerships with state agencies (including the Nevada System of Higher Education), local governments and the private sector to encourage the development of strategies that can mitigate risks and protect IT systems maintained by both public and private sectors. OCDC will also partner with the federal government so it can assist in strategy development, as well as be available for the state to receive assistance if something should arise. To mitigate risks to information systems, OCDC will consult with DEM and EITS to develop strategies to prepare and protect the security of information systems.

Per AB471, OCDC is required to establish policies and procedures that would allow for state agencies to notify the office of threats to their information systems, and in turn for the office to notify other agencies and appropriate law enforcement or prosecuting authorities. When the gathering of intelligence is needed and the initiation of investigations into cyber threats occurs, OCDC will partner with the Investigation Division within DPS, specifically the Nevada Threat Analysis Center, to gather all pertinent information. When a threat has been received by a state agency or private entity, it is up to the Administrator to convene a Cybersecurity Incident Response Team, which will be made of members of state, local, and federal agencies.

Finally, OCDC is required to prepare and publish a statewide strategic plan every two years that outlines their policies, procedures, best practices and recommendations to mitigate the risk of cyber threats. It is also required to publish a yearly report, due no later than July 1 each year that includes a summary of the progress made by OCDC during the past year in executing and administering the duties outlined in AB471. The report must also include a general description of any threats to the security of an information system that required the response team to activate, as well as a summary of goals for the next year and any challenges they think they might face.

The CSC recognizes this extraordinary new capability and authority on cyber-related issues within Nevada and the potential opportunities that such an office provides. Given the significant threats posed by cyber attacks, the CSC supported this measure and will continue to do so through the Commission. This report is intended, in part, to provide a foundation for the new Administrator of OCDC by capturing the important roles, history, and investments made by the state, as well as recommendations for the OCDC Administrator to consider for the initial strategic plan.

3. Mission and Purpose of the Cyber Security Committee

Governor Sandoval, who also serves as the Chair of the Nevada Commission on Homeland Security, provided specific guidance on the CSC's focus. The appointment letter given to each member of the CSC provides the following quote:

> *The Cyber Security Committee is responsible for providing advice and recommendations to the [Nevada Commission on Homeland Security] on Nevada's cybersecurity risk, cyber threat preparedness posture, statewide cybersecurity plans, cyber related training and exercises, and enhancement of security awareness through education, public awareness, and engagement with public and private sector partners.*

This guidance not only provided a clear and concise direction for the CSC, but also allows the experts appointed to the committee to further develop the committee's scope through regular meetings.

During the March 29, 2017, CSC meeting, the committee agreed to make this direction the vision statement for its work. Additionally, the CSC established three agreed-upon roles that would define the purpose of the committee. In order to achieve the Governor's vision, the committee would:

1. Provide insight to the Nevada Commission on Homeland Security on cyber related issues;
2. Raise issues to the Commission on existing and emerging cyber gaps, threats, tactics and techniques; and
3. Guide the Commission on cyber security related issues.

Having established these three roles, the CSC developed the following mission statement:

> *The Cyber Security Committee serves the Nevada Commission on Homeland Security by providing advice and expertise, maintaining awareness of threats, and recommending strategic measures to combat those threats.*

Given this vision and mission, the CSC also developed two primary objectives for its work:

1. Vet and prioritize cybersecurity grant allocations for the Commission; and
2. Provide strategic cyber security budgetary and policy findings and recommendations for the Commission.

This report serves as the CSC's first major effort to fulfill these two objectives.

4. Objective 1: *Vet and prioritize cybersecurity grant allocations for the Commission*

As a result of the September 11, 2001 terrorist attacks, the passage of the Homeland Security Act of 2002 enabled DHS to act as a stand-alone, cabinet-level department tasked with addressing the coordination and unification of national homeland security efforts in 2003. The Homeland Security Grant Program (HSGP) was established as a funding mechanism to build and sustain national preparedness capability by enhancing the ability of states, local governments, and tribal governments to prepare, respond, and recover from terrorist attacks and other disasters. Funding received from the HSGP was applied to preparedness activities including Planning, Organization, Equipment Purchase, Training, and Exercise (POETE) in addition to management and administration costs. There has been significant improvement to the HSGP based on stakeholder input and risk assessments allowing the program to move from a completely competitive process to a national allotment process wherein funding streams within the HSGP are allotted specific amounts of funding based upon ongoing risk assessment-methodology. Presently, the HSGP plays an integral role in the implementation of the National Preparedness System through the support of building, sustaining, and delivering core capabilities that are essential to achieving the National Preparedness Goal of a secure and resilient nation. To do this requires the combined effort of the whole community in lieu of any exclusive effort on the part of single organizations or levels of government. Based on allowable costs, the HSGP is designed to support efforts to sustain and build core capabilities across five mission areas, including Prevention, Protection, Mitigation, Response, and Recovery. The HSGP is currently comprised of the following interconnected grant programs:

- **State Homeland Security Program (SHSP)**
  Provides assistance with state, local, and tribal preparedness activities addressing high-priority gaps in preparedness across all mission and core capability areas where a nexus to terrorism may exist. The SHSP funding stream is designed to support implementation of capability-based, risk-driven approaches addressing capability targets within urban area, state, and Threat and Hazard Identification Risk Assessments (THIRA). The THIRA process establishes capability targets, and those targets are assessed in the State Preparedness Report (SPR) as a mechanism to inform POETE needs to prevent, protect, mitigate, respond, and recover from terrorist acts or other catastrophic events.

- **Urban Area Security Initiative (UASI)**
  Provides assistance for unique capability-based and risk-driven POETE needs of high-density, high-threat urban areas on the basis of capability targets identified through the THIRA process and other associated assessment efforts. Additionally, assistance is provided to build sustainable and enhanced capacity to prevent, protect, mitigate, respond, and recover from acts of terrorism.

- **Operation Stonegarden (OPSG)**
  Supports enhanced coordination and cooperation among the United States Border Patrol, Customs and Border Protection, and local, state, tribal, territorial, and federal law enforcement agencies. Funding supports joint effort investments to secure borders and travel corridors between the United States and bordering countries of Mexico and Canada in addition to states and territories within international water borders.

Prior to 2012, two additional grant programs were included in the HSGP, namely the Metropolitan Medical Response System (MMRS) and Citizen Corps Program (CCP), both of which have been subsequently incorporated into the SHSP and UASI grant programs under the HSGP. Nevada currently qualifies for both the SHSP and UASI grant funding streams under the HSGP, and DEM is the designated State Administrative Agency (SAA) and sole entity eligible to apply for HSGP funding.

Over the course of the past eight years, the national HSGP funding allocation has declined significantly as the process for allocation transitioned from a reactive and competitive basis to a risk-based methodology used to allocate funding for state's preparedness activities. DHS uses comprehensive risk methodology with a focus on threat, vulnerability, and consequence to determine the relative risk of terrorism faced by a particular area. The risk is calculated on population affected, critical infrastructure, and the security of the economy. A noticeable trend in declining and stagnant HSGP allocations is seen from 2008 to 2016 equating to nearly a 39% drop in funding to 50 states and eligible territories. Figure 1 illustrates this declining trend in the HSGP program allocations including the SHSP, UASI, MMRS, CCP, and OPSG:

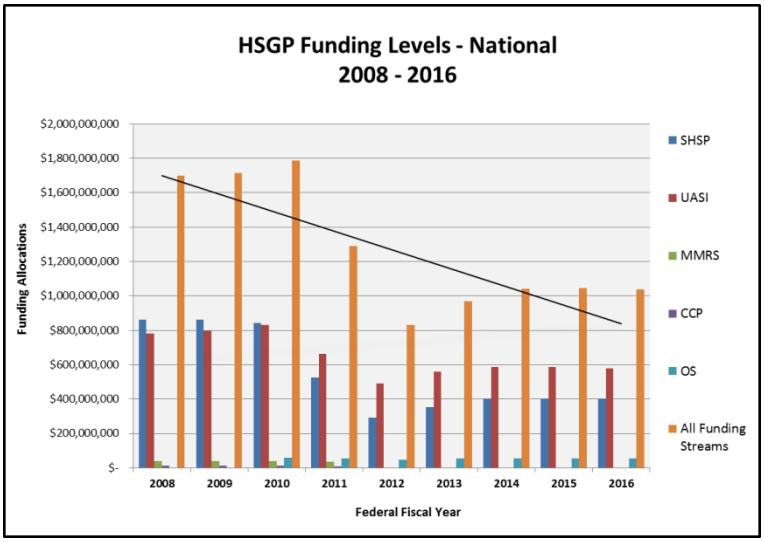


Figure 1. HSGP Funding Levels – National

Although the methodology for funding the SHSP remains based on minimum amounts established under legislative mandate in addition to DHS's risk methodology, the same cannot be said of the UASI methodology for funding. Eligible HSGP urban areas under the UASI funding stream are determined through analysis of the relative terrorism risk faced by the 100 most populated Metropolitan Statistical Areas (MSA) within the United States. As relative risk is assessed in a classified manner, predicting where a state will fall in the annual funding allocation remains a mystery. With the lack of certainty regarding whether UASI funding will be available for Nevada, there is a constant threat that Nevada may receive only its SHSP funding allocation which significantly impacts the Las Vegas Urban Area and subsequently the ability to fund statewide projects as SHSP funding then must be further spread to cover urban area projects with statewide impact.

Nevada is uniquely transparent with the HSGP process, specifically in the selection of SHSP and UASI projects requesting federal funding. As the process of administering the HSGP lies with DEM acting as the SAA, preparation for the process begins in the fall as DEM conducts a Threat and Hazard Identification Risk Assessment (THIRA), which is a multifaceted process by which all states identify the events or conditions under which state capabilities are planned for and measured. Though not specific to those events with a terrorism nexus, the THIRA is a federal requirement in obtaining HSGP funding, and input for the THIRA can come from a multitude of sources including after action reports, improvement plans, multi-year training and exercise plans, surveys, quarterly reports, and other THIRA assessments. Completion of the THIRA involves statewide participation and outreach to federal, state, county, city, regional, non-profit, and private sector

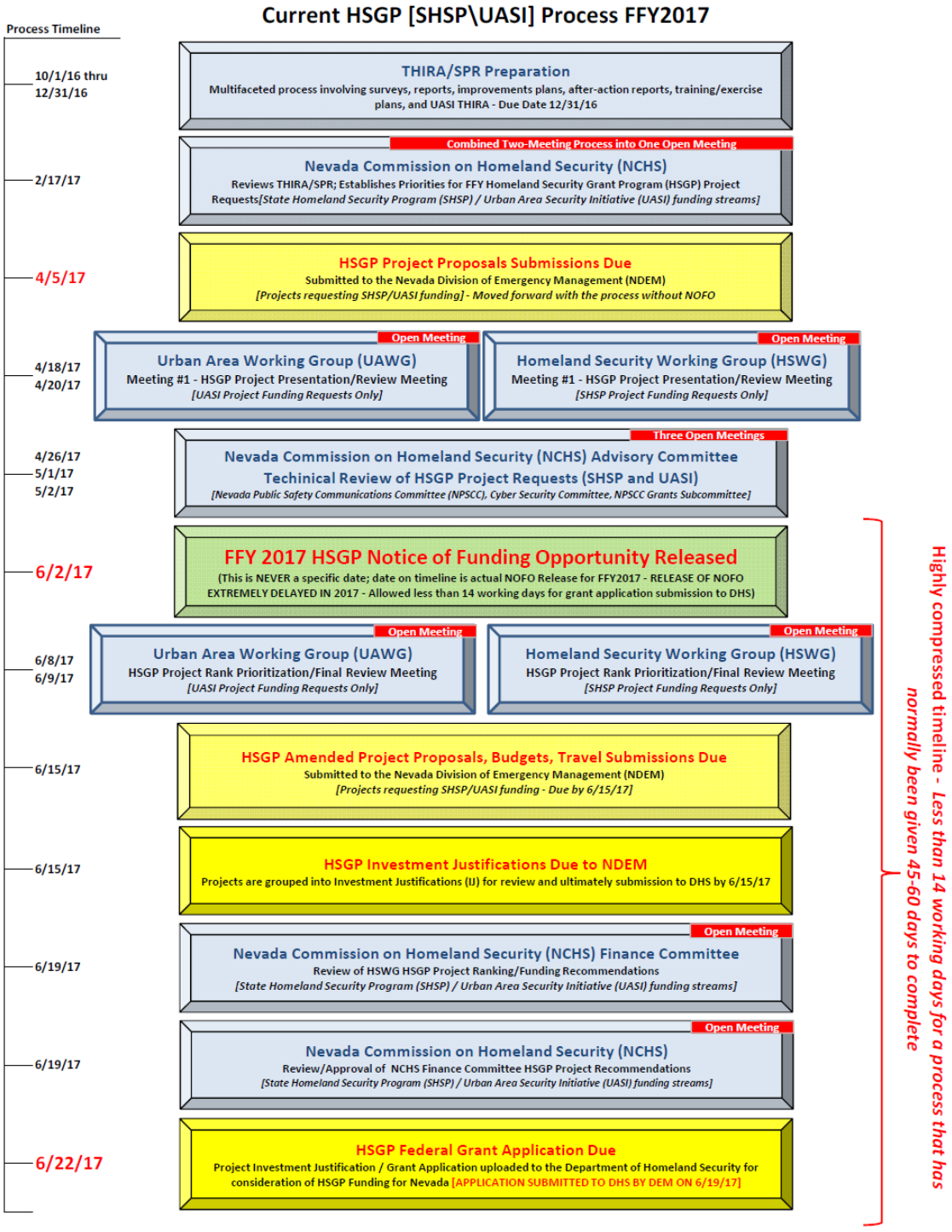
partners. The THIRA is the foundational assessment, under which the State Preparedness Report (SPR) is conducted. The SPR enhances this process by measuring the state's core capabilities contained in five mission areas against the events identified in the THIRA, with the requirement of each state to identify the top 5-6 events from the THIRA to measure capability against. This process has the ultimate goal, in theory, to build capability for the top 5-6 events identified in the THIRA.

Each January, the results from the Nevada THIRA are translated to a visual tool referred to as the "Nevada Heatmap" showing increases, decreases, or static change in each of the 32 core capabilities established by DHS. As foundational reports for the HSGP process, both the THIRA and SPR are integral in the creation of Nevada's capability priorities and ultimately the drivers of the final grant award for the state including the SHSP and UASI funding streams. With the completion of the THIRA and SPR, the process moves in an administrative direction over the course of the next three months with the management of the HSGP Notice of Funding Opportunity (NOFO) release and subsequent open meeting schedule allowing for the preparation, submission, vetting, and ultimate submission of the HSGP Grant Application to DHS. The allowable process time to complete these tasks ranges typically from 45-60 days. During this time, significant effort is placed on HSGP messaging, timelines, grant guidance, stakeholder outreach, project submission and review, and committee approvals necessary and required of the process.

Nevada is uniquely set up with a legislative mandate to provide a comprehensive state oversight structure for the coordination of domestic preparedness for acts of terrorism and related emergencies. Per Nevada Revised Statutes (NRS) 239C.160, the Nevada Commission on Homeland Security is tasked with making recommendations with respect to actions and measures that may be taken to protect residents and visitors of the state from potential acts of terrorism and related emergencies in addition to serving as the public body serving in review capacity for the state's applications to the federal government for homeland security grants and related programs.

Upon release of the THIRA and SPR data, the NCHS reviews and approves a selected number of core capabilities to be used in consideration of HSGP project requests for the current fiscal year. HSGP project solicitations are sent out through DEM, collected, reviewed, and summarized. The HSGP projects submitted for those projects with statewide impact are presented to the Nevada Homeland Security Working Group (HSWG) for review, vetting, technical review, and ultimately rank-prioritization for funding consideration. The HSGP projects submitted for those projects with Las Vegas Urban Area impact are presented to the Urban Area Working Group (UAWG) in a similar and parallel process. Recommendations from the HSWG and UASI are forwarded to the NCHS Finance Committee for additional

review, and then final funding recommendations are put before the NCHS for approval in submitting the final HSGP Grant Application to DHS.



The NCHS approved priorities for 2016 and 2017 include the core capabilities of Cybersecurity, Intelligence and Information Sharing, Public Information and Warning, Operational Coordination and Operational Communications. The cyber security capability is the need to protect, and restore if needed, electronic communications and services from damage, unauthorized use, and exploitation. The intelligence and information sharing capability is critical to provide timely and accurate information concerning physical and cyber threats to the United States, its people, property, or interests. The information gathered results from the planning, collection, processing, analysis and dissemination of available information. Public information and warnings allow for coordinated, prompt and reliable information sharing through the use of clear and consistent methods that are both culturally and linguistically appropriate so the message is effective for the whole community. This is supported by operational communications that ensure timely communications that support security and situational awareness between affected communities in the area impacted and the response forces. None of this is possible without the proper operational coordination that helps establish and maintain a unified and coordinated operational structure. It also helps integrate all the critical stakeholders and allows for the execution of core capabilities.

Overview and status of cyber security projects that have been funded by grant year.

Homeland Security Grant Program Cyber Projects

As of 11/21/2017

Subgrantee	Project	Allocation	Deobligated	Spent	Remaining Balance	Program Activities/Accomplishments
FFY 2013						
Department of Administration	Cybersecurity (SHSP)	$359,652.00	$ 95,321.47	$264,330.53	$ -	1. Fund 1 full time Cyber Analyst. Job duties include: monitoring State/County/City networks using commercial enterprise tools and receiving, interpreting and conveying cyber threat information from monitoring efforts and from other sources. 2. Purchase commercial network/endpoint traffic analysis service. 3. Purchase commercial global threat view portal service. 4. Conduct training classes.
City of Henderson	Statewide Data Disaster Recovery (SHSP)	$180,000.00		$180,000.00	$ -	1. Conduct Business Impact Analysis, Data Disaster Recovery Strategy and Planning for both the City of Henderson and the Las Vegas Metropolitan Police Department.
FFY 2014						
Department of Administration	Advanced Persistant Cyber Threats	$558,478.52	$ 9,361.99	$549,116.53	$ -	1. Purchase Firewall Audit Software. 2. Purchase Intrusion Prevention Software. 3. Purchase Kill Chain Software. 4. Purchase Encryption Software. 5. Professional services to aid in deployment of new software (includes travel to various locations implementing software).
Washoe County Sheriff's Office	Cybersecurity (SHSP)	$205,238.00	$ 2,397.10	$202,840.90	$ -	1. Purchase forensic computers & associated software. 2. Purchase network scanning tools. 3. Purchase network routers and switching devices. 4. Purchase forensic imaging devices. 5. Purchase server equipment. 6. Purchase laptops for mobile response. 7. Purchase network attached storage arrays.
FFY 2015						
Department of Administration	Cyber Protection (SHSP)	$468,842.00	$ 2,913.77	$212,869.33	$ 253,058.90	1. Coordination and evaluation of the Cybersecurity Protection Grant Partnership. 2. Security Monitoring and analysis, statewide. 3. Security Monitoring and analysis, City of Henderson. 4. Security Monitoring and analysis, City of North Las Vegas.
Washoe County Sheriff's Office	Cybersecurity (SHSP)	$134,100.00		$134,010.41	$ 89.59	1. Purchase forensic software to analize malware and attack methods. 2. Purchase server storage, protection and networking component upgrades. 3. Purchase network scanning devices. 4. Purchase Cardnal Wireless Scanner. 5. Purchase network attached storage arrays. 6. Outfit a custom forensic password cracking computer station. 7. Outfit 3 computer forensic workstations.
Clark County	Disaster Recovery (UASI)	$180,000.00	$ 30,000.00	$150,000.00	$ -	1. Vendor for an architectural review and recommendations for the SCOPE II co-located failover system.
City of Las Vegas	Web Application Firewall (UASI)	$ 31,000.00	$ 983.40	$ 30,016.60	$ -	1. Purchase and installation of a web application firewall device. Includes a vendor product manager, project manager and training.
City of Las Vegas	Oracle Access Manager (UASI)	$110,000.00		$ 22,000.00	$ 88,000.00	1. Funds for a Project Manager, Product Specialist and Product Engineer 2. Software training.
FFY 2016						
City of Henderson	Cyber Incident Response Planning ($52,000 from SHSP & $84,000 from	$136,000.00		$ 609.98	$ 135,390.02	1. Creation of a Cyber Incident Response Program that includes policies, plans, procedures and runbooks. 2. Training for incident response.
University of Nevada, Reno	Cyber Statewide Capacity and Needs	$100,000.00		$ 305.86	$ 99,694.14	1. Faculty for Cyber Security Center & Center for Applied Research. 2. Complete research, Needs Assessment, Gap Fit Analysis, Policy Barriers and Recommendations, and Funding/Financing Strategy. A final report will be compiled.
Washoe County Sheriff's Office	Cybersecurity (SHSP)	$ 25,375.00		$ 11,523.16	$ 13,851.84	1. Purchase forensic software to analyze malware and attack methods. Also includes encryption breaking software. 2. Purchase network scanning devices. 3. Purchase server storage, protection, and networking component upgrades.
Department of Administration	Information Security Management	$572,306.00		$ -	$ 572,306.00	1. Purchase APT Phase II; Preemptive Breach Detection System. 2. Purchase Enterprise Risk Management Tool. 3. Purchase Systemic Disaster Recovery Evaluation Tool. 4. Purchase Security Risk Dashboard. 5. Purchase Data Loss Prevention Tool.
Ely Shoshone Tribe	Cybersecurity (SHSP)	$ 3,000.00		$ -	$ 3,000.00	1. Purchase 38 operating systems to protect against everyday cyber attacks

Prioritized list of cyber security grant recommendations for consideration by the Homeland Security Working Group and the Urban Area Working Group.

Nevada Commission on Homeland Security - Cyber Security Committee				
APPROVED FFY16 HSGP PROJECT PROPOSAL REVIEW RANKING - MARCH 8, 2016				
Project ID	Project Name	Investment Justification	Agency	RECOMMENDED RANK
SHSP PROJECTS ONLY				
SHSP Project Proposals were ranked in the following order (1 = Highest Priority, 5 = Lowest Priority)				
A	Information Security Management System Modernization	Cybersecurity	State of Nevada EITS	1
E	Cyber Incident Response Planning	Cybersecurity	City of Henderson	2
D	Washoe County Cyber Security	Cybersecurity	Washoe County Sheriff's Office	3
C	Nevada Cyber Statewide Capacity and Needs Assessment Plan	Cybersecurity	University of Nevada Reno	4
F	Ely Shoshone Tribe Cyber Security	Cybersecurity	Ely Shoshone Tribe	5
UASI PROJECTS ONLY				
UASI Project Proposals were ranked in the following order (1 = Highest Priority, 2 = Lowest Priority)				
E	Cyber Incident Response Planning	Cybersecurity	City of Henderson	1
I	Geospatial Security and Data Exchange	Cybersecurity	Clark County Information Technology	2

Nevada Commission on Homeland Security - Cyber Security Committee				
APPROVED FFY17 HSGP PROJECT PROPOSAL REVIEW RANKING - MAY 2, 2017				
Project ID	Project Name	Investment Justification	Agency	RECOMMENDED RANK
SHSP PROJECTS ONLY				
SHSP Project Proposals were ranked in the following order (1 = Highest Priority, 3 = Lowest Priority)				
A	Cyber Security Capabilities	Cybersecurity	State of Nevada EITS	1
B	Washoe County Sheriff's Office Cybersecurity	Cybersecurity	Washoe County Sheriff's Office	2
C	Nevada Cybersecurity Workforce Development	Cybersecurity	University of Nevada Reno	3
UASI PROJECTS ONLY				
UASI Project Proposals were ranked in the following order (1 = Highest Priority, 2 = Lowest Priority)				
E	Mesquite Network Security	Cybersecurity	City of Mesquite	1
D	Southern Nevada SCADA System Cybersecurity Assessment	Cybersecurity	Las Vegas Water District	2
SHSP/UASI PROJECTS COMBINED				
SHSP and UASI Project Proposals were ranked in the following order (1 = Highest Priority, 5 = Lowest Priority)				
A	Cyber Security Capabilities	Cybersecurity	State of Nevada EITS	1
B	Washoe County Sheriff's Office Cybersecurity	Cybersecurity	Washoe County Sheriff's Office	2
E	Mesquite Network Security	Cybersecurity	City of Mesquite	3
D	Southern Nevada SCADA System Cybersecurity Assessment	Cybersecurity	Las Vegas Water District	4
C	Nevada Cybersecurity Workforce Development	Cybersecurity	University of Nevada Reno	5

5. Objective 2: *Provide strategic cyber security budgetary and policy findings and recommendations for the Commission*

Based on this overview of the CSC and the statewide grant process for homeland security and cyber security, the CSC developed the following recommendations. These recommendations are intended to be general in nature, and they are intended to provide an initial starting place for further planning and discussion. The recommendations are provided below.

Recommendation 1: The OCDC Administrator should establish metrics to assess successful cyber security grant proposals submitted to the Nevada Commission on Homeland Security.

Recommendation 2: The OCDC Administrator should develop a cyber security funding map for the next five years to provide focus for state general fund and federal grant investments. In order to assist with this recommendation, and in addition to the overview of grant expenditures provided on previous pages, an overview of cyber security investments made by the legislature through the state's Enterprise Information Technology Services Division is provided below.

Budget Account (BA) 1389 – BUDGET TOTALS

2019 – $ 2,384,383 (does not include grant funding)
2018 – $ 2,319,392 (does not include grant funding)
2017 – $ 1,775,999 (does not include grant funding)
2016 – $ 1,727,283 (does not include grant funding)
2015 – $ 1,123,589 (does not include grant funding)
2014 – $ 1,119,832 (does not include grant funding)

BA 1389 – ACTUAL BUDGET SPEND TOTALS

2017 – $ 2,031,102 (includes work programs)
2016 – $ 2,270,463 (includes work programs)
2015 – $ 2,031,650 (includes work programs)
2014 – $ 2,138,874 (includes work programs)

Cyber security initiative funding Fiscal Year (FY) 2018/2019 for BA1385 and BA1386:

BA1385: FY18 - $347,182; FY19 - $142,561
BA1386: FY18 - $53,852; FY19 - $42,909

EITS HSGP Cybersecurity

2017 – $250,000
2016 – $572,306
2015 – $465,928

Notes: other state agency budgeted expenditures on cyber security are not available at this time; DEM has the details on the other HSGP cyber security related grants.

Recommendation 3: Working with other state, tribal, local, and private partners, OCDC should establish operational and information sharing protocols for cyber security within Nevada.

Recommendation 4: Together with the CSC, OCDC should develop a framework by which CSC can assess future grant projects for funding and recommendation to the NCHS.

6. Conclusion

Through this report, the CSC has provided a general framework of cyber security activity in our state. In recent years there has been considerable investment, attention, and focus on developing important cyber security capabilities and capacity, and these efforts have led to considerable success. With this focus and investment, though, the Governor and the Nevada Commission on Homeland Security have identified need for strategic focus on coordination. This report intends to contribute to addressing these needs, particularly in assisting the new Administrator of the Office of Cyber Defense Coordination.

Considerable interest and energy around cyber security in Nevada continues, and it should. The threats to Nevada's information technology infrastructure, and the subsequent consequences for Nevada's economy, society, and ability to provide government services remain high, and they are evolving. Nevada must, and it certainly will, continue to think strategically about investing in cyber defense and preparing against cyber threats.

A great deal of work has taken place to date, as seen in this report, but for those efforts to continue to be meaningful in the future, Nevada must remain focused. The CSC hopes that this initial report provides the basis of a roadmap for the way ahead. And it remains committed to working with statewide partners to ensure our safety and security.