Executive Summary

The University of Nevada, Reno (UNR) ranks among the top 150 national universities in research and development. Researchers at UNR are nationally and internationally known in areas that include earthquake engineering, renewable energy and environmental science. It is a High Activity Research University with a goal of obtaining a Very High Activity Research University designation. To attain that goal requires a significant cyberinfrastructure (CI) to support the growing research agenda.

UNR’s collective effort in CI seeks to develop, provide, and communicate an evolving, customizable set of integrated, broadly defined, high-performance, cost-effective, and sustainable research IT capabilities and services to the University community and its collaborators. The foundation for this is a coherent collection of well-managed resources. These resources primarily consist of the following:

- Network capacity to collect data from multiple sources including remote sensor deployments.
- High performance compute capability, both on premise and off premise, including storage capacity with provision for protection both from disaster and unauthorized access.
- Data curation that preserves UNR research data and results and makes them appropriately accessible to the national and international research and education communities.
- Cybersecurity that both insures compliance and privacy but does not adversely affect the ability to collaborate and appropriately share data and information.
- Ability to monitor and measure performance of the UNR CI system.
- Adherence to the prevailing standards and best practices for CI.
- Access to expertise for advice and training on how to best use these resources.
- A sustainable business plan with an institutional governance process.

This plan is built on the work of many, including statewide EPSCoR efforts, CI plans of the Nevada Research Data Center, various UNR departments and research labs, the Office of Vice President for Research and Innovation and the Office of the Vice Provost and Chief Information Officer, and the UNR HPC committee.

Cyberinfrastructure Goals:

To achieve and maintain a robust CI environment UNR will horizontally integrate with intra-campus resources and vertically integrate with regional and national CI investments and best practices.

Specific goals for the UNR CI plan include the following:

1. Provide network services that support reliable, high-performance connectivity among research groups and clusters on campus, and University collaborators both nationally and globally that is IPv6 enabled and a research network DMZ with full SDN capability.
2. Continuing expansion and evolution of High Performance Computing (HPC) capabilities including a sustainable operations plan to support high-end computational research efforts on campus.
3. Enhance collaborative relationships with national HPC and CI centers (e.g., NSF XSEDE, Open Science Grid, NIH CTSA) to support high-end users and their most demanding applications.
4. Leverage CI assets across the UNR campus and seamless access to CI assets external to UNR.
5. Enable eduroam and continue to adhere to InCommon protocols for secure, transparent access.
6. Develop the human resources to increase CI support and expand baseline CI knowledge and technology adoption among students and faculty.
7. Develop defined, sustainable, and extensible research data storage and curation capabilities.
8. Provide collaboration tools for virtual and physical communities (research & education).
9. Expand and extend capacity and robustness for sensor networks across the great basin and statewide that can be used for multiple research efforts.
10. Implement a governance structure with oversight of a sustainable business plan that can be executed by the appropriate central and distributed units across UNR.

Network Infrastructure

Current

The network (Figure 1) core is a diverse series of five routers (Brocade VDX) fully meshed in a VCS fabric with 40 Gbps links, allowing for data to move through the core at 160 Gbps. These are dispersed around campus to fiber aggregation nodes with UPS and generator back-up. The campus is segregated into 17 regions each having two 10 Gbps links using single mode fiber to the diverse core allowing for redundancy and high throughput. Each building has connectivity via fiber with a mix of 1 Gbps and 10 Gbps links based on traffic requirements. Wireless connectivity is integrated as a core part of the total campus network. In 2014 and 2015 wireless access points (WAPs) were expanded to all research and instructional spaces.

To provide researchers a dedicated network, a Science DMZ environment was deployed in 2015 reserved specifically for research related traffic. The Science DMZ is connected to each border router using 10 Gbps links and is available in two on-campus colocation datacenters and in the computer science building. Nodes are connected at 1 Gbps ports; however, 10 Gbps capacity is available as needed. All routers, core devices and firewalls are IPv6 capable. As of 2016, IPv6 connections are only available in the Science DMZ for research purposes. All routers, core devices and firewalls are OpenFlow 1.3 capable. In 2016, SDN is supported on all Science DMZ nodes for research applications. The network is configured to follow best current practices for network ingress filtering as documented by the Internet Engineering Task Force in BCP 38 defined by RFC 2827. Each campus subnet has an anti-spoofing ACL to ensure only valid IP addresses can be used. Rules are in place to ensure RFC 1918 addresses are not allowed over WAN links.

UNR is connected to Internet2 via the Nevada System of Higher Education System Computing Services (SCS) which maintains a 100 Gbps connection to the Internet2 backbone national network. The campus connected in 2016 to the SCS WAN via redundant 20 Gbps fiber connections.

Network performance is measured by perfSONAR. An initial installation of nodes (2015) measures performance both within the Science DMZ and inside the campus core. This deployment allows
throughput testing through the border firewall and is instrumental for evaluating network performance. SolarWinds and Intermapper are used to gather link information and provide reporting and alerts.

The Seismic Monitoring Networks are operated by the Nevada Seismological Laboratory and supported by several institutions and organizations. This is a mix of landline, microwave, and wireless networks. It provides transport for a statewide matrix of sensors that is aggregated at the laboratory located on the UNR campus and connected to the university network.

Plans for Future (Sustainability)
IPv6 will be extended to all network locations. Bandwidth will grow to a base of 10 Gbps to all locations and expand to 40 Gbps as needed to campus research facilities. The redundant connections to the WAN will grow to 40 Gbps and then to 100 Gbps as need is anticipated and funding is secured. Wireless coverage will expand to 100% of the campus. Measurement by perfSONAR will be expanded. Analysis of the collected data will be used to relieve network choke points. A goal of 100% wireless coverage will be pursued. Staff will gain training and expertise in SDN and work with researchers for appropriate use of SDN capabilities. The Seismic Monitoring Networks will be hardened and bandwidth capacity increased. Coordination will begin in fall, 2016 between UNR and other University of Nevada system institutions (Desert Research Institute, University of Nevada, Las Vegas) and the system network office to ensure the respective Research DMZ networks are compatible.

High Performance Computing & Storage
Current
To meet growing computation and storage demands of researchers UNR has committed to investing in a High Performance Computing (HPC) infrastructure and related support services. In February of 2015, our HPC cluster was upgraded to over 420 cores, 7 TB RAM, and 100 TB of storage, with InfiniBand connectivity. This system is available to all UNR researchers and graduate students. Additional HPC clusters of varying capacity are also prevalent on campus at departmental or individual researcher levels.

In 2016 a campus HPC Plan was adopted after review by the HPC committee, composed of researchers from across the campus. Implementation began in June, 2016. The resource access component of this plan includes three levels of activity: local, community condominium, and off premise. Local activities are those computing resources with a strong need to remain distributed at local points of research activity. The community condominium is the centrally located and managed HPC cluster for use by the entire UNR campus. Off-premise activity facilitates access to compute resources at other institutions or cloud based services to meet needs not addressed through the campus infrastructure. The community condominium’s business plan is based on a shared ownership and cost model with three tiered options for access: 1) shared ownership of the system, 2) chargeback for priority use, or 3) no charge for limited use of the system including graduate student use.

Scalable, high speed block and file storage systems provide campus access to consolidated data. An existing scale-out NAS solution provides over 160 TB of tiered file storage on a redundant platform that supports de-duplication. Redundant SAN’s with a dedicated fiber channel storage network provide 78TB of block storage and is co-located in campus data centers with backup generators, UPS, and environmental monitoring. All storage systems are backed up to a disk de-duplication appliance which is encrypted and replicated to an off-site facility.

The UNR NevadaBox service offers file storage and sharing hosted by a third-party cloud provider. This provides unlimited cloud storage with a secure sign-in, ability to store sensitive data, and the ability to share and collaborate with outside entities. In 2015 UNR Central IT began a dedicated research
An environment called Wolfcloud to provide robust, on-demand virtual server multiple O/S environments to faculty and sponsored students. Access to these resources from remote locations is available.

**Plans for Future (Sustainability)**
The expanded central HPC cluster will be in place in spring, 2017. Local storage capacity will be doubled in the same timeframe. Access to cloud compute and storage services will similarly be expanded. Until the business plan for the new HPC plan begins to cover both operational and expansion costs, the university will subsidize HPC central operations. Negotiations will continue to partner with major data center providers to provide space and power for the UNR HPC system.

**Research Data Management**

**Current**
The VPRI’s office established a digital repository in 2015 and data management services to enhance the research support available to the university’s faculty. ScholarWorks – UNR’s digital repository - assists in collecting, preserving, and distributing the university’s intellectual output. The repository’s discovery services and search engine optimizations will ensure that the uploaded research articles and other uploaded content are easily discovered by major search engines. Data management services help faculty at every stage of data lifecycle including data creation, data collection, data storage, data archiving and preservation, data access, data analysis and data discovery. Direct faculty support is available for many services including development of data management plans, metadata issues, long term data storage and consultations for uploading research data into ScholarWorks repository.

**Plans for Future (Sustainability)**
There will be an awareness and training campaign on the availability of the repository and the research data management services. The configuration will be updated to support additional content (Thesis and Dissertations, University Publications and Art/Music collections) and additional features (statistics, reporting and faculty profiles). The data management services will be expanded to help departments, centers, and faculty with data processing needs for batch uploading of content into the repository.

**Cyber Security**

**Current**
UNR’s strategic approach to cyber security is a policy-driven data classification methodology, combined with strong technical safeguards and proactive user engagement. This allows deployment of clear and concise data policies, along with an agile data governance environment, to provide a secure and adaptable framework for increasing the ability to do research on both regulated and non-regulated data.

In 2016 a robust border network control and monitoring system was in place using a combination of layer 7 application firewalls and network inspection using fiber taps and an SDN switch to distribute flows to a CERT NetSA SiLK capture system. Big data analytic environments built to grow to 40Gbps were installed in 2016 to handle both the campus administrative network and the increasing demands of the Science DMZ. UNR subscribes to the InCommon certificate service to increase utilization of encryption for all online services. UNR maintains an inclusive Identity Management System that allows auto-provisioning for students, faculty and staff and accommodating guests, affiliates, and visiting scholars. Shibboleth is the primary authentication gateway for all federated services. A campus wide Active Directory (AD) environment provides a multi-platform authentication and authorization system to all constituents. Eduroam authentication was enabled on the campus in early 2016.

**Plans for Future (Sustainability)**
Moving forward UNR will enhance Information Security and Identity Management in multiple ways:
• (ongoing) Enhance positions within distributed research and academic technology-support units to include cyber security responsibilities and work with central Information Security in planning, incident response, and training scenarios.

• (2016) Deploy a new incident response system based on a customized cloud-based tracking system to centralize various alert reporting systems and produce actionable metrics and data.

• (2016) Full bi-directional replication of all AD accounts to Microsoft Azure Premium Services.

• (2017) Add intrusion detection capability to our existing SDN monitoring system using BRO and the model specified in the “Berkeley Lab 100G Intrusion Detection” whitepaper.

• (2017) Deploy InCommon Federation services in a fully fault tolerant and redundant architecture.

• (2017) Implement Microsoft Azure Premium service for an offsite source of identity services along with Multi Factor Authentication services available to the majority of users.

• (2018) Further segment the internal network to isolate internal research networks from administrative networks to gain flexibility and capability for the needs of researchers.

Training & Support

Current

Training has been sporadic for both faculty and students in the use of CI resources. This is an area in most need of development. In response to this, central IT staffing (including both support and training) has been increased in 2014, 2015, and 2016 to support the growing UNR research portfolio. Security staffing has doubled in the last three years from 2.5 FTE to 5.0FTE and operations spending has increased accordingly. Central IT HPC support personnel has grown to 2.5 FTE in the same time period. The College of Engineering has also hired dedicated IT support personnel that collaborate with the central HPC Staff. A position was created and filled in the Office of the VPRI in 2015 to handle research data curation. Both off-premise public cloud services and campus virtual services have been expanded with appropriate staff support in 2014-2016. An HPC subcommittee of the University Technology Council was created in 2015 composed of a cross-section of research faculty to assist in planning training and support activities.

Plans for Future (Sustainability)

A Director of Cyberinfrastructure position in the central IT unit, with academic standing in a department, is planned for 2017. This will be funded internally. HPC facilitator positions are planned for 2017 and 2018. These are to be doctoral-level staff to consult with researchers to match need with the best combination of CI resources, both on and off premise.

The HPC subcommittee will become a separate standing Cyberinfrastructure Oversight Committee (CIOC) in fall of 2016 reporting jointly to the Office of the VPRI and the Office of the CIO. A member of this committee will have a seat on the University Technology Council to provide coordination and communication. In addition to oversight of the UNR HPC resources, the CIOC will identify and prioritize training needs and opportunities for the campus. These will be facilitated jointly out of the VPRI and CIO offices until the Cyberinfrastructure Director is hired. Training, workshops and other CI related activities will be included in the duties of that position.