Idaho State University Cyberinfrastructure Plan

Executive Summary

The overall cyberinfrastructure (CI) plan at Idaho State University is to provide a robust and responsive educational and research cyberinfrastructure that supports and engages Idaho State University's students, faculty, staff, collaborators, and stakeholders; in other words, the ISU campus community. To accomplish this will require a resilient high-performance network, desktop, workstation, and server computers running current 64-bit operating systems, proactive cybersecurity measures, and skilled personnel ready to support the campus community. This strategy closely aligns with national objectives of the National Science Foundation (NSF), the National Institutes of Health (NIH), the Department of Energy (DOE), and other agencies.

Mission

Idaho State University is a public research institution that advances scholarly and creative endeavors through academic instruction, and the creation of new knowledge, research, and artistic works. Idaho State University provides leadership in the health professions, biomedical, and pharmaceutical sciences, as well as serving the region and the nation through its environmental science, and energy programs. The University provides access to its regional and rural communities through delivery of preeminent technical, undergraduate, graduate, professional, and interdisciplinary education. The University fosters a culture of diversity, and engages and impacts its communities through partnerships and services.

One of ISU's four *Core Themes* specifically describes the integral role played by research at the university.

> <u>Learning and Discovery:</u>
> Idaho State University fosters student learning and discovery through teaching, *research*, and creative activity. ISU delivers high quality academic programs at all levels: technical certificates; undergraduate, graduate, and professional degrees; as well as postgraduate professional training.

Furthermore, the mission of ISU's Office of Research states:

> Our mission is to foster and maintain mutually beneficial relationships with federal, state, and corporate sponsors and provide high quality and timely service to our faculty and staff – while maintaining a balance between the interests of Idaho State University, the State of Idaho, and the interests of industry – for the public good.

As an EPSCoR state, Idaho institutions have been building research infrastructure to aid Colleges, Departments, and Programs transform themselves, as well as support the Idaho Science & Technology (S&T) plan, contribute to individual institutional strategic plans and build regional, national, and international recognition. The Idaho EPSCoR Committee stresses that their ultimate goal is to help institutions like Idaho State University build the intellectual environments where faculty can excel and build the research capacity of Idaho.

Introduction

Across the nation, cyberinfrastructure strategies, plans, and deployments have been responding to demands for improved network connectivity and higher bandwidth while balancing the realities of cybersecurity and regulatory compliance. This same scenario holds true at Idaho State University. Without question, cyberinfrastructure is a critical component to the success and future of ISU.

For ISU to accomplish its goal of providing a robust and responsive educational and research cyberinfrastructure first requires a working definition of CI. That definition follows closely the definition formulated by the EDUCAUSE working group on Campus Cyberinfrastructure:

> "*Cyberinfrastructure consists of computing systems, data storage systems, data repositories, and advanced instruments, visualization environments, and people, all linked together by software and advanced networks to improve scholarly productivity and enable breakthroughs not otherwise possible*." (Stewart, C., et al.)

It is fully realized that building and maintaining an effective cyberinfrastructure will not be accomplished following a one-time capital investment. Instead, an effective CI will need to be responsive to new technologies, new opportunities, and new threats. To do this will require both initial investments and continued maintenance of facilities, equipment, and training of skilled staff.

ISU is committed to supporting this effort as evidenced by recent investments in cyberinfrastructure and accompanying staff, specifically the development of the Research Data Center (RDC) and creation of a Research Systems Administrator position for the RDC. ISU has centralized its investments and support, in collaboration with Information Technology Services (ITS), realizing this is, by far, the most efficient way to provide critical research services. For example, ISU has eliminated unneeded duplication of both networking, hardware, software, and staff. This centralized approach has allowed ISU to leverage university investments in cyberinfrastructure for the good of the entire campus.

Background

ISU joined Internet2 in 1999. Since that time, usage and demand for high-speed network connectivity has only increased at ISU. Indeed, collaborations with institutions and agencies other than ISU is a significant part of the university's research. Regular collaborators include DOE Idaho National Laboratory (INL), the University of Idaho, Boise State University, NASA Goddard Space Flight Center, NASA Ames, USDA Agricultural Research Service (ARS), Extreme Science and Engineering Discovery Environment (XSEDE[1]), and the Center for Advanced Energy Studies (CAES) in Idaho Falls, Idaho. Connectivity with the latter (CAES) is 10 Gbps as a result of ISU's cyberinfrastructure investments. More recently, ISU became a member of the Idaho Regional Optical Network (IRON; http://ironforidaho.net/), which relies upon Internet2 to achieve very high speed fiber optic capabilities (10 Gbps) across Idaho's member institutions with connections to GigaPoP sites (Seattle and Salt Lake City) outside the state.

Strategic Plan

In 2011, Idaho State University, the University of Idaho, and Boise State University worked collaborative to develop the Cyberinfrastructure Strategic Action Plan for Idaho Universities. This plan was approved by each of the member institutions on February 2013. While nearly four years old, the vision statement expressed in this document remains valid to this day:

> *"Idaho universities and other stakeholders have ready access to a statewide network of systems and resources that enable new research, effective statewide collaboration, and enhanced competitiveness for funding that creates new intellectual and economic opportunities for Idaho's citizens and serves the state, region, and beyond."*

Five high-level cyberinfrastructure goals were identified in the statewide Strategic Action Plan. These are:

1. Establish a CI Advisory Council (CIAC) for higher education in Idaho.
2. Assess and characterize existing and planned CI activities and collaborative research initiatives

[1] Weber, Xu, and ISU's CIO, Randy Gaines are XSEDE Campus Champions

3. Define and establish a strategy to develop the CI architecture and staffing including prioritized investments
4. Identify and project costs for prioritized investments of CI development
5. Identify CI funding opportunities to be pursued by Idaho universities and submit high- priority funding requests

Recent accomplishments and near-term goals

In 2013, a CIAC was established for higher education in Idaho. The council consisted of two members each from ISU (investigator Weber was a member), Boise State University, the University of Idaho, as well as one member representing the Idaho National Laboratory. In 2015 ISU's Vice-President for Research, Dr. Cornelis Van der Schyf launched a visionary initiative to develop a dedicated and centralized Research Data Center (RDC) on ISU's main campus in Pocatello. To date, ISU has invested nearly $1 M developing the RDC which includes a 40 Gbps core and 10 Gbps connectivity to each server as well as to I2. The RDC includes a very well thought out floor plan, dedicated power and cooling, physical and network security implementations, policy provisions, and a condominium-style approach for a Science-DMZ dedicated research data center. In addition, the 1,000 ft^2 RDC currently has space for the addition of several racks more racks, as well as electrical and cooling capacity for the additional hardware. When the RDC opens early in 2017, it will house all the GIS TReC's production servers (n = 9; three development servers will remain at the GIS TReC and its archive server will remain off-site). In addition, the RDC will house three large blade servers configured through a virtualized environment to support other researchers at ISU. One of these blade servers is designated specifically for protected environment (PE) applications only and will be available for researchers needing such resources. Within the RDC, ISU is implementing perfSONAR to monitor its network including the broader ISU Science DMZ. ISU is actively expanding its use of perfSONAR throughout the enterprise network, as time allows. Other recent accomplishments and near-term goals include:

- ISU has deployed IPv6 and has made it available especially for performance driven web applications such as the NASA RECOVER Decision Support System.
- ISU's Cisco hardware is BCP38-compliant and we are utilizing these features campus wide to enable anti-spoofing capabilities.
- ISU will become more involved with the In Common Federation and the advantages these services provide. Once our current identify management system is fully deployed over the next year we anticipate more use of the In Common Federation.
- Eduroam has been deployed to allow access to our campus' wireless network.

Cybersecurity accomplishments

Since 2012 ISU has made extensive efforts to increase its cybersecurity preparedness following the NIST recommended framework of Identify, Protect, Detect, Respond, and Recover. Major improvements have been made in the following areas:

- Information Technology policies were completely rewritten and adopted to reflect growing cybersecurity needs (http://www2.isu.edu/policy/2000/index.shtml policies 2400-2520)
- All faculty and staff are now required to complete regular security training using the SANS Advanced Cybersecurity Learning platform.
- A third party risk analysis was conducted on all functional areas that handle HIPAA protected data, as well as a compensating controls audit on all functional areas university wide. Concerns identified as high or critical risk were addressed. Audits continue to be refreshed annually.
- In addition to the traditional DMZ vs. intra-network segmentation, ISU's network infrastructure was further segmented into security zones consisting of two server levels (based on the sensitive nature of the data stored on the server), workstations, printers, and three levels of wireless access: Sensitive, Institutional and Public. An IPS system was installed and firewall and wireless services were significantly expanded to accommodate these changes.

- Where appropriate, malware is now centrally managed through the mandated installation of McAfee antivirus and encryption products on all ISU owned servers and workstations.
- Disaster recovery processes have been prepared and documented both at the Information Technology level and enterprise-wide.
- The use of data classifications have been enhanced and expanded.
- ISU entered into a contractual agreement with BOX for all cloud storage of institutional and sensitive data managed by the university. This has allowed ISU to gain better control of cloud storage as well as provide improved restore and recover capabilities.