Campus Cyberinfrastructure Plan for Florida International University

Executive Summary

This document presents a strategic direction and an action plan for *cyberinfrastructure* technology for the next three years (2021 – 2024) for the Division of Information Technology at Florida International University (FIU). The plan represents the strategic priorities necessary to guide the Division and the university in its deployment of cyberinfrastructure technologies and practices in the coming years. The strategic plan takes into account: (1) the particular challenges that confront higher education, (2) the increasing demands by faculty and students for technology, (3) today's fast pace of technological progression, (4) opportunities to leverage the effectiveness of existing resources, and (5) cybersecurity best practices and requirements in order to meet the regulations and compliance requirements to further protect FIU's data and resources.

Cyberinfrastructure Strategic Vision

Cyberinfrastructure provides access to national and international science and engineering communities through research environments that support data acquisition, data storage, data management, data mining, and data visualization. For FIU to remain competitive and to provide the best resources for its research faculty, a *cyberinfrastructure* strategic direction must be put in place. The strategy for *cyberinfrastructure* for the Division of Information Technology at FIU is to create and sustain an environment that supports faculty who have increasing needs to work collaboratively, securely, and to have use of CI resources not only at FIU, but where available. FIU's network and CI environment will provide the University's research community with a wide range of network services to enable FIU researchers and students to participate and collaborate in distributed knowledge creation communities.

Technology Infrastructure Environment at Florida International University

Over the past decade, the technology and cybersecurity environment has become an increasingly important and integrated element of universities. Introduction of computing in the elementary and secondary schools has given rise to a significant increase in the expectations of available technologies in colleges and universities. Computational science applications, involving new forms of data collection, analysis and synthesis, such as data mining techniques in the physical sciences, are emerging and competing for campus technology resources.

Research requirements are increasingly data driven. Researchers across disciplines now require ever increasing amounts of network bandwidth, data storage, protection of data, research, intellectual property, and resources, while still requiring technological expertise and support. Scientific discipline advances now depend on how well researchers can collaborate with one another. Likewise, scientific breakthroughs depend largely on advanced computing capabilities that allow researchers to manipulate large data sets, workflow, visualization, artificial intelligence (AI), digital transformation and cloud computing technologies.

The fast pace in technological progression of the past few years, the large amounts of information that are available has created, new emerging cyber threats, and compliance requirements create the need for a new information infrastructure for both research and end users. Libraries now face the challenge of remaining relevant. One consequence of this change is the move toward digital content collections that are readily accessible via the web. This has enhanced the role of libraries as "repositories for knowledge information, and data". In this new era, libraries will become the vital network whereby true collaborations will exist in an increasingly wide range of available information resources.

The most successful institutions will be those that are able to reap continual advantages from the power of rapidly changing technologies while effectively managing the disruption these changes inevitably bring. For example, as a result of the Covid-19 pandemic, FIU's technology infrastructure was rapidly transformed from managing and securing within campus to remote locations. To advance in the face of these impending demands, the Division of Information Technology at FIU must develop a c*yberinfrastructure* strategy and plan to meet the needs of researchers, faculty and students. The cyberinfrastructure technology environment at FIU will focus on enabling data intensive research that extends across multiple disciplines. The goal is to create an environment for a more systematic approach for high performance analytics as well as leveraging collaborative authoring platforms.

Current Network Infrastructure

Florida International University's use of technology enhances student learning and supports the instructional and research endeavors of faculty. As a member of both Internet2 and Florida LambdaRail (FLR) research networks, FIU maintains a robust and leading-edge technology infrastructure in support for its mission of research and teaching. All faculty and students have unlimited access to FIU's state-of-the-art technology infrastructure and information systems.

The Division of Information Technology at FIU has deployed a highly redundant and resilient network. The network backbone consists of 100 Gigabit redundant core nodes. FIUnet is a fully routed core with switching elements in every building. The core nodes are distributed across two buildings to ensure redundancy and resiliency in case of an outage in a building that houses a core router/switch. Every building has a pair of distribution layer router/ switches, which provide redundancy and resiliency at the building layer (Figure 1). Within the telecommunication rooms, FIUnet has access switches providing 10/100Gigabit Ethernet services over category 5E and category 6 cabling to end user devices. As new buildings come online, switches in those telecommunications rooms connect back to the distribution router/switches via two 10/100 Gbps links.

FIUnet connects to the Internet, Internet2, and Florida LambdaRail through two diverse dark fiber pairs that terminate at the Network Access Point (NAP) of the Americas. Both fiber links operate at 100 Gbps providing both load balancing and redundancy to FIU's Americas Path (AMPATH) point of presence (POP). Via AMPATH, FIU peers directly with Florida LambdaRail (FLR), Internet2, ESnet, Content Distribution Networks (CDNs), and Internet Service Providers (ISPs).

FIU's converged network supports approximately 6,000 Voice over Internet Protocol (VoIP) phones, 25,000 end stations, and the university's e-library. The network is comprised of approximately 400 Telecommunications rooms, 90 routers, 500 switches, 2,250 wireless access points, and 450 standalone uninterrupted power supply (UPS). All FIU buildings across all campuses and centers provide 802.11b, 802.11g and 802.11n wireless services with access to commodity and research networks.

Supporting Research and Education

High Performance Computing

Strategy: Provide access to high performance computing (HPC) resources to facilitate research with computationally intensive requirements

High Performance Computing Clusters play a critical role in various domain sciences in transforming human endeavors ranging from global climate change, materials development, hurricane modeling, and wind tunnel simulations. HPC-based technologies give FIU faculty and student researchers the ability to make significant contributions to solving large-scale problems that otherwise would not be possible. FIU's ever evolving research computing environment currently consists of the following three components: (1) HPC, (2) Shared-memory Multi-Processor (SMP), and (3) Virtual Computing Lab (VCL).

1) **Panther Cluster**: Provides about 3,312 CPU cores spread across multiple servers. There are a variety of nodes for different research needs (low memory, standard and high memory nodes. This is for highly parallelized CPU-based jobs that use distributed memory. This same environment can be used for High Throughput Computing (HTC).

2) **SMP Node(s)**: These are special-purpose nodes that are part of the Panther Cluster that provides large amounts of cores and memory on a single node for jobs with high shared memory requirements.

3) **Virtual Computing Lab (VCL)**: This is a cloud environment available to researchers that allows faculty to spin up a single server or a cluster of servers in a virtual environment. These are temporary resources. Most of the environment is limited to reservations lasting no longer than 8 hours; however, a portion is made available for longer-term reservations. Faculty use this environment to test changes to their research computing environments and it is used in their academic curriculums.

Strategy: Operate effectively an Instructional and Research Computing Center (IRCC)

The Instructional and Research Computing Center (IRCC) was formed to provide access to high performance computing technologies, storage for large data sets, and on-demand computer resources for the classroom. The center hosts High Performance Computing instructional workshops open to all faculty and students to help integrate these technologies into current and future research efforts, as well as into the classroom. The Division of Information Technology's IRCC department centrally manages these resources providing a university wide service available to all departments, students, and faculty at FIU.

Network Infrastructure

Strategy: Improve effective network services to support research and enterprise applications

The FIU campus network supports research and enterprise applications. Cyberinfrastructure on the FIU campus network has become complex and varied, with many end user devices, instruments, servers, HPC clusters, data management systems, etc. Researchers have the flexibility of connecting their CI to the campus network via a high throughput Data Transfer Node (DTN) and request ports with appropriate bandwidth capacities to support their applications. This flexibility will support faculty in both research and instructional technology. Data intensive research applications will benefit from this increase in bandwidth capacity to request access to network resources provided through the Science DMZ (see next section). Figure 1 shows three different cases for researchers to connect to the campus network. Case 1, on the left, represents a private researcher-owned Ethernet switch that is connected to a Science DMZ router (labeled ScDMZ router). Case 2 has a dedicated fiber uplink to the ScDMZ core at 100G and separate fiber uplink to the enterprise core. Case 3, on the right, the researcher connects to the enterprise switch uplinked to the enterprise router on a ScDMZ vlan. This strategy improves mobile communication systems and greater security through traffic isolation. Measurable outcomes will guide decisions to increase network resources for research and instructional technology activities. FIU's strategy is consistent with the Internet2 Innovation Platform: Abundant bandwidth (100Gbps), Programmability through Software Defined Networking (SDN), and Friction-free Science through a Science DMZ.

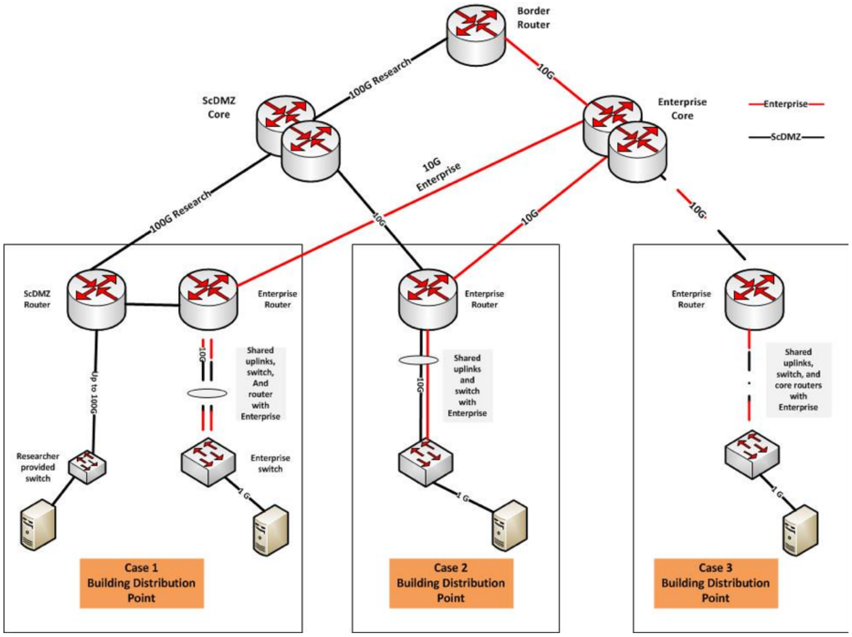
Border Router
100G Research
10G
ScDMZ Core
Enterprise Core
Enterprise
ScDMZ
10G Enterprise
100G Research
10G
10G
10G
ScDMZ Router
Enterprise Router
Enterprise Router
Enterprise Router
Up to 100G
10G
Shared uplinks, switch, And router with Enterprise
10G
Shared uplinks and switch with Enterprise
Shared uplinks, switch, and core routers with Enterprise
Researcher provided switch
Enterprise switch
1 G
1 G
1 G
Case 1 Building Distribution Point
Case 2 Building Distribution Point
Case 3 Building Distribution Point

Figure 1 Science DMZ and Enterprise Network

Strategy: Deploy a network design model that will optimize data transfer

FIU is continuing to optimize data transfers for its researchers by connecting researchers and their CI to its Science DMZ, in order to maximize friction free data flows. FIU's Preeminent Programs and Emerging Preeminent Programs are collaborative endeavors that demonstrate extraordinary success in providing unique learning opportunities, pioneering research and engagement. The computational and data movement requirements of these programs are being assessed to determine how the Science DMZ can enhance the research activities and output of these preeminent programs.

Strategy: Deploy IPv6 throughout FIU

FIU has enabled IPv6 on the campus network and will continue to deploy IPv6 throughout the university. Deployment of IPv6 will allow the university community to take advantage of IPv6 features such as its built-in security features.

Identity and Access Management

Strategy: Operating an effective federated identity and access system with campus CI resources

Today's research routinely requires researchers to share data and resources with colleagues across multiple institutions. FIU has built an FIU IAM infrastructure, consisting of (1) IBM Identity Security Manager,

(2) SAML Identity Providers (IdP), (3) FIU Directories, and (4) a central custom login page.

(1) ISIM is the core of the IAM architecture. It is source of all identity information at FIU and is responsible for provisioning and de-provisioning of access to systems and applications based on the role and responsibilities of the individual user. ISIM keeps passwords in sync across all resources and directory servers that it manages by replicating password changes to each target system. ISIM has the functionality to allow for the creation of customized workflows to carry out FIU business specific processes related to resource access.

(2) FIU has standardized on CAS (an open-source IdP) and Shibboleth (for certain use cases) as a SAML IdP. Both provide authentication services for both on-campus and external resources through integrations. Being a SAML based system, no passwords are exchanged between the requesting application and the IdP. Only a token is passed back to the requesting system stating the results of the authentication, along with needed identity attributes, so the requesting system can make an authorization decision.

(3) FIU's primary directory is Active Director (AD). It is used both for back-end authentication and authorization. It supports two-way password synchronization between ISM and AD. LDAP is our legacy directory and is uses for specialized use cases. It is kept in sync with AD via both being targets for ISIMs a provisioning service. Only internal FIU connections are allowed to FIU directories, so that no FIU credentials are directly entered into an external vendors' system. All external systems are integrated with CAS or our front-end SAFE application.

(4) Custom Login Page is a web application with custom logic that allows web-based access to system based on a users role at the University. Furthermore, it gives a centralized place for password changes, resets and two factor cell phone registration. This login page integrates with FIU's Duo two factor systems. This two-factor system can be opted into by general users. Its use is mandated for users with access to what FIU considers sensitive information or systems. The custom login page, integrates with IAM and AD for password changes, authentication and authorization – leveraging the attributes set for each user stored in these systems.

Strategy: Consolidate University servers/storage

Consolidating and hosting the servers in one central location would mean a much more efficient use of space. This initiative calls for the consolidation of the university's servers by virtualization and cloud computing technology. With server virtualization and cloud computing technology, the university will achieve savings on power consumption, enhance server security, and reduce the cost of support services. A virtual server environment uses less power than dedicated servers and reduces the number of servers. Since2010, all new servers are virtualized, except for servers with specialty applications or with computing intensive applications. When possible, existing servers will be gradually virtualized at the end of their hardware lifespan.

Strategy: Follow the CIA Triad model for the campus-wide approach to cybersecurity.

FIU has established several enterprise-wide policies to address privacy and the protection of data considering physical security, technical security, and user actions. FIU utilizes various cybersecurity frameworks in order to create am enterprise defense in depth cybersecurity infrastructure. FIU follows NIST800-53, CSC20, and NIST800-171. Over the last five years FIU has made several investments in cybersecurity tools in order to increase detection and shorten the time to mitigate. FIU has also emphasized focused on securing endpoint devices, promoting two factor authentication and increasing awareness amongst faculty, staff and students.

Florida International University (FIU) utilizes a layered defense approach for security to support the confidentiality, integrity, and availability of the systems and data FIU owns, stores, transmits, and manages. All network devices are connected on a private management network VLAN where Access Control Lists and restrictions are applied. Virtual Local Area Networks (VLANs) are configured throughout the network for network segmentation. These networks sit behind a firewall with threat and malware protection.

Remote Access is provided to FIU users via Virtual Private Network (VPN) or Virtual Desktop Interface (VDI). Both of these remote access methods require authentication with two factor authentication. Workstations connecting via VPN go through a posture analysis to determine if the workstation meets minimum security requirements such as Antivirus, updated patches, and local firewalls. VPN and VDI access are managed via Active Directory Groups. Next generation firewalls and IPS are configured and deployed in strategic/critical parts of the network. These devices are centrally managed, and configurations are reviewed periodically. Perimeter anti-malware and anti-spam tools are in place and configured. URL filters are also in place, but only configured to filter malicious URLs. E-mail security protections such as URL rewrite, malware, attachment defense, and SPAM filtering are also configured for all employee accounts. Threat prevention, host data loss prevention, and whole disk encryption are installed on all managed hosts joined to the Active Directory Domain. Windows hosts are patched with Microsoft System Center and Configuration Manager (SCCM). JAMF and patch my PC are used to patch managed MACs and third-party applications. Notification of missing patches is done via the vulnerability reports, notifications, or assessments. Vulnerability scans are performed on a regular basis to all endpoints connected to the FIU network. Vulnerability reports are shared with the various IT administrators for corrective action. Follow-ups and rescans are performed. Internal Security Risk Assessments are performed by the IT Security Office for various departments at the University. External risk assessments are performed as well by third party vendors which are hired to perform these assessments for compliance or regulatory requirements. In addition, FIU has an enterprise Incident Response Plan (https://security.fiu.edu/uploads/docs/Incident-Response-Plan.pdf) which will be activated in the event of a major incident or breach. Furthermore, we do have a cyber insurance policy which we can use to assist with containment, remediation, and communication efforts in the event of breach.

User awareness and training is a key component of FIU's security strategy. All employees are required to take the annual cybersecurity awareness training. Monthly phishing campaigns are sent to all employees as well. Other trainings for compliance and regulatory requirements such as HIPAA, PCI, CUI, and FERPA are also offered to employees.

The FIU Cybersecurity team keeps abreast of new cybersecurity threats which could impact FIU by subscribing to various news, blog, and groups for information regarding cybersecurity threats. We are also members of REN-ISAC, MS-ISAC, ISACA, and the South Florida ISSA. FIU's CISO is a member of the SUS Committee on Cyber Risk Management which meets monthly to discuss new security trends, threats, and issues impacting higher-ed and research institutions. We work closely with our vendors and partners to make sure our security tools and applications are current and that we are informed of new roadmaps to these technologies.

In addition, FIU has several initiatives and tools used to limit compromising access to our computer network. Physical access controls are enabled to sensitive areas and areas where critical systems are kept. Network Segmentation is configured throughout the FIU network to create different virtual local area networks (VLANs) for different data types and uses. 802.1x is configured on all our physical network drops, if a device does not support 802.1x, mac filtering is utilized. Our wireless network is also segmented, our primary SSID is configured to use WPA2 with 8021.x for authentication. Guest access is on a separate restricted vlan with limited ports and bandwidth. In the event of a DDoS attack, we do have DDoS mitigation capabilities.

Two-factor authentication (2FA) is offered to all our users. Most of our enterprise applications such as our ERP, Office365, LMS, VPN, and VDI support 2FA. Server backups take place daily for incremental and weekly, monthly, quarterly and annually for full backups. Backups are maintained for 30 days. Network device backups take place daily for incremental and weekly, monthly, quarterly and annually for full backups.

Closing Remarks

This document described the strategic plan for cyberinfrastructure for the Division of Information Technology at Florida International University (FIU). The strategic goals for cyberinfrastructure are to develop and implement a plan that will place FIU at the forefront of new CI technologies. The vision is to create and establish a cyber technology environment that is sustainable, and which will enable faculty and students to participate in national and international research as well as science and data communities.