

POSSIBILITIES

SPRING 2020 • DIVISION OF INFORMATION TECHNOLOGY

ABOUT THIS ISSUE

A new year brings forth resolutions, fresh beginnings and, of course... ANNUAL REPORTS!!!! For the Fiscal Year 2019 Annual Report, the Texas A&M Division of Information

Technology chose to focus on ways we are "Better Together" and work collaboratively to make a positive impact at Texas A&M. This issue features a small sample of

some of those articles. The annual report can be seen in its entirety at it.tamu.edu/annualreport.

CONNECTING WITH THE FUTURE

Next Generation Aggie Network in Initial Stages

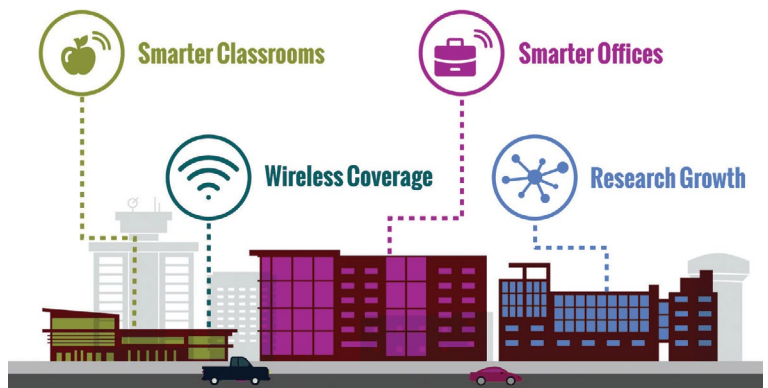
As the old adage goes, "everything is bigger in Texas." Texas A&M University exemplifies that saying with one of the largest campus research and education data networks in the country, connecting over 180,000 wired devices and 110,000 unique Wi-Fi users daily.

As technology becomes more pervasive, demand for greater and more advanced network capabilities is skyrocketing. In addition, university growth in the last ten years has increased network demand exponentially, with a 40% increase in student enrollment and over four million new square feet of construction. In order to keep pace, the Next Generation Aggie Network is a necessity.

For almost three decades, equipment has been added and upgraded on a cyclical basis. The first step of the next generation network is replacing legacy equipment and "laying the foundation," which could cost approximately \$20-\$25 million.

A three-year project was launched in FY19 to upgrade the core campus fiber plant and allow the network to support a minimum of 10 gigabit connections to all main campus buildings. Phases one and two included 44 buildings and is 75% complete. A funding request is currently pending for phase three, which will upgrade 34 additional buildings.

Once the upgrades and legacy equipment replacements are complete, the next phases will be implemented. Read the full story at it.tamu.edu/annualreport.



BECOMING A DRIVING FORCE

New Technology Calls for Testing Facility at RELLIS

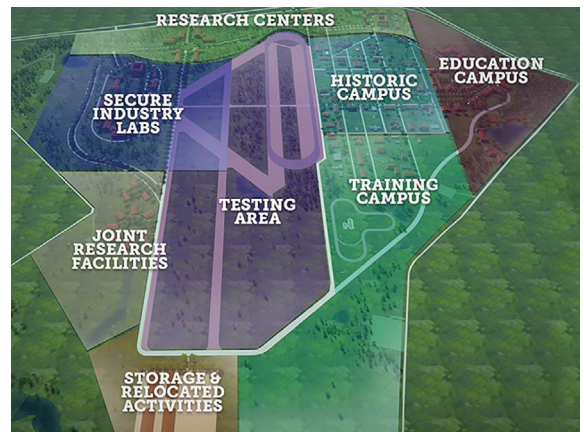
Texas A&M University is joining forces with the US Army Futures Command to research technologies that will modernize the nation's armed forces — and possibly change “life as we know it” — thanks to the focus on fifth generation (5G) wireless technology.

A \$130 million combat development complex will be constructed at the RELLIS campus. The complex is funded by a \$50 million appropriation from the Texas Legislature for an “Innovative Proving Ground” and \$80 million from The Texas A&M University System Board of Regents for a “Research Innovation Center.” Recently the U.S. Army Futures Command and TAMUS entered a \$65 million cooperative agreement supporting research.

The complex will include a track for testing autonomous vehicles, a one-kilometer long tunnel for testing hypersonic weapons, runways, underground and open-air battlefields and laboratories. In addition, \$8 million will be used to establish one of the world's leading 5G proving grounds or test centers for public safety and the Department of Defense.

Walt Magnussen, Chief IT Consultant for Vendor and Agency Relations, said the test center will be “one of a kind” and will attract industry as well.

“If Ford, Chevy or Toyota want to test out the technology with their vehicles, they don't want to build a test center,” he said. “This will allow them to come here to test their vehicles. I think we need to recognize the wisdom and vision of the legislature for funding something like this, because this could very well be a major source of economic development within the state. It will bring leading companies to Texas, but more directly to Texas A&M University.”



DIVISION HAS HEAD IN 'THE CLOUD'

Aggie Innovation Platform Unites Popular Online Services

The division is working together with three popular cloud services to create the Aggie Innovation Platform (AIP). The platform gives the Texas A&M community access to the on-campus Aggie Cloud as well as other secure environments including Amazon Web Services, Microsoft Azure and the Google Compute Platform. This coincides with the migration of the old virtual machine (VM) architecture to the Aggie Cloud.

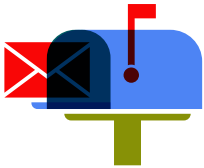
The platform will provide the Texas A&M community access to the on-campus Aggie Cloud as well as

public cloud services from Amazon Web Services, Microsoft Azure and the Google Compute Platform. The AIP will support research, education and operations by reducing the barriers to innovation and reducing the time to realize and implement new ideas. The AIP will also facilitate the development of other domains such as the Secure Health Research Environment (for working with HIPPA and PHI data) and NIST 800-53 compliant facilities.

The Division of IT: "Better Together"

Protecting Texas A&M

On average, the Division of IT protects:



168,843
Mailboxes



135,000
Devices



227,048
Accounts



688,700
Active Identities

Staying Connected

Texas A&M University is among the top 10 largest physical campuses in the nation, and needs one of the largest networks to support it.



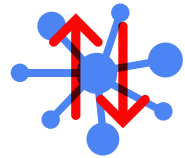
7,331
Wireless access points on the College Station Campus



183,600
Devices on the Texas A&M network each day



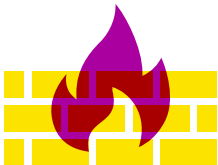
17.4 million
Square feet of wireless coverage on the College Station campus



52TB+
Data transferred over the network each day during a semester

Securing Our Information

The Division of IT protects Texas A&M electronic resources around the clock.



1 million
Connections to malicious websites blocked by the firewall daily



1.5 petabytes
Data inspected for threats, malware and attacks each day



3.5 million
Wi-Fi sessions on the A&M network secured each day



3.5 million
Emails inspected daily for spam, phishing and viruses

Student Cybersecurity Employee Scores a "Zero"

A second-year student in the Division of IT's Cybersecurity Apprenticeship Program (CAP) made a splash recently by discovering a zero-day vulnerability, a security hole unknown to software vendors and antivirus firms.

While performing regular signal analysis, one of the 10 CAP students noticed unusual signal behavior, researched it, and discovered malware being distributed through legitimate apps that would activate the device's microphone so the malware could track the user through voice and other data. This allowed Texas A&M to pinpoint the malware and stop it before it spread across the university.



Upon discovery, the team sent an alert to infected individuals informing them of the malware and giving instructions for removal. They also communicated the find campus-wide so others could avoid the malicious app.

Created in 2018, CAP was designed to add an additional layer of security monitoring to campus while preparing students for the booming cybersecurity industry — which currently has a shortage of approximately

three million professionals. The initial group of 10 students was chosen from over 100 applicants in a technology discipline who possess an understanding in networking, application protocols and programming languages. The long-term goal of the program is to help position Texas A&M University as the leader in cybersecurity education.

“ Through their work and in the classroom, we’re teaching them how to actually be proactive security investigators. ”

Chris Wiley, Principal Security Operations Engineer

“CAP is very innovative in that the students are working on live, real-world data,” said Principal Security Operations Engineer Chris Wiley. “The students are seeing signals and data crossing every country, since there are scholars on campus from different universities around the world. In a typical school setting, the students would be working on pre-canned, vanilla case material.”



GIVE US FEEDBACK!

Help make PossibillTies better by taking a quick, one-minute survey! Simply scan the code at the left or visit <https://bit.ly/2107Mqf>.

