



Ignyte Signs into Cyber Agreement with the Air Force

WRIGHT-PATTERSON AIR FORCE BASE, Ohio – In the complex world of electronic information transfer, inherent vulnerabilities and cybersecurity threats require constant attention and rapid responses to counter potential threats to any company's cyber infrastructure. Those threats can be extremely crucial to national defense organizations such as the United States Air Force, but its countermeasures can be generated and improved through collaborations between the military and the civilian sector for dual-use protection.

In late 2020 and early 2021, 16th Air Force's 67th Cyberspace Wing (67 CW) signed Patent License Agreements (PLA) with two private sector companies to expand and improve on the software code developed by the Air Force, more specifically 67 CW's 90th Cyberspace Operations Squadron (90 COS), to detect software vulnerabilities. Shortly afterwards, 67 CW signed Cooperative Research and Development Agreements (CRADAs) with both companies, enabling the companies to leverage their research and development efforts and develop new technology with Air Force expertise, equipment, materials, and other resources in a protected environment. 67 CW could enter into the PLAs and CRADAs with the two companies because Air Force Research Laboratory has designated 67 CW as a federal laboratory. One of those companies was [Ignyte Assurance Platform](#), a leader in collaborative security and integrated cloud Governance, Risk, and Compliance solutions.

Since 2012, Ignyte has been simplifying regulatory processes to help businesses of all sizes comply with complex guidelines, enhance their cybersecurity posture, mitigate risks, and protect their resources faster and more cost-effectively. Led by both active and former Air Force and Navy veterans, the company has evolved from a small research and development organization to a globally deployed full-stack cloud-based application powered by artificial intelligence and language intent matching technology.

"We are on a mission to deliver cyber risk management automation and governance software for organizations looking to innovate away from slower and cumbersome processes," says Max Aulakh, Founder and Chief Executive Officer at Ignyte. "Our mission is very much complimentary to 16th Air Force Cyber to generate cyber insight, compete and escalation of information warfare. The joint agreement between Ignyte and U.S. Air Force is designed to further our capabilities bringing them to commercial markets."

This particular PLA revolves around a software scanning application tool, which scans network files and calculates the probability that a certain file is malicious or not. Current detection software scans items for known problematic signatures; whereas, Air Force technology is designed to look for suspicious items that do not have a signature and thus may escape detection by current methods.

Ignyte and the Air Force's combined effort stands to create a more unified approach to a more stable cyberspace. With taxpayer money funding government entities such as the military, the ability to transfer technology created with the military back to the taxpayer or civilian users is the intent of the Air Force Technology Transfer and Transition Program (T3) which oversees PLAs.

Continued >



According to Aulakh, industry is currently lacking strong tooling and support for emerging requirements such as Cybersecurity Maturity Model Certification (CMMC), Open Security Controls Assessment Language (OSCAL), and the Federal Risk and Authorization Management Program (FedRAMP). Ignyte has been tracking the specific supply chain security legislations proposed by the Department of Defense (DoD) for the last five years and is strategically perusing this opportunity to work with the Air Force in this capacity. By 2026, the private sector is expected to secure their supply chain and become certified in accordance with CMMC and FedRAMP security programs imposed by the U.S. government.

“We expect these combined technologies to help the private sector in accelerating security around their critical assets and data,” Aulakh explains. “We plan on leveraging both Ignyte & Air Force’s technology to accelerate achievement of CMMC processes for commercial enterprises. Our combined capability will allow organizations to meet compliance objectives while helping quickly identify weaknesses within critical computing systems. This capability will be enabled through the use of advance techniques using artificial intelligence and machine learning.”

Aulakh says he became aware of the opportunity to work with the Air Force through Ignyte’s close relationship and partnership with the Air Force Research Laboratory at Wright-Patterson Air Force Base. He reveals that working with the military, and DoD in general, requires long term planning and proper resourcing, which can often lead to discouragement along the way. “I would encourage organizations and entrepreneurs that are looking to work with the Air Force and the DoD to view this entire process as a way to serve our great nation,” he adds.

“The most difficult aspect of this process,” continues Aulakh, “is attempting to understand the internal mission and internal key capabilities without having the ‘need to know’ or clearances to make something usable for both sides. In order to bridge this gap, our team is now reinstating their prior clearances to gain a better understanding of critical capabilities required by both sides to develop technology that will be used by analysts on both sides.”

This PLA will provide priceless benefits within cyberspace, many of which will go unnoticed as they tend to occur in the background. However, one priceless benefit that will definitely

be noticed by Aulakh and the staff at Ignyte will occur within the mental space. “This agreement has validated our technical approach and has brought credibility to the many years of work that Ignyte has put into building its technology platform. This agreement will now help us mature and scale our capabilities rapidly for the commercial enterprise,” Aulakh concludes.

“These types of agreements allow tax dollars that have been spent on Air Force technology to be used for the ultimate benefit of American consumers,” explains Rebecca K. Lively, 90 COS’s Deputy Director. “Companies can take the hard work of our developers and continue to improve upon it, allowing us to reap the benefits without having to invest more in updating and sustaining the software.”

Lively has made recruitment and retention of talented workers a top priority for the 90 COS. “The distribution of royalties from the agreements will help to reward and incentivize our inventors and developers to continue to innovate, serving as a morale booster and retention incentive,” she says.

“Patent license agreements and CRADAs are some of our best tools for public-private convergence and partnership,” adds Eric Rosenberg, 67 CW’s Chief of Cyber Intellectual Property Law. Mr. Rosenberg spearheaded 67 CW’s efforts to transfer the Air Force technology. “We have a Congressional mandate to transfer technologies when appropriate. When deciding whether to transfer technology, we bring together various stakeholders to weigh the equities. Technology transfer in the cybersecurity context presents unique considerations. At the same time, it is essential to national security that we continue to strengthen and expand the defense industrial base through such transfers and collaborative research and development.”

Patent License Agreements are offered through the Air Force Research Laboratory’s Technology Transfer and Transition (T3) program office, enabling inventions developed and patented by Department of Defense laboratories to be transferred to the private sector for full productive use. Cooperative Research and Development Agreements enable research collaborations with private sector companies, universities, industry associations, and other organizations. A comprehensive suite of T3 mechanisms for partnering with industry and academia are offered through the office. To find out how you can partner with the T3 Program, please visit <https://www.aft3.af.mil>.



PARTNERING WITH A SHARED VISION

U.S. AIR FORCE TECHNOLOGY TRANSFER & TRANSITION PROGRAM OFFICE
AF.TECHTRANSFER@US.AF.MIL | [HTTPS://WWW.AFT3.AF.MIL](https://www.aft3.af.mil)