U.S. DEPARTMENT OF ENERGY

INL Idaho National Laboratory

OAK RIDGE National Laboratory

Pacific Northwest NATIONAL LABORATORY

Sandia National Laboratories

DEPARTMENT OF ENERGY AND NATIONAL LABS

CYBERSECURITY TECHNOLOGIES VIRTUAL SHOWCASE

A Better Way to Bring Federal Cybersecurity Technologies to the Market

CYBER CAPITAL PARTNERS

THE OPPORTUNITY

Virtual Cybersecurity Technology Showcase

The Department of Energy (DoE), Idaho National Laboratory, Sandia National Laboratory, Pacific Northwest National Laboratories, and Oak Ridge National Laboratory, with support from Cyber Capital Partners, are excited to showcase their winning cybersecurity technologies.

By partnering with a cybersecurity investment and business advisory company, DoE streamlined its methodology to make it easy for a cybersecurity technology buyer to see the latest proof of concept technologies.

It is with your participation that DoE, in concert with the Labs' Offices of Technology Transfer, can prioritize the commercialization investment to make these technologies into real American companies.

While this is one step in a much larger discussion of public/private partnerships, this effort will have an immediate impact on the United States' cyber security position.

BACKGROUND

The State of Affairs

The United States (U.S.) Government is at the leading edge of cybersecurity innovation. Since World War II, the DoE remains at the forefront in national security research and development (R&D). Through the 17 DoE National Laboratories, the U.S. Government continues to invest significant resources in advancing cybersecurity innovation; conducting the R&D for the national security requirements of the Department of Defense, the intelligence community and the Department of Homeland Security.[i] As a result of this cybersecurity R&D, DoE has the opportunity to commercialize some of this emerging cybersecurity technology to American companies.

i https://www.energy.gov/sites/prod/files/2017/02/f34/DOE%20State%20of%20the%20National%20Labs%20Report%2002132017.pdf

HIDDEN GEMS

Government Funded Best-in-Class Emerging Cybersecurity Technologies

The cybersecurity technologies developed by the DoE at the National Labs are far superior to those that typically enter the cybersecurity new venture ecosystem from the private sector. Why? The starting point for a Principal Investigator (PI) at a National Lab is decades ahead of most entrepreneurial technologists due to their knowledge of U.S. Government cybersecurity capabilities, their access to like-minded scientists, technologists, and engineers, and the resources provided to them by the U.S. Government.

Once these technologies reach proof-of-concept, the U.S. Government decides to either keep the technology classified or release it for commercialization. Despite their superiority, most of these best-in-class cybersecurity technologies sit unutilized after being released for commercialization.

> ***The U.S. Government invests approximately $135 billion in science and technology, advancing our nation's innovations. Only 20-30% are successfully commercialized.***

While some of the intellectual property (IP) created needs to remain under the protection of the U.S. Government, much of it can be adopted by American companies for the purpose of expanding private sector companies competitiveness.[ii]

ii https://thehill.com/blogs/congress-blog/technology/317788-lets-use-technology-transfer-to-drive-growth)

THE PROBLEM

Barriers to Commercialization

Any U.S. individual or company can approach the National Labs to access the technology through a paid license or open source. So why don't these technologies become widely adopted? There are three reasons:

01 Multiple Champions, Conflicting Visions

Commercialization of technologies requires multiple champions. The US customer, Federally Funded Research & Development Centers (FFRDCs), the technologist, the licensee and its investors, and the end customer each play a significant role in determining which technologies succeed from concept to utilization in the commercial sector. These parties have different visions of technology commercialization depending on their interests and motivations.

02 Complicated, Costly Process

Second, the commercialization process is difficult to navigate, the technology is time consuming and costly to review, and those tasked with the job — such as CISOs and CIOs of American private sector companies — are inundated with daily demands from their organizations along with solicitation from a barrage of commercial entities selling cybersecurity technologies.

03 Commercialization is a Secondary Priority

Third, the National Laboratories and FFRDCs primarily serve as the R&D partner to the DoE, to develop new advanced technologies for the DoD, DHS and IC to protect the United States. Managed by two dozen non-profit organizations and universities, FFRDCs have the primary priority to provide impactful science. The process to commercialize these technologies involves the DoE, the FFRDC's management organization, the government customer and the individual laboratory's technology transfer team, for a wide portfolio of technologies. Each lab recognizes the needs to improve technology transfer process to fulfill the priority of commercializing these technologies.

> ***It's hard! Who has the time, money or resources needed to evaluate all of these technologies?***

A "PACT" to Improve Tech Transfer

As part of the dozen new initiatives within the U.S. Department of Energy's Practices to Accelerate the Commercialization of Technologies ("PACT") program, the Cybersecurity Virtual Showcase is designed to promote the transition of research developed at the Department's National Laboratories toward the marketplace to promote U.S. competitiveness and national security.

HOW PACT SOLVES THE TECH TRANSFER PROBLEM

Virtual showcases will accelerate U.S. competitiveness by significantly improving the process of Technology Transfer to the commercial sector in the following ways:

Easy Access to Information

Gain admission to a central repository to scan the portfolio of technologies most likely to address current problems your organization is facing.

Tailored Review Process

Simplify your participation for the entire review process.

We Are Here to Help

Experience continuity with support from those that were there since the beginning. A team of motivated internal champions formed to accelerate the time from proof-of-concept to product and business. This team remains available to address any questions or concerns.

Clear Market Insights

Boost demand awareness. The technologies that address near and future customer demands are the ones most likely to find a market. Having a full awareness of the needs of the market is a research intensive exercise. This program will provide immediate feedback on the fit of the technology with the demands of the market.

Expanded Resources

Leverage internal and external resources. The DoE and Labs partnered with Cyber Capital Partners to build a community around the portfolio of technologies, expanding the team resources available for down selecting, marketing, and administering the tech transfer program and overseeing its candidate technologies.

High Value, No Cost to You

Participate in a cybersecurity technology showcase designed to value your time and input, all at no cost to you. Your opinion is the contribution we seek.

Cyber Capital Partners is honored to support the Department of Energy in showcasing these national assets.