Response for:

National Institute of Standards and Technology, Department of Commerce.

Request for Information:

Federal Technology Transfer Authorities and Processes

July 26, 2018

Submitted by:

Allison Schwartz
Global Government Relations Leader
schwartza@dnb.com
(703) 807-5065

dun & bradstreet

Dun & Bradstreet is pleased to respond to the National Institute of Standards and Technology, Department of Commerce's Request for Information regarding Federal Technology Transfer Authorities and Processes.

As noted in the RFI, the Federal government invests approximately $150 billion per year in R&D. Of this total, approximately one-third is invested at over 300 federal laboratories[1] across the country and approximately two-thirds is invested at universities and private sector R&D institutions. Quantifying and identifying the federal investment may produce economic gain and maintain a strong technological innovation base which then gets transferred to private companies to create new products and services for a growing economy.

The compilation of technology transfer legislation, including the Stevenson-Wydler Technology Innovation Act of 1980 and the Bayh-Dole Act of 1980, provides a pathway for federally funded research to make its way to the marketplace. In Secretary Wilbur Ross' comments at the April 2018 *Unleashing American Innovation Symposium*[2], he stated that recent studies have indicated that federally funded research conducted by universities is five times more likely to result in a licensed patent technology and seven times more likely to result in an active patent license.

Uniform national patent protections also provide a reliable and navigable pathway for researchers to protect intellectual property rights, regardless of whether they are being created together with the federal government, a university, or a business of any size. These protections are a key part of the strength of the American innovation system.

The modernizing of federal technology transfer policies and procedures has been governed by legislation for the past four decades and ensuring that the appropriate return on investment is achieved with federal dollars is important. However, continued and expanded public-private partnerships focused on solving future problems will be critical to maintaining and advancing the United States' lead in technology innovation.

About Dun & Bradstreet

For over 178 years, Dun & Bradstreet has been dedicated to growing valuable business relationships through the collection, curation, and analysis of data. For 90 years, Dun & Bradstreet has partnered with federal, state, local and provincial organizations to co-develop innovative solutions that fulfill mission critical objectives. Moreover, nearly 90% of the Fortune 500 companies, including small and medium enterprises, are customers of Dun & Bradstreet. Dun & Bradstreet partners with customers in every facet of business and government – providing timely and critical information and analysis to drive business and economic growth in

[1] https://www.federalregister.gov/documents/2018/05/01/2018-09182/request-for-information-regarding-federal-technology-transfer-authorities-and-processes#footnote-2-p19053

[2] https://www.nist.gov/tpo/unleashing-american-innovation

all sectors of the economy, improve operations, identify supply chain risk, support national security, and reduce fraud, waste, and abuse.

With more than 300 million global company records, Dun & Bradstreet has the largest commercial database in the world. Data is collected from more than 30,000 sources globally. Our experienced staff of industry-specific business analysts, government specialists, and data experts integrate customer data with ours – resulting in unique, unbiased insights and analytics that can be applied to unique business objectives.

The Dun & Bradstreet analytics brings data to life – enabling customers to derive rich, actionable insight that drives data-driven decisions. Our analytics solutions apply the latest statistical and computational techniques to provide customers with multi-dimensional analytic models and scores, and access to dashboards that deliver the information needed to make critical decisions.

Given the global nature of today's economy and technologies, we are happy to submit comments on how to update and modernize the technological transfer authorities and processes for the federal government.

Modernizing Technology Transfers and Processes

Government data varies, and robust cybersecurity practices are necessary to ensure that data assets can be effectively protected and leveraged appropriately. Without the necessary cybersecurity practices, the confidentiality, availability, and integrity of such assets cannot be safeguarded, resulting in reduced adoption, and legal, operational, and reputational risks. The following are several areas that should be addressed in formulating a cybersecurity strategy for data management:

Risk Management and Governance - Technology is constantly evolving, and a balanced risk-based approach is necessary to ensure that security requirements foster, rather than stifle, innovation. The development of flexible yet content-rich frameworks to assess and measure information security risk are critical to ensuring that agencies are positioned to leverage data as a strategic asset. The continued evolution of governance frameworks within organizations, and common lexicons for agencies to assess risks should be promoted to achieve this goal.

Validation of Data - Currently the government lacks consistent requirements to validate much of the data that is possesses and collects across the federal government. Ensuring there is a requirement to verify and validate data is critically important to ensuring quality and security of that data. Outdated security methods – such as reliance on passwords or verification of information that may have been compromised is not sufficient and could pose an impediment to digital transformation. Encouraging the development and adoption of more modern authentication techniques which include

monitoring of validity of the data collected is critically important to ensure safe and quality data collection.

Secure Development and Configurations – The systems used to gather, store, process, and analyze data are increasingly complex and interconnected. Effective methodologies and techniques to build security into government systems is critical to ensuring a proactive and optimized approach to achieving risk management and security goals.

With these practices and principles applied, the government can help to protect the quality of the data it created, collects and curates and can also help to provide a more efficient pathway for technology transfers.

Partnering Models – Encouraging Public-Private Partnerships

While the government may have access to some data, there is other data which lay outside the purview of the government scope, and which partnering with established corporations might be beneficial. For example, government may see how global business was conducted yesterday, but their data may lack insights on the future of business and creating innovative solutions for tomorrow's problems may be just out of reach. Expanding Public-Private partnerships to include more established corporation who may have different insight due to the business data they are able to digest would be beneficial to create new innovative technology to tackle the problems of tomorrow.

From the future of Cryptocurrency to how tomorrow's cyber-criminal may attack, predictive analytics based in AI and Machine learning will be imperative to ensure success. It is important to keep in mind that modern analytics are increasingly federated, with parts of the problems being solved by different counterparties. As an example, governments and private sectors both have concerns over new types of business transactions such as crypto currency/blockchain. Certain government agencies are in a position to see information not discoverable by the private sector, while the private sector has access to transactional information not typically available to government agencies. Furthermore, convergence of other disruptive technologies will necessarily result in expert knowledge which is widely dispersed across private and public sectors. Addressing these challenges is a critical imperative requiring strong collaboration and therefore we recommend expanding public-private partnerships to address these growing concerns.

Removing Barriers to Enable Technology Transfers

Partnering with private sector on analytics and data science can enable and accelerate new innovative technologies. In today's complex global environment being proactive is critically important. Having innovative technologies that can not only see what a nefarious actor is currently doing is not helpful for preventing future bad acts. Instead developing the algorithms

and using machine learning and analytics to identify what a nefarious actor might do in the future is needed to prevent the ever-changing tactics of cyber criminals.

Metrics for Determining ROI

Implementing stakeholder-informed action plans, with clear metrics and review times, will help improve accountability and transparency for Federal funded research. Moreover, such action plans should be across all agencies to ensure transparency of all research projects throughout the federal government and that timelines and outcomes are shared across agencies for more efficient technology creations. Such cross-government metrics and oversight will increase transparency and provide needed supervision of projects and allow for more efficient innovative solutions being transferred from lab to market.

New Approaches to Motivate Significantly Increased Technology Transfers

Technology transfer among collaborating partners is often seen as an objective function to advance capabilities. While such objectives can be helpful, especially due to the rapid rate of relevancy decay in many technologies, knowledge transfer is also extremely important. Programs like DARPA are partially helpful in this regard. Evidence suggest much more is needed however. Academic and industry fora which allow for sharing and challenging best practices are extremely helpful, private consortia due this sort of thing now within their cliques. An obvious counter concern is overly sharing best practices with potential advisories. This concern can be partially mitigated through careful vetting participants. Simply sharing technologies without sharing the knowledge and experience related to the evolution of those technologies can be suboptimal at best and negligent in the extreme.

Conclusion

As mentioned, the economy is increasingly global, and the interconnectivity of markets has given way to new analytical innovations. Modernizing the federal technology transfer and processes are critical to ensuring the United States maintains its technology innovation advantages. Expanding public-private partnerships to include access to data and analytics to solve the future problems will be critical for advanced insight and innovation. Dun & Bradstreet is happy to come in and discuss how such an expanded public-partnership might be constructed to ensure more federally funded university research would lead to increased innovation that also builds in transparency, oversight and efficiencies within the process.