VENABLE® LLP

Cybersecurity Alert

January 2013

What You Need to Know About the Proposed Maryland Investment Tax Credit for Cybersecurity

AUTHORS

Anthony J. Rosso
Michael J. Baader
Dismas Locaria
Marta D. Harting
John R. Stierhoff
Andrew E. Bigart

RELATED PRACTICES

Corporate
Government Contracts
State and Local Government

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

On January 16, 2013, Maryland Governor Martin O'Malley proposed a budget for FY2014 that includes several provisions aimed at boosting the state's already robust cybersecurity industry, including a new $3 million tax credit program. This alert provides an overview of the proposed Maryland budget provisions aimed at cybersecurity and provides recommendations for companies looking to take advantage of state and federal cybersecurity opportunities in Maryland.

What are the Key Maryland Budget Proposals Impacting Cybersecurity?

According to Governor O'Malley's budget proposal, Maryland is the nation's "epicenter for cyber security." To continue to spur investment, the Governor's budget includes the following proposals (subject to final legislative approval):

- **Funding of $3 million for the CyberMaryland Investment Incentive Tax Credit Program.** This program, styled on a popular tax credit for the biotechnology industry, is aimed at stimulating the development of new cyber products (not services), including those used in commercial industries. To be eligible for the tax credit, the applicants must be based in Maryland, have at least $100,000 in equity, and have been in existence for fewer than five years. Qualifying investors will receive back one-third of their investment through the tax credit program. ***Credits will be available on a first come, first served basis through an online registration process.***
- **An additional $1 million for continued investment in the state's incubators, test bed sites, and Department of Business and Economic Development staffing.** For example, the Cyber Incubator@bwtech, located adjacent to the University of Maryland, Baltimore County (UMBC) campus, currently delivers business and technical support to early stage companies providing cybersecurity-related products and services.
- **Funding of $2.5 million to launch the Employment Advancement Right Now (EARN) program.** EARN will focus on preparing Maryland's workforce to succeed in the 21st century, especially in key industry sectors such as cybertechnology.

How to Position Your Company to Take Advantage of Cybersecurity Opportunities

The proposed CyberMaryland Investment Incentive Tax Credit Program is based on Maryland's successful biotech tax credit for early-stage biotech companies. Based on our experience and lessons learned in helping clients navigate the biotech tax credit, companies interested in the proposed cybersecurity tax credit should take steps now to position themselves to move quickly once the budget is approved by Maryland's General Assembly.

- If the program follows the biotechnology model, investors will need to complete a certification from the Maryland Department of Business and Economic Development as a "qualified cybersecurity company" as part of the application for the tax credit.
- Make sure that your company and owners are up-to-date on their state and federal taxes.
- Confirm that your company is in good standing with Maryland and has satisfied all necessary corporate formalities.
- Develop a business plan for your proposed qualified investment, including general descriptions of the cybersecurity and related technology used or intended to be used or developed, the methods and goals of development, and existing or anticipated commercial or governmental uses of the finished product.
- Be proactive! If you are interested in the program, please contact us for information on how to support passage of the cybersecurity tax credit. Once the program is approved, don't hesitate to contact the relevant authorities for guidance and additional information.

Finally, it bears noting that just a few days after Governor O'Malley announced the proposed cybersecurity tax credit, the media reported that the U.S. Department of Defense ("DoD") is planning to

significantly expand U.S. Cyber Command (located in Fort Meade, Maryland). According to reports, U.S. Cyber Command is expected to grow nearly five-fold to 4,900 troops and civilians over the next several years. This expansion means that cybersecurity may be one of the few federal procurement areas to see growth in the coming years. See the following **link** detailing a DoD plan to create a fast track acquisition process for cybersecurity defense products and services.

Companies looking to leverage the Maryland funding opportunities to grow their federal cybersecurity business should keep the following best practices in mind:

- Establish a state and federal business monitoring and marketing presence to identify cybersecurity opportunities at their infant stages so that you are able to quickly respond when the agency moves a procurement forward;
- Anticipate and prepare to address certain basic government contracting prerequisites before the DoD goes to market for providers. For federal procurements, these may include registration with the System for Award Management (SAM) (formerly the Central Contractor Registration (CCR) and the Online Representations and Certifications Application (ORCA);
- Possess a Commercial and Government Entity (CAGE) code;
- Implement general compliance requirements, including a written code of business ethics and conduct, and if the company is other than “small,” having in place a suitable compliance program;
- Meet various socio-economic requirements (e.g., having an affirmative action plan);
- Ensure products are manufactured in compliance with domestic preference requirements; and
- Obtain facility and staff clearances so that your company is able to bid and work on projects that involve classified information.

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, and legislative and government affairs.

If you have any questions concerning this alert, please contact any of the authors.