# Evaluation of the Credit for the Purchase of Cybersecurity Technology or Services



DEPARTMENT OF LEGISLATIVE SERVICES 2023

# Evaluation of the Credit for the Purchase of Cybersecurity Technology or Services

**Department of Legislative Services**
**Office of Policy Analysis**
**Annapolis, Maryland**

**December 2023**

**Contributing Staff**

***Writers and Contributors***
Tatiana Hill
Heather N. MacDonagh
Brett A. Ogden
Charity L. Scott

***Reviewers***
George H. Butler, Jr.
Ryan Bishop
Victoria L. Gruber

**For further information concerning this document contact:**

Library and Information Services
Office of Policy Analysis
Department of Legislative Services
90 State Circle
Annapolis, Maryland 21401

Baltimore Area: 410-946-5400 ● Washington Area: 301-970-5400
Other Areas: 1-800-492-7122, Extension 5400
TTY: 410-946-5401 ● 301-970-5401
TTY users may also use the Maryland Relay Service
to contact the General Assembly.

Email: libr@mlis.state.md.us
Home Page: http://mgaleg.maryland.gov

**DEPARTMENT OF LEGISLATIVE SERVICES**
OFFICE OF POLICY ANALYSIS
MARYLAND GENERAL ASSEMBLY

**Victoria L. Gruber**
Executive Director

**Ryan Bishop**
Director

December 2023

The Honorable William C. Ferguson IV, President of the Senate
The Honorable Adrienne A. Jones, Speaker of the House of Delegates
Members of the General Assembly

President Ferguson, Speaker Jones, and Members:

The Tax Expenditure Evaluation Act (formerly the Tax Credit Evaluation Act) establishes a process for evaluating certain tax credits, exemptions, and preferences. Under the Act, the Department of Legislative Services (DLS) is required to evaluate the Credit for the Purchase of Cybersecurity Technology or Services by July 1, 2023.

DLS has conducted its evaluation of the program and makes several findings and recommendations about the tax credit. The document is divided into six chapters.

- **Chapter 1** provides an overview of the Tax Expenditure Evaluation Act and the Credit for the Purchase of Cybersecurity Technology or Services.
- **Chapter 2** provides a discussion of the program's objectives and goals.
- **Chapter 3** provides information on the cybersecurity industry and program, including other cybersecurity-related programs in the State.
- **Chapter 4** provides information on income tax credit activity.
- **Chapter 5** discusses how the program is not effective in fulfilling its objectives of assisting small businesses with the purchase of cybersecurity technologies and services and promoting the cybersecurity industry in the State.

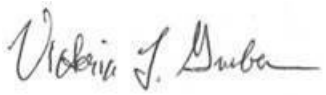


Legislative Services Building •90 State Circle • Annapolis, Maryland 21401-1991
410-946-5500 • FAX 410-946-5508 • TDD 410-946-5501
301-970-5500 • FAX 301-970-5508 • TDD 301-970-5401
Other areas in Maryland 1-800-492-7122

- **Chapter 6** summarizes the findings of the report and discusses recommended changes to the tax credit program.

We wish to acknowledge the cooperation and assistance provided by the Department of Commerce. DLS trusts that this report will be useful to members of the General Assembly in future deliberations about the Credit for the Purchase of Cybersecurity Technology or Services.

Sincerely,



Victoria L. Gruber
Executive Director

Ryan Bishop
Director

VLG:RB/GHB/bao

# Contents

# Executive Summary

Since the mid-1990s, the number of State business tax credits has grown significantly as have related concerns about the actual benefits and costs of these credits. In response to concerns about the fiscal impact of tax credits on State finances, the Tax Expenditure Evaluation Act (formerly the Tax Credit Evaluation Act) establishes a process for evaluating certain tax credits, exemptions, and preferences.

As part of the Tax Expenditure Evaluation Act, the Department of Legislative Services (DLS) is required to evaluate the purchase of cybersecurity technology and cybersecurity service (purchase cybersecurity) credit on a number of factors, including (1) the purpose for which the tax credit was established; (2) whether the original intent of the tax credit is still appropriate; (3) whether the tax credit is meeting its objectives; (4) whether the goals of the tax credit could be more effectively carried out by other means; and (5) the cost of the tax credit to the State and local governments.

The Purchase Cybersecurity Tax Credit Program was established in calendar 2018 in order to promote the cybersecurity industry in Maryland by helping small businesses purchase cybersecurity technologies and services. As of June 2023, the Department of Commerce (Commerce) has certified 86 businesses that have been awarded a total of $2.1 million in credits. On average, in each year, 38 buyers are awarded $444,145 in credits for buying cybersecurity technologies and services from 12 sellers. Most buyers and sellers are located in Central Maryland, and over half of buyers only claim the credit in one year.

DLS makes several findings and recommendations related to the purchase cybersecurity tax credit, as follows.

## The Credit Appears to Be Underutilized

Activity level for the tax credit has been low. Less than 0.1% of small businesses are participating in the program, which suggests that the program is underutilized. Theories for why the tax credit has been underutilized include (1) small businesses do not view cybersecurity as necessary for their business; (2) cybersecurity is still too expensive even with the tax credit; (3) small businesses may not be aware of the credit; and (4) the credit is nonrefundable, so there is no benefit for businesses without an income tax liability.

**Recommendation: DLS recommends that the General Assembly should consider terminating the Purchase Cybersecurity Tax Credit Program and instead explore other options, such as grants, to increase cybersecurity in the State for small businesses.**

If the General Assembly decides not to eliminate the Purchase Cybersecurity Tax Credit Program, DLS has several recommendations to improve the credit that are discussed in the following.

**Recommendation: Commerce and the Comptroller should increase efforts to advertise the tax credit to raise awareness of the program.**

## The Legislative Intent and Performance Metrics of the Credit Are Not Defined

Chapter 578 of 2018 established the tax credit but did not specify a specific goal or intent for the credit. Without clearly defined goals and objectives, it is difficult to identify metrics and data requirements to evaluate the effectiveness of the tax credit.

**Recommendation: The General Assembly should clearly define the intent of the Purchase Cybersecurity Tax Credit Program in statute and consider requiring the intent of any new tax incentive to be clearly expressed.**

**Recommendation: Commerce should define performance metrics for the tax credit program and periodically evaluate the program based on those metrics.**

## One Company Has Overclaimed Credits

Commerce may not certify purchases from a single cybersecurity company that total more than $200,000 in a tax year. However, for tax year 2019, the aggregate credits claimed for cybersecurity technology or cybersecurity services purchased from the seller company Epoch, Inc. exceeded the statutory cap of $200,000.

**Recommendation: Commerce should report to the General Assembly on the safeguards in place to prevent companies from overclaiming credits.**

## Requirements of the Program Add Unnecessary Complexity

Statute requires Commerce to award 25% of the authorized tax credits to qualified buyers that purchase cybersecurity services. This requirement adds a layer of unnecessary complexity, and it is unclear why it matters whether a business buys a service versus a technology.

**Recommendation: The General Assembly should eliminate the statutory requirement that Commerce award 25% of authorized tax credits to qualified buyers that purchase cybersecurity services.**

## Incremental Credits Are Preferred for Incentivizing Growth

An effective tax credit program avoids providing windfalls – awarding tax credits for activity that businesses would have done anyway – by focusing as much of the benefit on increasing marginal spending rather than total or recent spending. The design of the Purchase Cybersecurity Tax Credit Program is likely to provide windfall credits for activities that would have occurred in the absence of the tax credit, due to it being based on a business's total recent expenditures rather than for incremental increases.

**Recommendation: The General Assembly should consider options to redesign the credit to prioritize new spending in cybersecurity.**

## Businesses Are Not Required to Add Back Credits

Statute requires businesses claiming certain business income tax credits to add back to their income the amount of that credit claimed, but the purchase cybersecurity tax credit is not one of them.

**Recommendation: The General Assembly should consider requiring businesses to add back to their income the amount of the purchase cybersecurity credit claimed.**

## Cyberattack Risks Vary by Industry

The purchase cybersecurity tax credit provides a tax credit for any small business regardless of its industry or risk level. However, cybersecurity risks tend to vary by industry. While the healthcare and financial industries have the highest average cost of a data breach, manufacturing is the industry most commonly targeted by cybercriminals.

**Recommendation: The General Assembly should consider providing enhanced credits for industries most at risk of cyberattacks.**

## Commerce Has Not Established an Expert Panel

Commerce, in consultation with the Maryland Technology Development Corporation, may establish a panel composed of experts in the areas of cybersecurity technology and services in order to assist Commerce in determining if a cybersecurity business meets the requirements for a qualified seller. As of July 2023, Commerce has not elected to establish this panel.

**Recommendation: Commerce should report to the General Assembly on why it has not elected to establish this panel. If their answer is insufficient, the General Assembly should consider requiring instead of authorizing Commerce to establish a panel. Otherwise, DLS recommends eliminating the panel in statute.**

# Chapter 1. Overview and Background of the Credit for the Purchase of Cybersecurity Technology or Services

## Overview

Since the mid-1990s, the number of State business tax credits has grown significantly as have related concerns about the actual benefits and costs of many of these credits. Prior to 1995, there was one tax credit for individuals (earned income) and two primarily business tax credits (enterprise zone and Maryland-mined coal credits). Since 1995, at least 40 tax credits primarily for businesses and at least 20 tax credits primarily for individuals have been established. This includes temporary and expired tax credits.

According to the Department of Budget and Management's (DBM) tax expenditure reports, the fiscal impact of individual income tax credits has increased from an estimated $140.5 million in fiscal 2003 to about $350 million in fiscal 2022.

Although the reduction in State revenues from tax credits is generally incorporated in the State budget, many tax credits are not subject to an annual appropriation as required for other State programs. However, most of the larger business credits are subject to an aggregate annual limitation that limits fiscal uncertainty. This limitation is typically either an annual budget appropriation, such as under the historic revitalization and biotechnology incentive investment tax credits, or a limitation on the maximum annual amount of credits that can be awarded, such as under the research and development, film production activity, and job creation tax credits.

Most of these limitations became a component of business tax credits after a significant and unexpected increase in the fiscal cost of the Heritage Structure Rehabilitation Tax Credit Program (since renamed as the historic revitalization tax credit). Of the major business tax credits, only the One Maryland tax credit is not subject to an aggregate annual limitation or annual budget appropriation. The American Institute of Certified Public Accountants lists appropriate government revenues as one of the guiding principles of good tax policy, stating the need to have appropriate levels of predictability, stability, and reliability in a tax system. Improving fiscal certainty can be achieved through annual program limits.

## Tax Expenditure Evaluation Act

### Overview

In response to concerns about the impacts of certain tax credits, Chapters 568 and 569 of 2012 established the Tax Credit Evaluation Act, a legislative process for evaluating certain tax credits. The evaluation process was conducted by a legislative evaluation committee and done in consultation with the Comptroller's Office, DBM, the Department of Legislative Services (DLS),

and the agency that administered each tax credit. The committee reviewed the following credits: enterprise zone; One Maryland; earned income; film production activity; sustainable communities (historic revitalization); businesses that create new jobs; job creation; research and development; biotechnology investment incentive; and Regional Institution Strategic Enterprise Zone Program.

Chapter 575 of 2021 expanded the scope of the Tax Credit Evaluation Act, renaming it to the Tax Expenditure Evaluation Act, and eliminated the evaluation committee. Under the Tax Expenditure Evaluation Act, DLS must evaluate tax credits, exemptions, or preferences on request from the Senate Budget and Taxation Committee, the House Ways and Means Committee, the Executive Director of DLS, or the Director of the Office of Policy Analysis of DLS. In addition, beginning October 1, 2022, DLS must (1) evaluate at least once every 10 years each income tax credit that is primarily claimed by businesses and has an annual fiscal impact exceeding $5.0 million; and (2) in consultation with the Senate Budget and Taxation Committee and the House Ways and Means Committee, publish on its website a schedule of the evaluations that will be conducted. In December 2022, DLS published its evaluation of the More Jobs for Marylanders Program income and sales tax credits and its reevaluation of the One Maryland and enterprise zone tax credits. Current law specifies that the innovation investment incentive and purchase of cybersecurity technology or service tax credits must be reviewed by July 1, 2023.

Under the Tax Expenditure Evaluation Act, DLS is required to evaluate the tax credit, exemption, or preference on a number of factors, including (1) the purpose for which the tax credit, exemption, or preference was established; (2) whether the original intent of the tax credit, exemption, or preference is still appropriate; (3) whether the tax credit, exemption, or preference is meeting its objectives; (4) whether the goals of the tax credit, exemption, or preference could be more effectively carried out by other means; and (5) the cost of the tax credit, exemption, or preference to the State and local governments.

## Credit for the Purchase of Cybersecurity Technology or Services

### Overview

Chapter 578 of 2018 created a tax credit (purchase cybersecurity) against the State income tax for qualified buyers who purchase cybersecurity technology or services from a qualified seller. A qualified buyer may claim an income tax credit equal to 50% of the eligible costs incurred to purchase the cybersecurity technology or service, not to exceed $50,000 per qualified buyer. The Department of Commerce (Commerce) may not certify purchases from a single qualified seller that total more than $200,000 in a tax year.

A qualified seller is a for-profit business that (1) is engaged primarily in the development of innovative and proprietary cybersecurity technology or the provision of cybersecurity service; (2) has its headquarters and base of operations in the State; (3) has less than $5.0 million in annual revenue; (4) is a minority-owned, woman-owned, veteran-owned, or service-disabled veteran- owned business or is located in a historically underutilized business zone designated by

the U.S. Small Business Administration; (5) owns or has properly licensed any proprietary technology or provides cybersecurity services; and (6) is in good standing. A qualified buyer is any entity that has less than 50 employees in the State and is required to file a State income tax return.

Commerce, in consultation with the Maryland Technology Development Corporation, may establish a panel composed of experts in the areas of cybersecurity, technology, and services in order to assist Commerce in determining if a cybersecurity business meets the requirements for a qualified seller. As of July 2023, Commerce has not established this panel.

The Secretary of Commerce must approve each application that qualifies for the purchase cybersecurity tax credit. The Secretary was authorized to approve a total of $2.0 million in tax credits in tax year 2018 and, beginning in tax year 2019, may approve $4.0 million annually in tax credits. The Secretary must award 25% of the total tax credits awarded in each year to qualified buyers that purchase cybersecurity services.

Commerce may revoke its certification of the purchase cybersecurity tax credit if any representation made in connection with the application for certification is determined to have been false. A qualified buyer may have an opportunity to appeal any revocation to Commerce before notification of the Comptroller. The Comptroller may make an assessment to recapture any amount of tax credit that a qualified buyer has already claimed.

On or before December 31 each year, Commerce must report annually to the Governor and General Assembly specified information on the economic development programs administered by Commerce, including the purchase cybersecurity tax credit. The information required in this report was expanded under Chapter 116 of 2022 to include (1) a statement indicating if Commerce reduced, revoked, or recaptured a tax credit or any financial assistance from a tax credit recipient; and (2) if applicable, the amount recovered, any penalty assessed, and a justification for the reduction, revocation, or recapture.

Finally, Commerce and the Comptroller must jointly adopt regulations to implement the tax credit application, approval, and monitoring processes. As of July 2023, these regulations have not been adopted.

## Legislative Changes

The purchase cybersecurity tax credit requirements and benefits remain as they were originally enacted in 2018. The Senate passed legislation in 2019 (Senate Bill 726) proposing to expand eligibility for the tax credit, but the bill failed to advance in the House of Delegates. Senate Bill 726 would have expanded eligibility for the tax credit by eliminating the requirement that a qualified buyer must have fewer than 50 employees in the State.

## Tax Credits in Other States

Tax credits for the purchase of certain products is a common incentive offered by many states, including Maryland. States use these incentives, for example, to encourage the purchase of energy efficient vehicles and appliances. However, DLS is unaware of any similar tax credit programs in other states that require purchases be made from certain businesses or that specifically provide tax credits for purchasing cybersecurity technology or services.

While DLS is not aware of any states with tax credit programs like purchase cybersecurity, other states provide tax credits designed to improve cybersecurity and to build their cybersecurity workforce. Oklahoma, for example, offers the software/cybersecurity employee tax credit, which provides up to $2,200 annually for qualifying employees who receive a degree from an Accreditation Board for Engineering and Technology accredited institution, or $1,800 annually for qualifying employees who are awarded a certificate from a technology center accredited by the Oklahoma State Board of Career and Technology Education. To receive the credit, employees must meet strict educational requirements and obtain employment in a qualified industry for a qualified employer.

## Commerce Clause

One reason why other states may not have a program similar to the purchase cybersecurity tax credit program may be due to concerns over the Commerce Clause of the U.S. Constitution. After Senate Bill 228 of 2018 was enacted as Chapter 578, the Attorney General of Maryland issued a letter raising a significant Commerce Clause concern but concluded that the bill is not clearly unconstitutional. The Commerce Clause prohibits states from legislating in ways that impede the flow of interstate commerce." *Star Scientific, Inc. v. Beales*, 278 F.3d 339, 354-55 (4th Cir. 2002). The Attorney General of Maryland wrote that providing a tax credit for investing in a Maryland cybersecurity company creates an advantage for in-state businesses to raise revenue and arguably ties a taxpayer's effective tax rate to whether an investment involved a local company, thus risking a determination by a reviewing court that the tax credit is unconstitutional. The burden on interstate commerce is arguably less, however, because the pool of buyers and sellers who benefit from the tax credit do not include all in-state companies selling cybersecurity products or services. The Attorney General concluded "there is no doubt a risk that a court would find the tax credits offered in Senate Bill 228 violate the Commerce Clause… Nevertheless, it is our view that the bill is not clearly unconstitutional."

# Chapter 2. Intent and Objectives of the Credit for the Purchase of Cybersecurity Technology or Services

## Program Does Not Specify a Goal or Objective

Chapter 578 of 2018 established the purchase of cybersecurity technology or service (purchase cybersecurity) tax credit but did not specify a specific goal or intent for the credit. In addition, program regulations have not yet been issued as of July 2023 that could specify intent.

Without clearly defined goals and objectives, it is difficult to identify the metrics and data needed to evaluate the effectiveness of the tax credit. The Tax Expenditure Evaluation Act requires the Department of Legislative Services (DLS) to evaluate whether the original intent of the tax credit, exemption, or preference is still appropriate; however, there is no statutory requirement for tax credits, exemptions, or preferences to include an intent.

## Program Benefits Cited by Department of Commerce and Program Advocates

While there is no intent stated in statute or regulation, the Department of Commerce (Commerce) states on its website that the credit is designed to promote the cybersecurity industry in Maryland by helping small businesses purchase cybersecurity technologies and services from Maryland cybersecurity companies to protect business information. Commerce's fiscal 2022 annual report states, "as the purpose of this program is to build local supply chains in the cybersecurity industry and to support Maryland-based cybersecurity firms, any assistance rendered through it to any Maryland business counts as a successful outcome."

In its advocacy for the tax credit, Governor Lawrence J. Hogan, Jr.'s Administration testified that the credit incentivizes Maryland's small businesses to "take the actions needed to mitigate their cyber risk." Maryland's Technology Development Corporation commented that the tax credit "represents a dual value to the region. On one hand the tax incentive will be helping locally based businesses improve their cyber health through the purchase and implementation of state-of-the-art cyber products while at the same time promoting the procurement of products from early-stage Maryland-based cybersecurity companies, thereby increasing their value."

The Hogan Administration noted in its written testimony that the Administration and Commerce engaged cybersecurity stakeholders during the 2017 interim on best practices to grow and nurture the Maryland cyber sector. This discussion highlighted that the key for growth and success for emerging cybersecurity companies is revenue since investors look at a company's sales when making investment decisions. The Administration stated, "successful cybersecurity start-ups in Maryland reported to us that for every dollar in revenue, they can raise $10 in investments."

The Cybersecurity Association of Maryland, Inc. (CAMI) asserted that "several key factors inhibit connections between Maryland businesses and Maryland's cybersecurity companies. Maryland's cyber industry places a disproportionate focus on government work and because many out-of-state competitors may have large marketing budgets and be better known, Maryland's cybersecurity solution providers are often overlooked by buyers in Maryland." Additionally, small businesses in general often do not believe a cyber breach will happen to them and view cybersecurity as "too expensive for the little guy." Continuing, CAMI argued that the tax credit would be "especially helpful to encourage Maryland businesses to take action to address cyber risks and do so by purchasing local solutions" that would "be a win for Maryland cybersecurity companies, Maryland businesses, as well as those customers whose personal data would be compromised if a breach takes place."

Other proponents of the tax credit wrote that the credit incentivizes "companies to buy local" and motivates Maryland-based cybersecurity companies "to maintain a physical presence in the State while growing and expanding their customer base." Proponents also argued that the tax credit would bring "more high paying Maryland jobs and more state tax revenues."

## Is the Intent of the Purchase Cybersecurity Tax Credit Still Valid?

DLS assumes that the intent of the tax credit is, as Commerce states on its website, to promote the cybersecurity industry in Maryland by helping small businesses purchase cybersecurity technologies and services from Maryland cybersecurity companies to protect business information. As the intent of the purchase cybersecurity tax credit is twofold, to promote the cybersecurity industry in Maryland and to help small businesses protect business information, DLS examined each intent separately.

### Helping Small Businesses Protect Business Information

Helping small businesses protect business information from cyber threats is important. In recent years, cybersecurity and privacy issues have drawn attention from the general public and policymakers due to many ransomware attacks and data breaches that have occurred in Maryland and throughout the nation. Cyberattacks can cost businesses money and disrupt services. In the *2021 U.S. Small Business Recovery and Technology Report*, small-business owners identified taking appropriate security precautions as the number one challenge they faced when it comes to technology. In the same report, 29% of survey respondents reported having been the victim of a cyberattack, of which half of those experienced a service interruption and a third had information falsely sent from their domains and/or email addresses.

The U.S. Cybersecurity and Infrastructure Security Agency reports nearly 59% of U.S. small- and medium-sized businesses do not have a contingency plan that outlines procedures for responding to and reporting data breach losses. An analysis of research data compiled by the Ponemon Institute found that the average cost of a data breach in 2023 was $4.45 million, a 15.3% increase from $3.86 million in 2020. The analysis also found that only one-third of

companies discovered the data breach through their own security teams, and when attackers disclosed a breach, it costs organizations almost $1.0 million more compared to internal detection.

The Federal Bureau of Investigation's *2022 Internet Crime Report* states Internet crime complaints that it has received, along with losses, have risen in the past five years from 351,937 complaints and $2.7 billion in losses in 2018 to 800,944 complaints and $10.3 billion in losses in 2022. These complaints consist of a wide array of Internet scams affecting victims globally. Victims in Maryland have risen from 8,777 victims totaling $47.2 million in 2018 to 11,644 victims in Maryland totaling $217.9 million in 2022. The U.S. Securities and Exchange (SEC) Commission reports, "the number of reported breaches disclosed by public companies has increased almost 600% over the last decade, from 28 breaches in 2011 to 131 breaches in 2020 and 188 breaches in 2021." McKinsey & Company predicts that damage from cyberattacks will increase to $10.5 trillion by 2025, a 300% increase from 2015 levels.

SEC attributes the substantial rise in the prevalence of cybersecurity incidents to the following factors: "the increase in remote work spurred by the COVID-19 pandemic; the increasing reliance on third-party service providers for information technology services; and the rapid monetization of cyberattacks facilitated by ransomware, black markets for stolen data, and crypto-asset technology."

In addition to the number of cybersecurity incidents increasing, the costs and adverse consequences of cybersecurity incidents to companies are growing. These costs include business interruption, lost revenue, ransom payments, remediation costs, liabilities to affected parties, cybersecurity protection costs, lost assets, litigation risks, and reputational damage. Maintaining customer digital trust is important to a business's success; McKinsey & Company found almost 10% of survey respondents in the past 12 months stopped business with a supplier after learning of a data breach. SEC observed that costs to companies and their investors of cybersecurity incidents are rising, so the commission adopted rules on July 26, 2023, requiring registrants to disclose material cybersecurity incidents that they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.

The intent of the purchase cybersecurity tax credit to help small businesses protect business information is even more applicable today given the costs of cyberattacks and the increase in frequency and sophistication of cyberattacks. As the frequency, costs, and sophistication of cyberattacks increase, so does the importance of the cybersecurity industry.

## Promoting Maryland's Cybersecurity Industry

Strengthening Maryland's cybersecurity industry can be viewed as a valid goal. Maryland-based national security organizations like the National Security Agency, the Defense Information Systems Agency, and U.S. Cyber Command serve as anchor organizations for the cybersecurity cluster in Maryland. The clustering of established companies, startups, and business incubators around anchor institutions creates technology spillovers that boost innovation by enhancing the exchange of ideas and "open innovation."

Academic studies have found that industries located within a strong cluster are associated with higher employment growth and wage growth, along with an increase in the number of establishments and patents. One study lists the benefits of clustering as a pool of specialized labor, knowledge spillover, access to capital, and interorganizational linkages. A program that is focused on promoting the cybersecurity industry within Maryland and encouraging the growth of the State's cybersecurity cluster will likely produce long-term benefits to the State.

# Chapter 3. Cybersecurity Industry, Recent Developments, and Programs

## Cybersecurity Industry in Maryland

The cybersecurity industry plays an important role in Maryland's economy. There are over 500 cybersecurity organizations located in Maryland, and Maryland's cybersecurity ecosystem is geographically focused around large federal installations, including the National Security Agency (NSA) and Fort Meade. Recent industry publications have consistently ranked Maryland as one of the nation's leaders in the cybersecurity industry. The Maryland Department of Commerce (Commerce) states on its website that Maryland is a "hotbed of innovation in the cybersecurity sector" and has one of the industry's largest concentrations of cybersecurity expertise and resources. Maryland's cybersecurity workers are highly skilled and highly specialized, and many have experience at Maryland-based national security organizations such as NSA, the Defense Information Systems Agency, the National Institute of Standards and Technology (NIST), Intelligence Advanced Research Projects Activity, the Johns Hopkins University Applied Physics Lab, U.S. Cyber Command, and the Department of Defense Cyber Crime Center. In addition, Maryland is home to 20 higher education institutions that are recognized as National Centers of Academic Excellence in Cybersecurity. In calendar 2019, one industry expert noted that Maryland's universities and colleges "have awarded 10,000 bachelor's degrees in cybersecurity-related programs since 2015, more than anywhere else in the country."

## Recent Developments in Cybersecurity

In recent years, cybersecurity has become a high priority for many lawmakers, especially in light of several recent ransomware attacks and data breaches that have occurred in Maryland and throughout the nation. Since calendar 2019, there have been several high-profile ransomware attacks in the State, including multiple Southern Maryland towns losing computer access after a third-party vendor was attacked, an attack on the Baltimore County Public Schools and Baltimore City government operations, and an attack on several servers at the Maryland Department of Health during the COVID-19 public health crisis.

Because of the increased frequency of cybersecurity attacks and the operational disruptions and economic loss from these attacks, lawmakers are attempting to catch up with cyber attackers and technology by altering criminal statutes and increasing criminal penalties for these acts, establishing new entities or tasking existing entities with monitoring cybersecurity, developing and providing advice on best practices, and requiring private entities to meet specified cybersecurity standards and reporting requirements.

In December 2022, the Department of Legislative Services reported on *Recent Developments in Cybersecurity*, focusing on recent legislation and other actions in Maryland to

address cybersecurity issues and cybersecurity-related actions taken by other states and the federal government. The following discussion highlights some of the measures and actions described in that report.

# Executive and Legislative Action in Maryland

## Gubernatorial Action on Cybersecurity

In June 2019, Governor Lawrence J. Hogan, Jr. signed Executive Order 01.01.2019.07, which created the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative created the Office of Security Management (OSM) within the Maryland Department of Information Technology (DoIT) and charged the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch information technology (IT) systems. The office is led by the State Chief Information Security Officer (SCISO) who is appointed by the Governor. The order also established the Maryland Cybersecurity Coordinating Council to assist SCISO and the office in their duties.

In July 2021, Governor Hogan announced several cybersecurity measures, including a partnership with NSA, a memorandum of understanding with the University of Maryland Baltimore County (UMBC) to establish the Maryland Institute of Innovative Computing, and an executive order creating a statewide privacy framework to govern the manner in which the State secures the personally identifiable information of its residents. In calendar 2022, Governor Hogan announced several budgetary investments to bolster the State's cyber readiness and workforce development programs. The additional funding aimed to expand and accelerate critical IT projects throughout the State, launch the Maryland Cyber Range for Elevating Workforce and Education, and provide universal and equitable access to Advance Placement Computer Science courses in every State high school.

## Cybersecurity Legislation

### Maryland Cybersecurity Council

Chapter 358 of 2015 established the Maryland Cybersecurity Council, staffed by the University of Maryland University College (now called the University of Maryland Global Campus). The council is required to work with NIST, as well as other federal agencies, private-sector businesses, and private cybersecurity experts to address State cybersecurity issues. The council's responsibilities include (1) examining inconsistencies between State and federal cybersecurity laws; (2) assisting private-sector cybersecurity businesses in adopting, adapting, and implementing the NIST cybersecurity framework of standards and practices; and (3) recommending legislative changes to address cybersecurity issues. The council engages in a variety of activities to fulfill its duties, including conducing public outreach and education, informing legislation, and developing and producing materials on cybersecurity issues.

### 2022 Cybersecurity Legislative Package

A package of cybersecurity bills passed by the General Assembly during the 2022 session codified the Maryland Cyber Defense Initiative (discussed previously) and further established reforms related to cybersecurity and IT asset funding, maintenance, and safeguarding. Chapter 231 established data security standards for insurance regulators, insurers, and other carriers to mitigate losses from data breaches. Under the Act, carriers must perform a prompt investigation when learning that a cybersecurity event has or may have occurred and then notify the Maryland Insurance Commissioner under certain circumstances.

Chapter 241 established the Cybersecurity Preparedness Unit in the Maryland Department of Emergency Management and the Information Sharing and Analysis Center in DoIT. It also required certain local governments to create cybersecurity preparedness plans, complete assessments, and report local cybersecurity incidents. Units of local government that use the State-operated broadband network must certify their compliance with the established minimum standards.

Chapter 242 codified and expanded the responsibilities of the Maryland Cybersecurity Coordinating Council, OSM, and SCISO. Chapter 242 also required State agencies and local governments to report cybersecurity incidents and required units of State government and certain units of local government to complete cybersecurity preparedness assessments. In addition, DoIT's responsibilities were expanded to include centralizing the management and direction of certain IT while allowing State agencies to maintain their IT units. To accomplish this goal, DoIT was further required to develop a centralization transition strategy and conduct a performance and capacity assessment.

Chapter 243 established an independent Modernize Maryland Oversight Commission to ensure the security of information and to advise the State on appropriate cybersecurity upgrades. Additionally, it required water and sewer systems that serve more than 10,000 users and receives financial assistance from the State to assess their vulnerability to cyberattacks and make plans to address the vulnerabilities. Chapter 243 also established the Local Cybersecurity Support Fund to financially support local government cybersecurity preparedness activities.

### Public Utility Cybersecurity Legislation

Chapter 499 of 2023 requires the Public Service Commission to include one or more cybersecurity experts on its staff, collaborate with OSM to establish cybersecurity standards and best practices for regulated public service companies, and report cybersecurity-related information to the SCISO every two years. Each public service company, except common carriers and telephone companies, must (1) establish cybersecurity standards that meet or exceed standards adopted by the commission; (2) adopt a "zero-trust" cybersecurity approach to on-premises and cloud-based services; and (3) submit to a third-party cybersecurity assessment every two years and submit related certifications of compliance to the commission.

## Small Business Cybersecurity Resilience in Maryland Program

Commerce was awarded Cybersecurity for Small Business Pilot Program funds from the U.S. Small Business Administration. Through its Small Business Cybersecurity Resilience in Maryland program, Commerce will use the federal funds to provide training and direct services for 40 small businesses to help them mitigate future cyberattacks through employee training and the installation of advanced hardware and software. Service providers will be contracted to conduct security scans of the clients' existing cybersecurity systems. All small business employees will complete cybersecurity hygiene training, and selected employees, as identified by those security scans, will complete more extensive training regarding cybersecurity fundamentals tailored to their level of knowledge. Additionally, these selected employees will complete industry-specific training regarding issues of particular concern to their business. After training is completed, mitigation services contractors will supply and install the highest priority hardware and software as identified on the security scan for up to $10,000 per business.

## Federal Actions

In May 2021, President Joseph R. Biden, Jr. signed an executive order designed to improve cybersecurity by "protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur." The executive order requires that all federal information systems should meet or exceed the standards and requirements set forth in and issued pursuant to the order. In addition to safeguarding federal networks, the executive order aims, by setting criteria for federal procurement, to use the federal government's purchasing power to drive markets and thereby make all software more secure.

The following November, President Biden signed the Infrastructure Investment and Jobs Act, allocating approximately $1.9 billion to guard states and local government entities against cybersecurity attacks. The Act created a State and Local Cybersecurity Grant Program through the U.S. Department of Homeland Security to address cybersecurity threats against state and local governments and established a Cyber Response and Recovery Fund to assist the Cybersecurity and Infrastructure Agency's response to a cybersecurity attack. It also provided funding for cybersecurity research for telecommunications equipment and industrial control systems, established grants and research programs to develop the capacity of the energy sector at the federal, state, and local level to assess risks to cybersecurity and provided funding through several federal entities for infrastructure projects that have a tangential focus on cybersecurity development.

## Recent Legislative Activity in Other States

According to the National Conference of State Legislatures (NCSL), at least 40 states and Puerto Rico considered more than 250 bills or resolutions dealing with cybersecurity in calendar 2022. NCSL reports that the most common enactments (1) require government agencies to implement cybersecurity training, establish and implement formal security policies and practices, provide mandatory training to employees, and report cybersecurity incidents; (2) provide funding for cybersecurity programs and practices in state and local government; (3) mandate election-related security practices; and (4) establish or enhance cybersecurity workforce training and education programs.

## Workforce Development

Concerns over cybersecurity workforce shortages appear to be a national concern. NCSL, cybersecurity and IT experts, and sources of employment and education data have highlighted that human resources in the cybersecurity industry remain in scarce supply. In 2022, the International Information System Security Certification Consortium, a nonprofit that offers cybersecurity training and certification programs, reported that in the United States there are approximately 1.2 million cybersecurity professionals in the workforce and an unfilled need for another 436,080 workers. Additionally, the U.S. Bureau of Labor Statistics projects "information security analyst" will be the eighth fastest growing occupation over the next decade, with an employment growth rate of 35% compared to the 5% average growth rate for all occupations.

According to CyberSeek, a cybersecurity data aggregator, there are only enough cybersecurity workers to fill 68% of the cybersecurity jobs that employers demand in Maryland, compared to 69% nationally. CyberSeek estimates there were 52,767 workers employed in cybersecurity-related jobs from May 2022 through April 2023, while there were 30,128 online job listings for cybersecurity-related positions during that timeframe. CyberSeek is a tool created in partnership with the National Institute of Standards and Technology, Lightcast, and CompTIA to facilitate filling cybersecurity vacancies and share data regarding the cybersecurity job market.

Heightened awareness of the human resource needs in cybersecurity and IT is prompting leaders in government and industry to examine ways to expand educational opportunities and grow the cyber workforce. In July 2022, President Biden hosted a National Cyber Workforce and Education Summit, bringing together leaders from government and across the cyber community, with a focus on building the cyber workforce; improving skills-based pathways to cyber jobs; and improving diversity, equity, inclusion, and accessibility in the cyber field.

Cybersecurity is a top focus of the Maryland Department of Labor's Employment Advancement Right Now (EARN) program. The EARN Maryland program is an industry-led initiative that helps businesses cultivate the skilled workforce that they need to compete while preparing Marylanders for meaningful careers. Beginning in fiscal 2018, the budget for EARN has included a $3 million targeted investment into cyber and IT. This added investment has allowed

EARN to grow the number of Cyber and Information Technology grantees from 3 to nearly 20 in calendar 2022. The program has placed more than 2,000 individuals into employment in the industry and provided training for over 1,900 incumbent workers.

## Other Cybersecurity Investment Programs in Maryland

Given the large importance of the cybersecurity industry to Maryland's economy, the State, along with other organizations, provides various forms of support to the industry as discussed in the following.

### Maryland Innovation Investment Tax Credit

The Maryland Innovation Investment Tax Credit program, administered by Commerce, offers a refundable income tax credit for investments in qualified Maryland technology companies, including cybersecurity companies. An investor who invests at least $25,000 in a qualified Maryland technology company (QMTC) can claim a credit equal to 33% of the investment, not to exceed $250,000. If QMTC is located in Allegany, Dorchester, Garrett, or Somerset counties or, under certain circumstances, is located in a Regional Institution Strategic Enterprise zone, the value of the credit for investments made in these companies is equal to 50% of the investment, not to exceed $500,000.

### Maryland Technology Development Corporation Programs

The Maryland Technology Development Corporation assists Maryland's next wave of startup companies through a variety of resources and seed funds. The Cybersecurity Investment Fund supports Maryland companies in the development and commercialization of new cybersecurity products or services by providing investments of up to $100,000. The Technology Commercialization Fund invests more broadly in early-stage technology companies.

### Other Programs

According to Commerce's website, DataTribe is a cybersecurity-focused startup foundry in Fulton, Maryland that provides capital, facilities, and a variety of services to qualified cybersecurity startups. In addition, the Cyber Incubator@bwtech, located adjacent to UMBC, provides dedicated space and resources for early stage and cybersecurity startup companies.

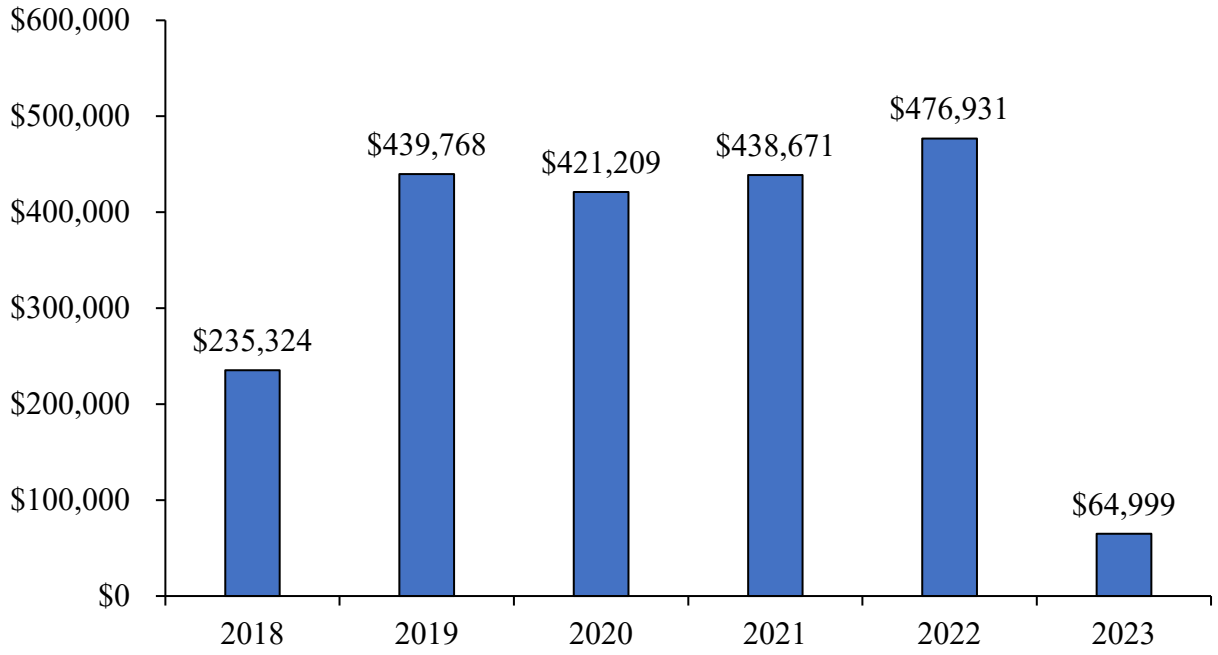
The Cybersecurity Association of Maryland is a statewide 501(c)(6) nonprofit organization established in 2015. The organization was originally created to drive the growth of Maryland's cybersecurity industry and now serves the cybersecurity ecosystem through advocacy, education, and building community. It connects cybersecurity companies with businesses and government entities seeking cybersecurity products and services and connects cybersecurity job seekers in Maryland and beyond with jobs and resources for gaining the skills, education, and certifications needed for jobs of interest.

# Chapter 4. Program Fiscal Impact

## Annual Amount of Credits Certified

The Department of Commerce (Commerce) certifies buyers that have met the qualifications of the Purchase Cybersecurity Program and the credit amount that the buyers can claim, along with certifying qualified Maryland cybersecurity sellers. As of June 2023, Commerce has certified 86 businesses that have been awarded a total of $2.1 million in credits. **Exhibit 4.1** shows the total amount of credits certified each year, and **Appendix 1** provides further details on the total number of buyers, sellers, and average credit claimed. On average, in each year through calendar 2022, 34 buyers were awarded a little over $400,000 in credits for buying cybersecurity technologies and services from 11 sellers.

**Exhibit 4.1**
**Purchase Cybersecurity Tax Credits Certified**
**Calendar 2018-2023**



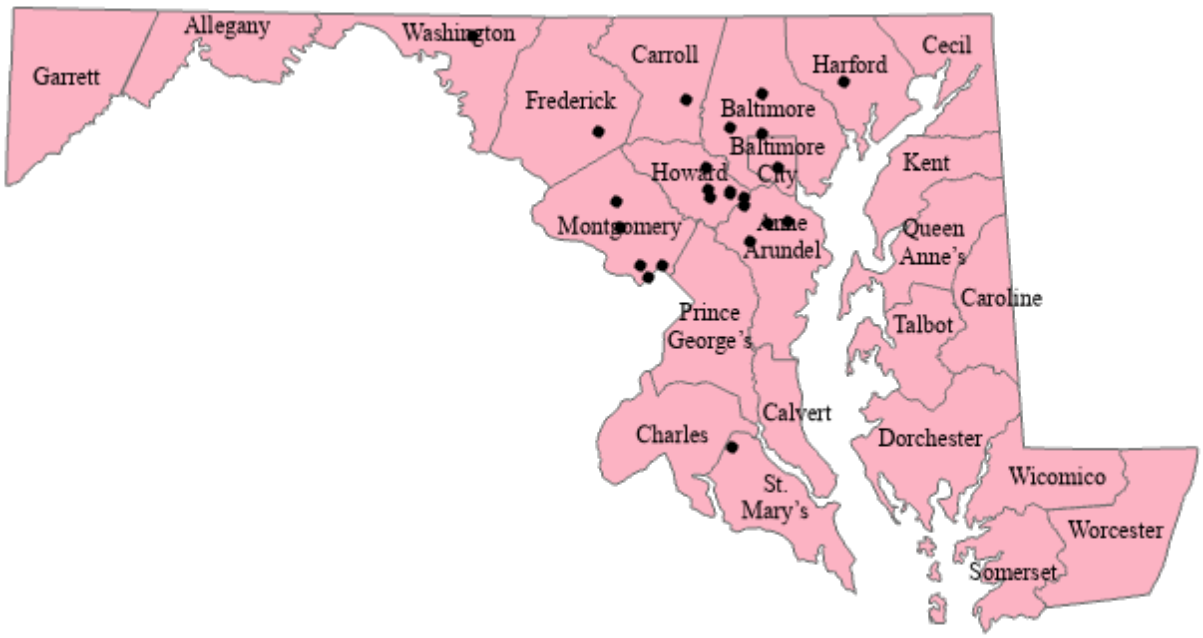

Note: Calendar 2023 is through June 2023.

Source: Department of Commerce; Department of Legislative Services

## Most Buyers and Sellers Are Located in Central Maryland

**Exhibit 4.2** shows the location of the 25 qualified cybersecurity sellers as of July 2023. Most qualified sellers are located in Central Maryland, with 60% of sellers being located in Anne Arundel, Howard, or Montgomery counties. Only one seller is located in Western Maryland (Washington County), and no sellers are located on the Eastern Shore. One way to qualify as a qualified cybersecurity seller is to be located in a historically underutilized business zone as designated by the U.S. Small Business Administration (SBA), but no sellers have identified as being located in those zones.

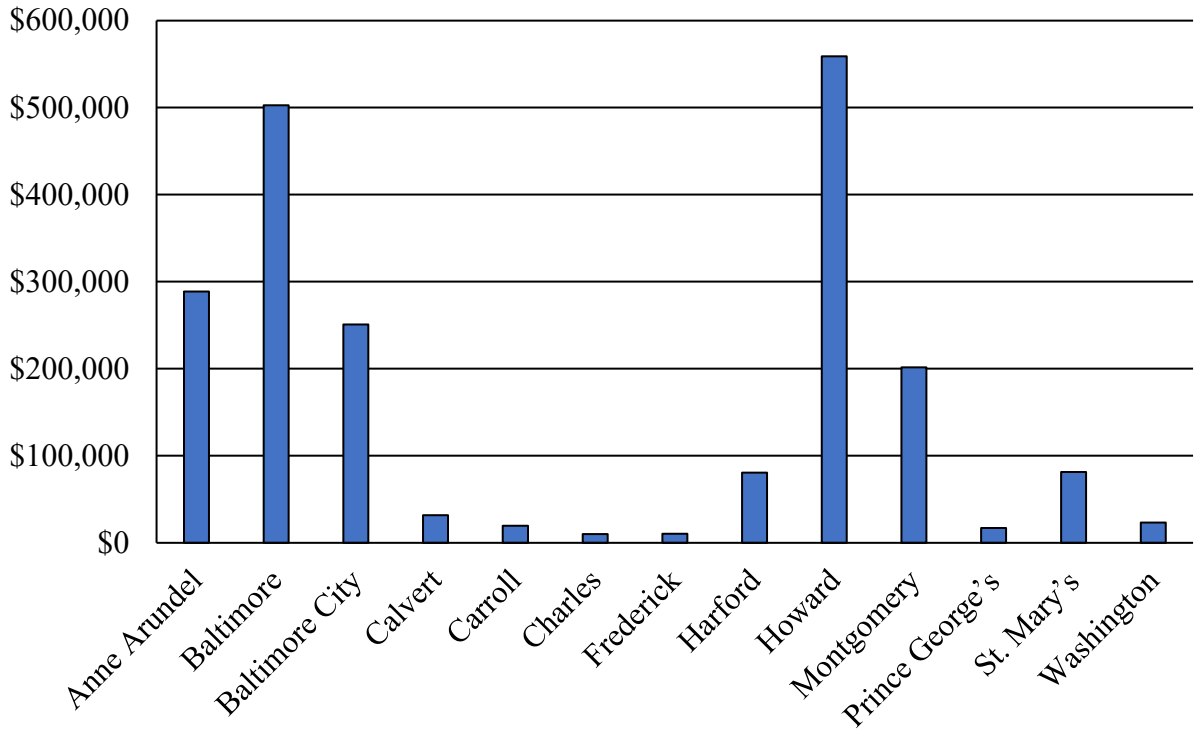
**Exhibit 4.2**
**Qualified Cybersecurity Sellers**
**July 2023**




Source: Department of Legislative Services

Likewise, most credits have been awarded to buyers that are in Central Maryland. Over half of all credits have been awarded to qualified buyers in Baltimore and Howard counties. Approximately a quarter of credits have been awarded to qualified buyers in Anne Arundel County and Baltimore City, and almost 10% of credits have been awarded to buyers in Montgomery County. **Exhibit 4.3** shows the certified credits by the county of the buyer. No credits have been awarded to buyers in 11 counties, which consist of all of the Eastern Shore counties (Caroline, Cecil, Dorchester, Kent, Queen Anne's, Somerset, Talbot, Wicomico, and Worcester counties) and Allegany and Garrett counties in Western Maryland.

**Exhibit 4.3**
**Purchase Cybersecurity Tax Credits Certified by County of Buyer**
**Total from Calendar 2018-2023**




Note: Total credits are through June 2023.

Source: Department of Commerce; Department of Legislative Services

## Sellers

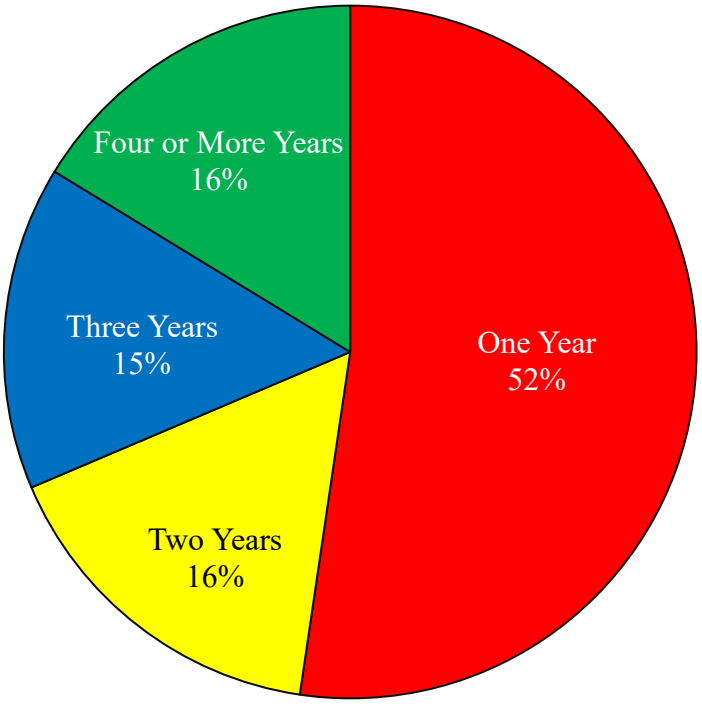
There are 25 businesses as of July 2023 that are qualified as cybersecurity sellers under the program. However, typically only between 8 to 13 companies have cybersecurity sales that benefit from the tax credit in a single year. Almost half of all tax credits from tax year 2018 to June 2023 have been from cybersecurity sales from one company, Epoch, Inc. Epoch, Inc. advertises that it is a qualified Maryland cybersecurity seller on its website and that, out of all the certified sellers, it has given the most tax credits to clients each year. In fact, Commerce has certified too many tax credits from Epoch, Inc. sales. Commerce may not certify purchases from a single cybersecurity company that total more than $200,000 in a tax year. However, Commerce approved $251,048 of tax credits in tax year 2019 for Epoch, Inc., so Commerce recaptured $51,048 in tax credits on February 26, 2020, when it realized its mistake.

To be a qualified cybersecurity seller, a business must have less than $5.0 million in annual revenue; be a minority-owned, woman-owned, veteran-owned, or service-disabled veteran-owned business; or be located in a historically underutilized business zone designated by SBA. Of the businesses that are currently qualified as cybersecurity sellers, all but two qualified by having less than $5.0 million in annual revenues. Almost half of the sellers identified as a minority-owned, woman-owned, veteran-owned, or service-disabled veteran-owned business, while no seller was located in a historically underutilized business zone.

## Buyers

Since 2018, 86 buyers have been certified for the credit, and since then, on average, 34 buyers received tax credit certificates in each year through tax year 2022. Over half of buyers have only claimed the credit in one year, as shown in **Exhibit 4.4**. As of June 2023, nine companies have claimed the credit in at least five years.

**Exhibit 4.4**
**Breakdown of Years Buyers Claimed Credit**




Source: Department of Legislative Services

Commerce has some theories on why companies typically only claim the credit for one year. Many buyers have specific cybersecurity needs that could be served by a one-time or one-year purchase. Once those needs are met, they do not need to continue purchasing these technologies and services from the same seller. For example, many sellers help buyers choose cybersecurity products and set up security hardware devices, firewalls, antivirus software, encryption software, etc. on computers and laptops. Many of those do not require repeated purchases from the same seller each year. After the seller completes the initial cybersecurity setup, the buyer company may have staff learn or develop the basic/general cybersecurity skills that can make the business less reliant on the seller's service.

Another reason could be that cybersecurity technologies and services may be expensive. Buyers are small companies under 50 employees, so they may still have financial limitations that prevent them from making a cybersecurity technology purchase or renewing a service contract. Even though the tax credit offsets some of the costs, the fees, freights, sales tax, and additional general information technology products or services purchased from the seller are ineligible. Another explanation is if the quality of service provided by a seller does not meet the buyer's expectations during the first year of a contract, the buyer may decide not to renew the contract. Additionally, the program has matured over the years, so Commerce may see an uptick in "repeat buyers," as it continues to progress and sellers continue to market their products and services as well as the availability of the tax credit. Lastly, buyers may have gone out of business themselves, their needs may have changed in subsequent years, or they potentially found a similar product/service at a cheaper price from another seller.

## Cybersecurity Services, Technologies, and Resellers

Most buyers are purchasing cybersecurity services as opposed to cybersecurity technologies. Statute requires Commerce to award 25% of the authorized tax credits to qualified buyers that purchase cybersecurity services. Commerce has $4.0 million available for tax credits for each tax year after 2018, so $3.0 million is available for the purchase of cybersecurity technologies, and $1.0 million is available for the purchase of cybersecurity services. While the total overall amount of tax credits certified by Commerce each year has been well under $1.0 million, the annual tax credit amounts certified for cybersecurity services far exceed those for cybersecurity technologies. Since tax year 2018 through June 2023, Commerce has awarded $428,600 of credits for cybersecurity technologies (21%) and $1.6 million of credits for cybersecurity services (79%). Tax credits for cybersecurity technologies have totaled approximately $100,000 or less in any given year.

The Department of Legislative Services questions the effectiveness of reserving 25% of authorized tax credits for qualified buyers that purchase cybersecurity services. If the purpose of the tax credit is to help small businesses protect business information, whether the business is purchasing cybersecurity technologies or services should not be of consequence as long as it is protecting business information. Commerce could not provide a rationale for distinguishing cybersecurity technologies from services other than noting its obligation to comply with the

statutory requirement. While this requirement has no clear benefit, the cost is added complexity and bureaucracy, as the requirement adds another criteria that Commerce must track.

Less than 1% of credits have been for third-party resellers. A reseller is any company selling cybersecurity technologies or services that is not identified as a certified qualified Maryland cybersecurity seller by Commerce. To be able to claim the tax credit for cybersecurity purchases from a third-party reseller, the cybersecurity technology or service being purchased must have originated from a qualified Maryland cybersecurity seller. This requires that the name of the qualified Maryland cybersecurity seller be identified on an invoice from a third-party seller along with a description of the cybersecurity technology or service that was purchased.

## Administrative Costs

Commerce administers the Purchase Cybersecurity Tax Credit Program. Commerce must approve tax credit applications from qualified buyers by determining whether the business is a small business and determining whether cybersecurity technology and products qualify for the credit. Commerce must also review seller applications and determine whether a company is a qualified seller. While Commerce may establish a panel to assist in determining whether a company is a qualified seller, Commerce has opted not to establish the panel. Currently one program administrator spends a portion of their time overseeing the program at Commerce, so administrative costs are minimal.

## Local Fiscal Impact

Local governments receive a portion of income tax revenues to support the construction and maintenance of local roads and other transportation facilities. Any purchase cybersecurity income tax credits claimed against the corporate income tax therefore decrease local highway user revenues.

Statute requires businesses claiming certain business income tax credits to add back to their income the amount of that credit claimed. Doing so helps local governments because local government revenues will increase minimally due to taxpayers adding back the amount of credit claimed against the personal income tax. Statute does not require a business to add back to its income the amount of purchase cybersecurity tax credit claimed.

# Chapter 5. Effectiveness of the Program

## Program Lacks Clear Goals

Statute does not state a goal or intent for the Purchase Cybersecurity Tax Credit Program. Without clearly defined goals and objectives, it is difficult to identify the metrics and data needed to evaluate the effectiveness of the tax credit. The Tax Expenditure Evaluation Act requires the Department of Legislative Services (DLS) to evaluate whether the original intent of the tax credit is still appropriate, whether the tax credit is meeting its objectives, and whether the goals of the tax credit could be more effectively carried out by other means. However, there is no statutory requirement for tax credits to include an intent, and since the intent, objectives, and goals of the tax credit are not clearly defined in statute, DLS can only infer these things.

Other states require that the intent of tax incentives to be clearly expressed. For example, in Minnesota, the legislature must include a statement of purpose and define measurable objectives in any bill that creates, renews, or continues a tax expenditure enacted after July 1, 2010. Washington requires any bill proposing a new tax incentive to include a performance statement indicating the incentive's legislative purpose.

DLS assumes the intent of the tax credit is, as the Department of Commerce (Commerce) states on its website, to promote the cybersecurity industry in Maryland by helping small businesses purchase cybersecurity technologies and services from Maryland cybersecurity companies to protect business information. In this chapter, DLS will examine how the Purchase Cybersecurity Tax Credit Program is meeting its objectives of (1) helping small businesses purchase cybersecurity technologies and services and (2) promoting the cybersecurity industry in Maryland and will discuss whether these goals could be more effectively carried out by other means.

## How Is the Program Meeting Its Objective of Helping Small Businesses Purchase Cybersecurity Technologies and Services?

### Program Is Underutilized

One of the assumed goals of the Purchase Cybersecurity Tax Credit Program is to help small businesses purchase cybersecurity technologies and services. Since 2018, 86 small businesses have been awarded the purchase cybersecurity tax credit. A business must have fewer than 50 employees in the State to be a qualified buyer. According to the U.S. Census Bureau, there are over 100,000 firms in Maryland with fewer than 50 employees. Thus, less than 0.1% of small businesses are participating in the program, which suggests that the program is underutilized.

There are many possible reasons for the program being underutilized. Small businesses may believe that they do not need cybersecurity technologies or services. In a recent survey of business owners, only 37% of small business owners reported believing that they are at risk of falling victim to a cyberattack, despite nearly half of cyberattacks being aimed at small businesses. Even though the tax credit is generous at 50% of the cost incurred to purchase cybersecurity technologies or services, businesses may not be willing to incur these costs if they believe there is no need to do so. According to the *2021 U.S. Small Business Recovery and Technology Report*, 10% of small business owners responded "Not at all" when asked how much of a concern cybersecurity is for their business. The percentage of small business owners that answered "very" dropped from 62% in 2019 to 42% in 2021, which the report attributes to growing concerns over economic slowdowns and trying to keep business afloat. The survey states, "Unfortunately, the decrease among small business owners who said they are 'very concerned' about cybersecurity does not correlate with any kind of easing-up in cyberattacks, highlighting a disconnect between perceived risk and the very real threat of a cyberattack".

While some small businesses may not perceive cybersecurity technologies or services as necessary, others may believe that even with the tax credit, cybersecurity technologies or services are too expensive. When asked about the underutilization of the Purchase Cybersecurity Tax Credit Program, Commerce cited small businesses having less buying power than larger businesses such that even with the credit, they may not have the ability to make those purchases. Additionally, McKinsey & Company claims many cyber solutions are mispriced for small and midsize businesses (SMB). McKinsey & Company state "Larger organizations can pre-pay or buy in bulk to obtain volume discounts, but many SMBs and midmarket companies are less able to negotiate hard for these services." McKinsey & Company go on to say, "SMBs and midmarket companies have a smaller base of employees over which to spread cyber-tooling costs, so they face a decision: either pay a disproportionate price per employee—by a factor of three to five or more than larger companies do, depending on the tooling category—or forego some security controls entirely." Thus, some small businesses forego cybersecurity tools.

Regardless of whether it is by choice or necessity, nearly half of small business owners handle company tech support themselves, according to the *2021 U.S. Small Business Recovery and Technology Report*. The same report finds that "Fewer small-business owners today say they have a high understanding of cybersecurity issues than two years ago" and "Just one-in-three small businesses have completed a technology audit, meaning most small businesses are missing a critical piece in their overall technology operations." Thus, small businesses may not even be aware of their vulnerabilities to cyberattacks.

Additionally, some small businesses may not be participating in the program because they do not have a tax liability. The Purchase Cybersecurity Tax Credit Program provides a nonrefundable tax credit so a small business must have a tax liability to benefit from the program. Another possibility is that small businesses are choosing to secure their cybersecurity needs from cybersecurity businesses that are not qualified sellers.

### Cyberattack Risks Vary by Industry

The purchase cybersecurity tax credit provides a tax credit for any small business regardless of its industry or risk level. However, cybersecurity risks tend to vary by industry. According to a study by the International Business Management Services, in its 2023 report, the healthcare industry has the highest average data breach cost of all industries at $10.9 million, followed by the financial industry at $5.9 million. While the healthcare and financial industries have the highest average cost of a data breach, manufacturing is the industry most commonly targeted by cybercriminals. Cybercriminals have been targeting manufacturers more frequently due to potential vulnerabilities of smart factories. According to Deloitte, many manufacturing companies are seeing an increase in cyber-related incidents associated with the control systems used to manage industrial operations. The failure of the purchase cybersecurity tax credit to target industries with high cyber-related incidents or breach costs may contribute to program inefficiencies.

## How Is the Program Meeting Its Objective of Promoting the Cybersecurity Industry in Maryland?

The other assumed goal of the Purchase Cybersecurity Tax Credit Program is to promote the cybersecurity industry in Maryland through increasing sales. Commerce's fiscal 2022 annual report states, "As the purpose of this program is to build local supply chains in the cybersecurity industry and to support Maryland-based cybersecurity firms, any assistance rendered through it to any Maryland business counts as a successful outcome." However, the Lawrence J. Hogan, Jr. Administration discussed in its testimony of support of the purchase cybersecurity legislation that investors look at a company's sales when making investment decisions and that this legislation would enable cybersecurity innovators to turn sales into investments at 8 to 10 times their value. Commerce could use a more analytical approach when defining success, such as measuring sellers' sales and investments. Analyzing that information could be useful in determining whether the program is meeting its objective of promoting cybersecurity firms in Maryland.

Several cybersecurity firms have appeared to benefit from the Purchase Cybersecurity Tax Credit Program. For example, almost half of all awarded tax credits have been for cybersecurity technologies or services for Epoch, Inc, totaling $1.0 million. Epoch, Inc. ranked fifty-third on the 2023 Channel Futures MSP 501 list, which examines organizational performance based on annual sales, recurring revenue, profit margins, revenue mix, growth, innovation, and supported technologies, and has improved on its rankings over the past three years. Despite Epoch, Inc.'s success, DLS questions how much of its success, if any, is attributable to the purchase cybersecurity tax credit.

Even if Maryland cybersecurity firms are experiencing an increase in sales, it may not be due to the Purchase Cybersecurity Tax Credit Program. Commerce noted that when businesses are unable to receive the tax credit due to the seller reaching the $200,000 seller cap, businesses typically continue to purchase the cybersecurity technology or service due to the business signing

a contract with the seller. It is difficult to estimate how much cybersecurity technologies and services would have been purchased in the absence of the tax credit.

Most tax incentives are designed to maximize their effectiveness by promoting economic activity that would not have otherwise occurred in the absence of the incentive. An effective tax credit program avoids providing windfalls – awarding tax credits for activity that businesses would have done anyway – by focusing as much of the benefit on increasing marginal spending rather than total or recent spending. The design of the Purchase Cybersecurity Tax Credit Program is likely to provide windfall credits for activities that would have occurred in the absence of the tax credit since it is based on a business's total recent expenditures rather than for incremental increases. Some businesses sign service contracts with sellers, so they are committed to purchasing the cybersecurity service regardless of whether they receive the tax credit.

## Alternative Ways to Protect Small Business Information and Promote Cybersecurity

### Cybersecurity Insurance

Cyber insurance is one option that businesses can pursue to protect against losses resulting from a cyberattack. A recent report by DLS examined cybersecurity insurance. With cyberattacks increasing in frequency and severity in recent years, companies have been obtaining cyber insurance to offset the costs that are incurred when, in the wake of attacks, the companies' operations go offline, and cyber ransoms are paid.

Standalone cyber insurance policies arose because traditional insurance policies (*e.g.*, commercial general liability, professional liability, errors and omissions, directors and officers, and kidnap and ransom) typically did not cover cyber risks expressly. Given the uncertainty as to whether damage from cyberattacks would fall under the coverage terms of more traditional plans, some insurers started to modify those policies to explicitly exclude cyber risks from traditional coverage. Standalone cyber policies thus developed to cover losses from data breaches, ransomware attacks, theft of unencrypted assets, insider threats, denial of service attacks, supply chain cyberattacks, phishing scams, exploitation of cloud misconfigurations, cybersecurity litigation, investigations, and business interruption coverage for network downtime, etc. According to one business report, the cost of business interruption and post-incident recovery costs make up more than half of the value of cyber insurance claims.

Cyber insurance typically covers first-party losses (*e.g.*, losses the insured party incurs directly from an incident, such as data retrieval and restoration, ransomware payments, breach notification, credit monitoring, public relations fees to handle reputational fallout), and third-party losses that arise from liability to others (*e.g.*, litigation, regulatory fines, or indemnification of clients). In general, cyber insurance policies are highly variable and tailored to the covered party. For example, particular policies may not cover the costs of future lost profits, personal injury, or physical property damage related to the incident. If a policy excludes losses arising from "acts of

war or terrorism," it could be an open question as to whether the coverage will apply if the cybercriminal was acting with the tacit support of a foreign power such as Russia or China.

A policy's cost is based on a number of risk-related factors, such as the covered entity's size and annual revenue, the type and sensitivity of data handled, and the overall security of the entity's network (*i.e.*, security measures already in place, incident response plans, network preparedness, and employee training). Insurance policies are often reassessed every year, and – especially given the recent increase in risks and payouts – premiums may increase, terms and conditions may be adjusted, and some insurers may reduce future payouts.

The increasing frequency and severity of claims – along with the ongoing, uncertain, and evolving nature of the threat posed by cyber criminals – is causing cyber insurance to become more expensive. According to the National Association of Insurance Commissioners, cyber insurance premiums have more than doubled since calendar 2015, totaling $3.2 billion in calendar 2020. The average paid loss for a cyber claim increased in 2020 to $358,000, from $145,000 in calendar 2019; the second quarter of 2021 saw cyber insurance rates increase 56%. However, coverage may still outweigh the cost of being uninsured. According to a 2018 study, 60% of small businesses close within six months of a cyberattack.

Additionally, given the increasing scale of cyber risks and the increased cost of payouts, insurance companies are tightening standards and asking tougher questions during the underwriting process, inquiring about entities' networks, and requiring entities to take proactive and preventive measures before a policy is approved. As such, in addition to the other regulatory efforts that may be pursued at the federal and State level, precautionary measures that are being imposed by insurers as part of the underwriting process may contribute to companies shoring up their networks and thereby raise the overall resiliency and strength of the cybersecurity environment.

### Cyber Maryland Program

Chapter 578 of 2023 established a Cyber Maryland Program in the Maryland Technology Development Corporation to create a talent pipeline in cybersecurity, serve as a hub for State workforce development programs in cybersecurity, and generally coordinate cybersecurity and research and innovation in the State, among other things. The purposes of the Cyber Maryland Program are to:

- create and execute a talent pipeline that materially reduces workforce vacancies by July 1, 2026;
- serve as a one-stop shop for employers seeking to leverage cyber workforce development programs offered by the State and its partners;
- inform cybersecurity training and education programs operated by public or private entities with industry-driven needs;

- build the most advanced local and State information technology workforce in the nation, which, to the maximum extent possible, reflects the racial, gender, ethnic, and geographic diversity of the State;

- coordinate and accelerate cybersecurity research and innovation in the State; and

- support the efforts of the Department of Information Technology to improve the State government's cybersecurity posture, including State agencies, local government units, and critical infrastructure.

The program must conduct ongoing research by collaborating with specified entities to collect and analyze real-time industry data to identify cybersecurity workforce needs as described in the U.S. Chamber of Commerce Talent Pipeline Management Approach. The program must use the results of its research to (1) increase the effectiveness of existing State cybersecurity workforce programs for employers in the State; (2) facilitate partnerships for new training and education programs to address the workforce needs identified in the program's research; and (3) develop a statewide strategic plan for cybersecurity workforce development.

Small cybersecurity companies, or small businesses that have a need for cybersecurity services, may benefit from the Cyber Maryland Program from increased coordination by State entities regarding cybersecurity workforce development and from a potentially larger cybersecurity workforce. Small businesses may also benefit from the expansion of the Maryland Department of Labor program. The program may bolster a more skilled and prepared cybersecurity workforce to meet the staffing demands of small businesses. Finally, small businesses may benefit from any additional funding received for cybersecurity programs as part of a grant from the program fund.

# Chapter 6. Findings and Recommendations

Based on the information and analysis provided in this report, the Department of Legislative Services (DLS) recommends changes to improve the Purchase of Cybersecurity Technology or Services (Purchase Cybersecurity) Tax Credit Program, as discussed further.

## The Credit Appears to Be Underutilized

Activity level for the tax credit has been low. Since 2018, 86 small businesses have been awarded the purchase cybersecurity tax credit. A business must have fewer than 50 employees in the State to be a qualified buyer. According to the U.S. Census Bureau, there are over 100,000 firms in Maryland with fewer than 50 employees. Thus, less than 0.1% of small businesses are participating in the program, which suggests that the program is underutilized. Theories for why the tax credit has been underutilized include (1) small businesses do not view cybersecurity as necessary for their business; (2) cybersecurity is still too expensive even with the tax credit; (3) small businesses may not be aware of the credit; and (4) the credit is nonrefundable, so there is no benefit for businesses without an income tax liability.

**Recommendation:** DLS recommends that the General Assembly should consider terminating the Purchase Cybersecurity Tax Credit Program and instead explore other options, such as grants, to improve cybersecurity in the State for small businesses.

If the General Assembly decides not to eliminate the Purchase Cybersecurity Tax Credit Program, DLS has several recommendations to improve the credit that are discussed below.

**Recommendation:** The Department of Commerce (Commerce) and the Comptroller should increase efforts to advertise the tax credit to raise awareness of the program. For example, the Comptroller should list the purchase cybersecurity tax credit on its website where it advertises other business tax credits.

## The Legislative Intent and Performance Metrics of the Credit Are Not Defined

Chapter 578 of 2018 established the tax credit but did not specify a specific goal or intent for the credit. Without clearly defined goals and objectives, it is difficult to identify metrics and data requirements to evaluate the effectiveness of the tax credit. The Tax Expenditure Evaluation Act requires DLS to evaluate whether the original intent of the tax credit is still appropriate; however, there is no statutory requirement for tax credits to include an intent.

Without clearly defined goals of the program, it is difficult to critically measure the program's success. Instead of critically analyzing the program, Commerce's fiscal 2022 annual

report states, "As the purpose of this program is to build local supply chains in the cybersecurity industry and to support Maryland-based cybersecurity firms, any assistance rendered through it to any Maryland business counts as a successful outcome."

**Recommendation:** The General Assembly should clearly define the intent of the Purchase Cybersecurity Tax Credit Program in statute and consider requiring the intent of any new tax incentive to be clearly expressed.

**Recommendation:** Commerce should define performance metrics for the tax credit program and periodically evaluate the program based on those metrics.

## One Company Has Overclaimed Credits

Commerce may not certify purchases from a single cybersecurity company that total more than $200,000 in a tax year. However, for tax year 2019, the aggregate credits claimed for cybersecurity technology or cybersecurity services purchased from the seller company Epoch, Inc. exceeded the statutory cap of $200,000. DLS noted inconsistencies in data provided by Commerce and questions whether there are adequate controls over the issuance of purchase cybersecurity tax credits.

**Recommendation:** Commerce should report to the General Assembly on the safeguards in place to prevent companies from overclaiming credits.

## Requirements of the Program Add Unnecessary Complexity

Statute requires Commerce to award 25% of the authorized tax credits to qualified buyers that purchase cybersecurity services. This requirement adds a layer of unnecessary complexity, and it is unclear why it matters whether a business buys a service versus a technology.

**Recommendation:** The General Assembly should eliminate the statutory requirement that Commerce award 25% of authorized tax credits to qualified buyers that purchase cybersecurity services.

## Incremental Credits Are Preferred for Incentivizing Growth

Most tax incentives are designed to maximize their effectiveness by promoting economic activity that would not have otherwise occurred in the absence of the incentive. An effective tax credit program avoids providing windfalls – awarding tax credits for activity that businesses would have done anyway – by focusing as much of the benefit on increasing marginal spending rather than total or recent spending. The design of the Purchase Cybersecurity Tax Credit Program is likely to provide windfall credits for activities that would have occurred in the absence of the

tax credit due to it being based on a business's total recent expenditures rather than for incremental increases.

**Recommendation:** The General Assembly should consider options to redesign the credit to prioritize new spending in cybersecurity.

## Businesses Are Not Required to Add Back Credits

Statute requires businesses claiming certain business income tax credits to add back to their income the amount of that credit claimed. Doing so helps local governments because local government revenues will increase minimally due to taxpayers adding back the amount of credit claimed against the personal income tax. Statute does not require a business to add back to its income the amount of purchase cybersecurity tax credit claimed.

**Recommendation:** The General Assembly should consider requiring businesses to add back to their income the amount of the purchase cybersecurity credit claimed.

## Cyberattack Risks Vary by Industry

The purchase cybersecurity tax credit provides a tax credit for any small business regardless of its industry or risk level. However, cybersecurity risks tend to vary by industry. According to a 2023 report by the International Business Management Services, the healthcare industry has the highest average data breach cost of all industries at $10.9 million, followed by the financial industry at $5.9 million. While the healthcare and financial industries have the highest average cost of a data breach, manufacturing is the industry most commonly targeted by cybercriminals. Cybercriminals have been targeting manufacturers more frequently due to potential vulnerabilities of smart factories.

**Recommendation:** The General Assembly should consider providing enhanced credits for industries most at risk of cyberattacks.

## Commerce Has Not Established an Expert Panel

Commerce, in consultation with the Maryland Technology Development Corporation, may establish a panel composed of experts in the areas of cybersecurity technology and services in order to assist Commerce in determining if a cybersecurity business meets the requirements for a qualified seller. As of July 2023, Commerce has not elected to establish this panel.

**Recommendation:** Commerce should report to the General Assembly on why it has not elected to establish this panel. If their answer is insufficient, the General Assembly should consider requiring instead of authorizing Commerce to establish a panel. Otherwise, DLS recommends eliminating the panel in statute.

# Appendix 1. Total Purchase Cybersecurity Tax Credits Certified

**Calendar 2018-2023**

| Certification Year | Sellers | Buyers | Total Credits | Average Credits |
|---|---|---|---|---|
| 2018 | 8 | 22 | $235,324 | $10,697 |
| 2019 | 13 | 33 | 439,768 | 13,326 |
| 2020 | 12 | 34 | 421,209 | 12,388 |
| 2021 | 13 | 43 | 438,671 | 10,202 |
| 2022 | 9 | 40 | 476,931 | 11,923 |
| 2023 | 2 | 9 | 64,999 | 7,222 |

Note: Calendar 2023 reflects through June 28, 2023.

Source: Department of Commerce