**New York State Department of Taxation and Finance**
**Office of Counsel**

TSB-A-24(12)S
Sales Tax
July 30, 2024

STATE OF NEW YORK
COMMISSIONER OF TAXATION AND FINANCE

ADVISORY OPINION

The Department of Taxation and Finance received a Petition for Advisory Opinion from [redacted] (Petitioner). Petitioner asks whether sales of two of its service offerings in New York State – network security monitoring services ("NSMS") and professional advisory services ("PAS") – are subject to New York State and local sales tax. We conclude that both services are protective services subject to New York State and local sales tax.

## Facts

Petitioner describes itself as a "Managed Detection and Response (MDR) service provider" that works with mid-sized financial institutions, healthcare facilities, and various other public and private institutions and entities. MDR is described on Petitioner's website as "an all-encompassing cybersecurity service used to detect and respond to cyber attacks." Petitioner indicates that it has two main service offerings: (1) NSMS and (2) PAS.

NSMS is a subscription-based service that detects, provides alerts regarding, and prevents cyber attacks on network-connected assets. If cyber attacks on network-connected assets are detected, Petitioner provides "advisor incident advice" to customers, and works with them to resolve issues and repair any deficiencies that exist. No software is downloaded or installed by customers as part of NSMS. Rather, NSMS works via the installation of a control box, or a sensor, on customers' servers that cannot be altered or otherwise influenced by them. When these sensors detect an abnormality, Petitioner will alert its customer and work with them to address the issue. NSMS has the following components:

> C1 - Described on Petitioner's website as the "primary sensor for [its] Managed Detection and Response," C1 is a "tool to provide operational information as to the functioning of a customer's [information technology] assets." C1 provides real-time threat detection and prevention, an ability to identify unknown cyber threats, and investigation and identification of threats by a team of analysts. C1 is available for purchase by itself, or in conjunction with PAS and/or the components discussed below.
>
> C2 - C2 works with C1 to provide "core network containment capabilities." C2 is a remediation service that assists with the containment of threats within the core of a customer's network. C2 is slated to be discontinued by Petitioner, as its functionality overlaps with C3, discussed below. C2 is ancillary to, and cannot be purchased separately from, C1.

C3 - C3 captures and monitors all endpoint activity, helps detect cyberattacks, hunts for both known and unknown threats, and prevents attacks from spreading. This is done via the provision of 24/7 monitoring for the detection, isolation and response to threats, and the ability to lock down and isolate compromised endpoints. C3 is only available for purchase in conjunction with C1.

C4: C4 collects, centralizes and correlates event data from any network-attached asset. C4 also allows Petitioner to monitor end-user and critical business applications in real time for suspicious use and behavior, and provides alerts regarding suspicious activities and anomalies. In addition, Petitioner's website notes that C4 offers "customizable security visuals," "out-of-the-box" and custom security reports, and provides the ability to run advanced search queries, generate alerts, manage profiles, and investigate events alongside Petitioner's analysts. C4 is ancillary to, and cannot be purchased separately from, C1.

C5: C5 is a feature that scans for vulnerabilities across a customer's infrastructure and assets. It provides notifications and reporting to minimize the risk of breach, and provides customers with advice and support to remediate critical vulnerabilities. C5 is available for purchase by itself (i.e., as a stand-alone service), and is an on-going service that, like the rest of NSMS, is offered on a subscription basis.

Petitioner's other service offering, PAS, provides "customized services, including the creation, oversight and implementation of formal cybersecurity policies and procedures for its customers." This includes consultation on how customers can lower their exposures to threats, as well as the development of cybersecurity programs that are tailored to their unique needs. Once in place, these programs are continually assessed by Petitioner to ensure their maturity and success. Information gained from NSMS's tools form the basis of PAS. Without this information, Petitioner indicates that PAS's deliverable would "be more speculation," and that the service provided would have "much more limited usefulness." Petitioner, in fact, advises that none of its customers merely purchase PAS by itself.

**Analysis**

Tax Law § 1105(c)(8) imposes sales and use tax on sales, other than sales for resale, of protective services provided by "protective systems of every nature." *See also Robert Bruce McLane Assoc. v. Urbach*, 232 AD2d 826 (2d Dept. 1995). This includes services that are designed to prevent unauthorized access to or use of a customer's information technology (IT) assets located in New York State. *See* TSB-A-15(47)S; TSB-A-10(14)(S). This also includes the service of monitoring for unauthorized access to or the use of IT assets. *See* TSB-A-15(47)S. Generally, the sales tax status of a service depends on its primary function. *See id*. *See, also e.g., Matter of SSOV '81 Ltd. d/b/a People Resources*, Tax Appeals Tribunal, January 19, 1995 (in order to determine a service's taxability, the analysis employed . . . focuses on the service in its entirety, as opposed to reviewing the service by components or by the means in which the service is effectuated).

Petitioner is an MDR service provider, which is "an all-encompassing cybersecurity service used to detect and respond to cyber-attacks." One of its offerings, NSMS, is a subscription-based service that detects, provides alerts regarding, and prevents cyber-attacks on network-connected assets. This offering has five components. C1 provides information as to the functioning of a customer's IT assets, as well as "real-time threat detection and prevention, an ability to identify unknown cyber threats, and investigation and identification of threats by a team of analysts." C2 continually assists with the containment of threats that are identified within the core of a customer's network, while C3 captures and monitors all endpoint activity, helps detect cyber-attacks, hunts for both known and unknown threats, and prevents attacks from spreading. C4 collects, centralizes and correlates event data from any network-attached assets, and allows Petitioner to monitor end-user and critical business applications in real time for suspicious use and behavior. C4 also gives customers the ability to run searches, generate alerts, and investigate events. Lastly, C5 scans for vulnerabilities across a customer's infrastructure and assets, and provides notifications and reporting to minimize the risk of breach. The primary purpose of each of these components is to monitor, protect and/or secure customers' IT assets from cyber-attacks on an ongoing basis, which is the very essence of a protective service. We therefore find that NSMS is protective service, and that its sale (and the sale of any of its components) is subject to New York State and local sales tax.

Likewise, we find that PAS also is a taxable protective service. Specifically, PAS provides "customized services, including the creation, oversight and implementation of formal cybersecurity policies and procedures for its customers." Although petitioner describes PAS in its petition as an "advisory" or "consulting service," the provision of which may not subject to State and local sales tax (*See, e.g.*, TSB-A-15[16]S; TSB-A-92[31]S), PAS is broader than that. In addition to consultation on how customers can lower their exposures of threats, for example, PAS also includes the development of cybersecurity programs, as well as their ongoing assessment. PAS, therefore, more accurately is described as a protective service, the sale of which is subject to New York State and local sales tax. *See, e.g.,* TSB-A-15(16)S (service provided on an ongoing basis to regularly monitor a customer's business to identify ways to reduce fraud qualifies as a protective service even if the charge is denominated as "counseling"). This is especially true where, as here, PAS has "limited usefulness" by itself, and generally is not purchased without NSMS.

Finally, protective services are provided in New York (i.e., "sourced" to New York) if the property being protected is in New York. *See New York State Sales and Use Tax on Protective and Detective Services,* N-90-20; TSB-A-16(20)S. Thus, to the extent that assets or data being protected are in New York (e.g., are in New York, reside on servers in New York, etc.), then Petitioner is providing a protective service in New York. If protected assets and/or data are located both inside New York and outside the State, Petitioner should collect tax only with respect to the services that protect the assets and/or data located in New York. In determining where its protective services are being provided, Petitioner may rely on a letter from the customer indicating the taxing jurisdiction or jurisdictions where the protected assets and/or data are located, absent a showing of fraud or knowledge on the part of Petitioner that the contents of the letter are untrue. Such a letter must be signed by the customer (or the appropriate employee or officer thereof) and contain a statement acknowledging that it is being furnished to allow Petitioner to determine the appropriate amount of New York State and local sales and use tax

due. Petitioner must keep the letters furnished by its customers as part of its sales tax records, and be able to associate each letter with related sales, for at least three years after the date of the last sale to which the letter relates. The customer is required to update the letter if there is a change in where the services are being provided. To continue to rely on the letter, Petitioner should regularly review with its customer the information contained in the letter to ensure that the information is still accurate, no less frequently than every three years.

DATED: July 30, 2024

/s/
MARY ELLEN LADOUCEUR
Principal Attorney

NOTE: An Advisory Opinion is issued at the request of a person or entity. It is limited to the facts set forth therein and is binding on the Department only with respect to the person or entity to whom it is issued and only if the person or entity fully and accurately describes all relevant facts. An Advisory Opinion is based on the law, regulations, and Department policies in effect as of the date the Opinion is issued or for the specific time period at issue in the Opinion. The information provided in this document does not cover every situation and is not intended to replace the law or change its meaning.