Data Transfer to the United States: Frequently Asked Questions

1. Has LogicMonitor, Inc. ("LogicMonitor") ever received a request for information pursuant to U.S. Intelligence Authorities?

We understand that based on a review of records over the past five years, LogicMonitor in the United States have not identified any such request.

2. Why would the U.S. government be interested in LogicMonitor's information?

It would not be. The U.S. government is primarily interested in information that relates to the ability of the United States to defend itself against an actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. LogicMonitor is highly unlikely to possess any of these types of information because of the types of customers we service (legitimate, and often large, publicly-traded, and/or highly regulated corporations, including without limitation, managed service providers, and resellers), the types of services it provides (technology systems instrumentation and observability), and the types of personal data it processes (ordinary commercial information like employee, customer, and sales records).

Unlike internet service providers or providers of email, telecommunications, social media, or similar accounts to the public, organizations like LogicMonitor are not traditionally the focus of U.S. surveillance laws.

3. Is LogicMonitor likely to receive a directive for information pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA)?

No. The communications sent or received via LogicMonitor's internal communication systems and the information stored on its servers, both of which could potentially be within the purview of Section 702, would be unlikely to contain the foreign intelligence information of interest to the U.S. government. Due to the nature of LogicMonitor's business, communications between LogicMonitor and its international subsidiaries or non-U.S. persons (such as clients) are unlikely to be targeted as sources of the foreign intelligence information the U.S. government seeks (i.e., evidence about terrorism, weapons proliferation, malicious cyber actors, etc.)

4. Is LogicMonitor likely to receive a surveillance request pursuant to Executive Order 12,333 (EO 12,333)?

No. EO 12,333 addresses the U.S. government's foreign intelligence collection techniques conducted outside the United States. It provides the basis for certain intelligence surveillance activities beyond the activities regulated by FISA. EO 12,333 does not authorize the collection of

communications on U.S. soil and does not require private entities to comply with surveillance requests.

5. Is LogicMonitor U.S. likely to receive a national security letter pursuant to the USA Patriot Act?

No. LogicMonitor U.S. does not typically maintain the information sought by national security letters, such as personal telephone and email records, financial records, and credit information.

6. Does LogicMonitor have any technical protections in place to mitigate the potential risk of requests for information pursuant to U.S. Intelligence Authorities?

Yes. LogicMonitor's policy is to ensure that all customer data transmitted across public networks is encrypted, which helps to mitigate the risk that the U.S. government could successfully leverage an electronic communication service provider or remote computing service to surveil LogicMonitor's customers' data while in-transit and obtain LogicMonitor U.S. data, such as under Section 702 or pursuant to a national security letter.