CloudCover™

2999 County Road 42W - #200
Burnsville, MN 55306-6995
Fax 877-532-0390

November 25, 2013

To: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

From: Stephen Cardot
Chief Executive Officer
CloudCover, Ltd.
2999 County Road 42 West, Ste 200
Burnsville, MN 55306

Re: Framework Adoption: Flexible Specificity Rule

Dear Mr. Sedgewick,

This year has presented the unusual assortment of data security revelations, both common and unforeseen cyber risk activity, as well as questionable compliance challenges. There is no reason to expect different in 2014.

The President stated in his Executive Order; I may paraphrase: "cyber security risks facing our country's infrastructure is the most challenging security concern, as a nation…" And as a result, the U.S. federal government took action by initiating the Cybersecurity Framework (CS Framework).

A primary challenge to the CS Framework remains toward adoption. On the surface, commercial participant's adoption attitude is annoyance and confusion. Even though the responsibility of security guidance is bestowed upon this CS Framework, we should remind ourselves that cyber security *must* be addressed on an industry basis — due to the fact that data privacy compliance is mandated on an industry-by-industry basis here in the U.S. and the EU. One must also understand that cyber security of personal identifiable information inherits distinctive data privacy challenges specific to critical sectors, e.g. finance, healthcare and government.

Today's corporate leaders face multiple challenges, including the need to innovate in extremely competitive business climates, address highly dynamic regulatory and compliance challenges both here and abroad, and secure the enterprise against a wide barrage of new and evolving sophisticated cyber threats. Successful U.S. organizations are beginning to understand a greater percentage of their cyber risk at a deeper, more data risk centric level. These companies require more flexible, adaptable cyber risk tools on a more customizable data risk management, industry basis.

That said, no industry, nor sector in the United States can ever say with complete certainty that they know all the risks that impact their first and third-party cyber risk obligations due to regulatory compliance. Company's ability to respond to unknown cyber threats is more and more dependent on next generation cyber securing technologies. To apply the Framework's current guidance principles may not only be an obstacle to adoption, but its practice recommendations may be ignored, if it cannot address the specific needs of specific industry's data risks.

The issue of cyber security or data risk is serious enough that in early 2012 the European Union (EU) published an opinion paper noting that "the wide-scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal identifiable information (PII) as well as insufficient information with regard to how, where, and by whom the data is being processed or subjected to handling risks." Data privacy and security is not simply a U.S. cyber security challenge, it is a global concern. Data risk actually has no boundaries, even though some would like us to believe so.

In order for an organization to adhere to new data privacy demands, businesses require robust information security solutions that deliver adaptable protections across any security domain within their network. Active compliance to regulatory standards across jurisdictional domains within cloud computing also must adhere to the new data privacy policy protections demanded in Europe, which also dramatically effects global commerce. This policy toward cloud computing is driving more specific and more flexible risk mitigation protocols and functionality.

To be even modestly compliant on both sides of the pond, organizations employing cloud-computing solutions are becoming more sensitive to data security and risk, as exhibited in their demand for more risk articulation in the lackluster service level agreements. Cloud-computing solutions must adapt their cyber security with respect toward data privacy compliance; otherwise they shall be left behind.

Simply put, governments, regulatory bodies, and consumers are concerned about data privacy and what steps organizations should take to actively protect the security of their PII data. They do not want to learn after the data breach, that their data was victim to loss or theft. Those days must end! Data risk compliance for the sake of privacy, including the most aggressive privacy mandates are driving new corporate risk management strategies toward real time risk mitigation models that shall become the new cyber security common "denominator" or as we say here in the Midwest — the really new normal.

To be given a betting chance for successful adoption, the CS Framework therefore needs to be more flexible yet modular. The successful rollout of the CS Framework must integrate adaptable cyber security guidance principles by employing data risk mitigation illustrating industry example. Industry adaptation will reinforce viral adoption.

As we all know, things do change. And, so shall the Framework. The Framework will become more like a living document, rather than a "cut-in-granite" one-stop cyber solution.

History has shown that flexibility and specificity illustrated by useful relative example, is most practical when successfully introducing anything new and important.

Respectfully,

Stephen C. Cardot
Chief Executive Officer
CloudCover