CloudCover™

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

November 22, 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: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick,

During the comment timeframe, CloudCover, Ltd. shall provide further comment on the topics identified below and offer further insight into why, what, and how these topics may be integrated into the Framework as to improve the acceptance by private U.S. business sectors, as well as further adoption in the cyber security industry.

1) Outcome-focused Performance Goals (OFPG) — Outcome-based methods are used in most U.S. businesses. For whole companies, outcome-based evaluations are the basis of stock exchange prices: Companies, which produce higher profit growth, are more valuable than companies, which perform poorly. Employees who are paid for piecework or by commission are examples of traditional employment use of outcome-based pay. Alternatives include seniority systems (oldest worker gets highest pay). Many private employers give standards-based tests to determine whether job applicants have necessary job skills (such as typing speed), and nearly all government employees have to take and pass a civil service examination. Furthermore, nearly all licensed professionals, from nurses to truck drivers to beauticians, already take such tests as a condition of entering their professions.

With that recognition, the following questions come to the surface concerning integrating outcomes-focused performance goals (OFPG) into the Framework:

- How receptive is industry to outcomes-focused performance goals in the cyber security domain?
- Would it make more sense if industry itself developed such OFPG -- on a sector-by-sector basis – rather than government?
- How else might a conversation about OFPG be fostered across the private sector?
- What incentives -- on a sector-by-sector basis -- would most likely encourage a company to try to attain a particular OFPG?
- How would industry propose to certify a company's reported attainment of a particular OFPG? What does the OFPG certification measure or look like?

2) Sustainability — Sustainability* science is not yet an autonomous field or discipline of its own, and has tended to be problem-driven and oriented towards guiding decision-making and measurement. Cyber Sustainable Security is a term that denotes cyber security as on-going requirement for sustainable operations and is measured on the

quantitative basis for the informed real time management of sustaining cyber security. The metrics used for the measurement of cyber sustainability (involving the sustainability of information technology systems, real time business and compliance domains, both individually and in various combinations) are evolving: they include indicators, benchmarks, audits, sustainability standards and certification systems like indexes and accounting, as well as cyber risk assessment, appraisal and other reporting systems. Sustainable cyber business practices, on the other hand, integrate cyber security concerns with people, economic metrics and data governance.

3) Data Governance — Data governance* (in terms of cyber security) encompasses people, processes, and information technology required to create a consistent and proper handling of an organization's data security posture and the risk handling of data across the business enterprise. Data governance initiatives improve data security and quality of cyber security adoption by assigning a team responsible for data's security, accuracy, accessibility, consistency, and completeness, among other outcome-focus performance metrics.

> * Governance, Risk Management, Compliance — GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness. Information systems will address these matters better if the requirements for governance, risk and compliance management are incorporated at the design stage, as part of a coherent Cybersecurity Framework.

4) Compliance Automation — Standards and compliance are all about implementing policies, procedures and technologies that reduce business risk, as well as being able to efficiently validate that controls are working according to stated policy expectations and mandated requisites. Beyond setting policy and procedures, many tools in its management portfolio must support compliance efforts. The question then becomes finding the right solution that best automate control verification and documentation, as well as streamline internal and external audit challenge/response processes. Compliance considerations for information technology management and cyber security should include the means to:

- Validate a broad set of policies across technologies
- Deliver on-demand results to auditor inquiries
- Readily obtain applicable data and documentation
- Normalize compliance-relevant data across disparate systems
- Diminish compliance liabilities and audit duration
- Meet auditing and data management standards
- Identify control gaps and prioritize incident response
- Adapt to existing security, governance and auditing processes
- Respond to complex and rapidly changing environments

Please consider the Preliminary Cybersecurity Framework comments as outlined. We shall follow up over the next few weeks with individual references to the comments provided. Thank you, for your review.

Respectfully,

Stephen Cardot
CEO, CloudCover