April 26, 2013

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW.
Room 4725
Washington, DC 20230

cyberincentives@ntia.doc.gov

RE: Incentives to Adopt Improved Cybersecurity Practices

Monsanto appreciates the opportunity to provide comments to the Department of Commerce on the issue of Cybersecurity practices and how the private sector can be better incentivized to adopt cybersecurity "best practices" that will be established by the National Institute of Standards and Technology.

Monsanto is a Fortune 500 company headquartered in St. Louis, Missouri. We are a high-tech, agricultural company that produces row crop and vegetable seeds, plant biotechnology traits, and crop protection chemicals. Worldwide, we employ approximately 21,000 people full time and operate in more than 66 countries. In the United States, we employ more than 10,000 people working in 146 facilities in 30 states.

We invest approximately $1.5 billion annually on research and development efforts -- more than $4 million per day – to maximize the potential of seeds and their yield output. Our scientists use both conventional breeding methods and agricultural biotechnology to develop products that have advanced agriculture and have made farming more economical, environmentally-friendly, and sustainable. We continue to expand our pipeline of innovative products to address current and anticipated challenges in agriculture, such as how to provide the food resources required when the world's population expands to about nine billion people by 2050.

As an innovative, high-tech company in a competitive industry, intellectual property and strong patent protections are our lifeblood. We also place tremendous value on our reputation with our grower customers and our employees. To that end, we place a premium on protecting our intellectual property as well as any confidential customer and employee information.

Accordingly, we have established and rigorously follow an effective set of best practices related to cybersecurity. Our dynamic program is carefully tailored to mitigate the unique cyber-threats that we face on a daily basis as a global leader in the agricultural industry. Moreover, the program has evolved over the past ten years based on extensive interaction and discussion with senior and executive internal leadership, industry peers, other Fortune 500 companies, and the

use of external consulting expertise. The program continues to evolve to meet increasing and ever-changing cyberthreats.

The federal government played no direct role in the development of our cybersecurity best practices. With regard to the establishment of a voluntary federal cybersecurity program, our concern would be that any such program would eventually become mandatory and focused upon specific countermeasures for all companies to implement rather than upon outcome-based criteria. We feel that a one-size fits all cybersecurity framework would not be the best way to protect Monsanto against the threats we face.

With regard to the conduct of additional required risk assessments and the determination of critical cyber infrastructure, we would be concerned that such activities could result in the release of confidential information about our business processes, proprietary information systems, and cybersecurity countermeasures that could be used by those who would do us harm. Monsanto would be more inclined to participate in the Critical Infrastructure Cybersecurity Program (the Program) if there were certain incentives available. Monsanto believes there are four main categories that these incentives fall under, which we have outlined below with our recommendations.

1. Protection of sensitive information: If risk assessments and analyses to determine critical cyberinfrastructure vulnerabilities are undertaken, these activities should be designed to avoid the release of sensitive information.

The Protected Critical Infrastructure Information (PCII) Program that was established by Congress as part of the passage of the Critical Infrastructure Information Act of 2002 (P.L. 107-296) could be used in developing a model for protecting sensitive information that is shared with the government to improve cybersecurity preparedness. PCII provides important protections to industry when it shares information with the Department of Homeland Security that Monsanto believes might also incentivize participation in the Program.

These protections include provisions that critical information cannot be:

- Disclosed through a Freedom of Information Act request, or through a request under a similar State, local, tribal, or territorial disclosure law.
- Disclosed in civil litigation.
- Used for regulatory purposes.

In addition, critical information can only be used:

- By a Federal, State, local, tribal, or territorial government employee or contractor who has taken PCII training;
- For homeland security purposes; and
- With a need-to-know that particular information for their official duties.

From our perspective, it is imperative that any critical infrastructure information be used only to enhance cybersecurity intelligence and preparedness. Additionally, we would want any sharing of such critical infrastructure information to be done in an anonymous fashion to ensure that corporate identity is not disclosed. Without such guarantees on anonymity, we would be unlikely to participate.

2. Sharing of technical threat indicators and periodic briefings: We are very interested in hearing more about new opportunities focused on sharing of cybersecurity intelligence between industry and the public sector. Our mutual efforts to improve cybersecurity could be greatly enhanced through increased sharing of technical threat indicators as well as periodic and timely threat briefings, both classified and unclassified.

3. Increased sponsorship of security clearances: Increased sponsorship of security clearances for companies would help facilitate timely conversations on emerging threats, and expedite and further enhance cybersecurity throughout the nation.

4. Clear scope and definition of "critical infrastructure": A clear scope and definition of critical infrastructure would present an incentive for companies to participate in the Program, as it would designate key actors and prevent industry uncertainty, which is a formidable disincentive to industry participation.

We appreciate the effort to enhance our nation's cybersecurity and believe the Program can be a mutually beneficial endeavor for both the public and private sectors under the right circumstances, including the incorporation of the aforementioned incentives for participation. Monsanto would welcome the opportunity to participate in any industry dialogue directed by the Department of Commerce on this issue.

We appreciate the opportunity to provide our comments on this important issue. Thank you very much for the opportunity to share our views.

Respectfully Submitted,

Michael D. Holland
Director of Federal Government Affairs
Monsanto