THOMSON REUTERS

August 1, 2011

U.S. Department of Commerce
Internet Policy Task Force
SecurityGreenPaper@nist.gov

RE: Comments on Cybersecurity Green Paper

Dear Sir(s):

Thomson Reuters is very pleased to provide its comments concerning the Department of Commerce's June 2011 Green Paper entitled *Cybersecurity, Innovation and the Internet Economy*. As the world's leading source of intelligent information for businesses and professionals, we leverage innovative technology to deliver critical information to leading decision makers in the financial; legal; tax and accounting; healthcare; science; and media markets. Therefore, we believe that Thomson Reuters is uniquely positioned to offer its views on pragmatic solutions aimed at strengthening the cybersecurity of organizations that rely on the Internet to do business.

First and foremost, we would like to commend the Department's Internet Policy Taskforce for recognizing the tremendous economic and social value of the Internet; for focusing on practical solutions for the U.S. Government and private sector to better protect businesses and consumers; and for promoting the Internet as an engine for economic growth, both in the United States and globally. To those ends, we trust that the Department will continue to ensure that its efforts in this space are in harmony with other cybersecurity policy initiatives currently underway at the Federal level including, but not limited to, the White House's own comprehensive cybersecurity initiative; efforts emanating from other agencies, including the U.S. Department of Homeland Security; and legislative proposals promulgated in the U.S. Congress.

Second, we are very pleased that the Department's Green Paper has given substantial deference to various existing standards, most notably existing National Institute for Standards & Technology (NIST) guidelines and the Payment Card Industry's Data Security Standard (PCI DSS), as well as more targeted standards aimed at protecting specific areas, as noted in the Green Paper. Thomson Reuters believes that the nation's cybersecurity framework does not suffer from a lack of current government-driven or industry-sponsored standards and codes. Rather, we believe that government and industry alike could benefit from new solutions to bridge better awareness of cybersecurity threats (starting at the undergraduate level) and to give more meaningful effect to existing commonly-accepted cybersecurity principles to which many organizations across a range of sectors already subscribe.

610 Opperman Drive
Eagan, MN 55123

Phone: + 1 651 687 8108
E-Mail: david.notch@thomsonreuters.com

thomsonreuters.com

It is in this context that we find the Department's proposal to facilitate the development of consensus-based codes of conduct on cybersecurity to be quite intriguing. As the Green Paper correctly notes, certain sectors, such as those comprised by primarily smaller businesses, which comprise a critical segment of our information economy, may lack the capacity to establish their own codes of conduct. However, other sectors, such as those comprised of larger and perhaps more established business "thought leaders" on cybersecurity, may already be setting the de facto "standard" in this respect. If the Department can provide constructive solutions to encouraging and enabling industry to better align all stakeholders' efforts to better protect their critical assets, and this can be accomplished in a consensus-driven and voluntary manner, then the Department's proposal in this respect appears to hold great promise. In particular, we would welcome new solutions to help smaller- and medium-sized firms to develop their own cybersecurity plans, with particular focus on:

- Best practices for asset inventory
- Security and risk management programs;
- Security controls (i.e., personnel and training, processes, technologies and physical safeguards);
- Incident management; and
- Asset recovery.

These particular solutions were part of a round table discussion in which I participated on May 16, 2011, convened by Federal Communications Commission Chairman Julius Genachowski.

Having said this, we believe that the Department's Green Paper is lacking in one important respect, i.e., how to track progress against the Department's proposed cybersecurity action items and principles. In other words, in order to help drive results, it seems as if the Department would first need to define what would constitute successful implementation of the Department's policy recommendations. Indeed, certain existing standards and frameworks, including those promulgated by industry, are periodically assessed to determine whether, for example, member organizations are giving effect to the standards. Therefore, the Department may wish to consider defining what would constitute successful implementation of its strategy, as well as the establishment of a mechanism to periodically assess its refined set of policy recommendations against actual government and business cybersecurity practices.

Finally, we appreciate the Department's desire to explore and identify incentives to encourage the adoption of voluntary cybersecurity best practices. Specifically, the Federal Government may wish to explore new solutions aimed at:

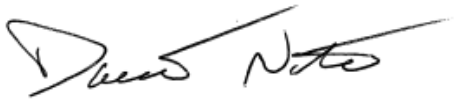
- Ensuring that the technology products and services that smaller businesses buy are secure through appropriate incentives to those developing said products and services;

- Providing research and development incentives in areas the competitive market would not normally address; and
- Fostering the proper legal framework that businesses can leverage when their systems become compromised.

However, we would like to express some concern with the concept of using security disclosures as such an incentive. While we agree that the adoption of transparency and disclosure of information practices can be a very effective and necessary tool to enable data subjects, to exercise informed decisions over the sensitive and often personally identifiable information they share online, we believe that there may be certain risks associated with the unnecessary public disclosure of detailed private and public sector cybersecurity plans and evaluations. In short, it seems that lax disclosure of potentially sensitive and proprietary cybersecurity plans could have the unintended consequence of undermining cybersecurity protection by, in effect, giving certain "bad actors" the roadmaps they would need to undermine our critical infrastructure and Internet security.

Once again, we would like to thank the Department of Commerce for its work in this very important area and for inviting the comments of key stakeholders such as Thomson Reuters.

Sincerely,



David Notch
Chief Information Security Officer
Thomson Reuters