NIST and NTIA Request Information on Cybersecurity Framework Incentives; Industry Has Significant Opportunity to Influence Regulatory Process

In the latest effort to implement President Obama's cybersecurity initiative, the National Institute of Standards and Technology ("NIST") and the National Telecommunications and Information Administration ("NTIA") have issued a request for comment as part of their joint effort to create a set of industry best practices to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework") and to incentivize its adoption. This request for comment offers industry a significant opportunity to provide input on cybersecurity policies and procedures and the impact of various incentive schemes. ***Comments are due by April 29, 2013***.

The February 12, 2013 Executive Order and the Presidential Policy Directive on cybersecurity have tasked NIST with creating the Cybersecurity Framework. When fully implemented, the Executive Order and Presidential Policy Directive could impose significant new regulatory burdens on owners of terrestrial wireless and wireline, undersea cable, and satellite networks. In the request for comment, NIST and NTIA make a series of very broad information requests intended to identify existing and potential new incentives for companies to adopt cybersecurity programs in general and the Cybersecurity Framework in particular. Specifically, NIST and NTIA request comment on the following topics:

Current Incentives, Disincentives, and Voluntary Governance Programs:

- Whether existing incentives adequately address the current risk environment and whether particular business sectors or company types lack sufficient incentives to make cybersecurity investments;
- Whether industries or groups already have voluntary governance mechanisms related to cybersecurity, whether organizations participate, and whether there are particular benefits or challenges associated with voluntary governance mechanisms;
- How businesses assess the costs and benefits of enhancing their cybersecurity and how businesses measure the success of cybersecurity programs;
- Whether existing public policies or private sector initiatives have successfully increased incentives to invest in security and whether companies find the cost of compliance with existing cybersecurity requirements burdensome relative to other costs of doing business;
- Whether disincentives currently exist that inhibit cybersecurity investments by firms.

New Incentives:

- How the U.S. government can best encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face and how the government should tailor incentives for small businesses and multinational corporations, respectively;
- Whether the U.S. government should take other actions, beyond the Cybersecurity Framework, to better promote and support the adoption of the Framework or other cybersecurity standards, practices, and guidelines;

- How incentives can help ensure that best practices and standards, once adopted, are updated in light of changing threats and new business models.

Specific Proposals:

- Whether it would be better to provide a legal safe-harbor to individuals and commercial entities that participate in the Cybersecurity Framework or to hold entities accountable for failure to exercise reasonable care in implementing security measures;
- Whether the U.S. government should require entities to participate in the Cybersecurity Framework prior to receiving government financial guarantees or assistance in relevant sectors;
- Whether liability structures and insurance can be used as incentives.

The request for comment addresses some of the key uncertainties of the Executive Order and Cybersecurity Framework. It also neglects to address a number of others, including how NIST will coordinate with the Department of Homeland Security and the U.S. Department of the Treasury—also tasked by the Executive Order to develop incentives—to design the final incentives program, and the extent to which incentives might be leveraged to make program participation all but mandatory for many providers. The request for comment provides a significant opportunity for industry to address all of these issues as it seeks to minimize regulatory burdens and uncertainties.

In addition, we recently attended the first of several NIST stakeholder workshops, at which NIST officials made clear that they view the development of the Framework as an industry-led process. The next stakeholder workshop will take place from May 29th through 31st at Carnegie Mellon University in Pittsburgh, Pennsylvania. At this multi-day workshop, NIST intends to begin the Framework drafting process alongside industry, suggesting that future workshops will involve meaningful, direct engagement with NIST on the design and implementation of new cybersecurity requirements.

* * *

For more information about the NIST-NTIA request for comments or about Wiltshire & Grannis's cybersecurity practice, please contact Kent Bressie at +1 202 730 1337 or kbressie@wiltshiregrannis.com, Tricia Paoletta at +1 202 730 1314 or tpaoletta@wiltshiregrannis.com, or Madeleine Findley at +1 202 730 1304 or mfindley@wiltshiregrannis.com.