WILTSHIRE & GRANNIS LLP

REGULATORY ADVISORY
12 MARCH 2013

NIST Requests Information for Cybersecurity Framework:
Industry Has Significant Opportunity to Influence Regulatory Process

To implement President Obama's cybersecurity initiative, the National Institute of Standards and Technology ("NIST") has issued a Request for Information ("RFI") as part of its effort to create a set of industry best practices to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). This RFI offers industry its first significant opportunity to provide input on cybersecurity policies and procedures and the impact of additional regulatory obligations. ***Responses to the RFI are due by April 8, 2013***.

The February 12, 2013 Executive Order and 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. (The fact that the European Union recently adopted its Cybersecurity Strategy proposing risk management requirements will create pressure for a harmonized set of requirements for critical infrastructure providers that seek to offer services in both markets.) In the RFI, NIST makes a series of very broad information requests intended to identify cross-sector security best practices, standards, and guidelines applicable to critical infrastructure; to encourage their adoption; and to identify areas for improvement. In particular, NIST requests information in the following areas:

Current Risk Management Practices:

- Policies and procedures currently in use to define, assess, or otherwise address cybersecurity risks;
- Standards, guidelines, and best practices currently available to address risks and the role these standards should play in assessing conformity of cybersecurity measures;
- Current local, state, national, and international cybersecurity regulatory and reporting obligations; and
- Interconnections among different types of critical physical and information infrastructure.

Use of Frameworks, Standards, Guidelines, and Best Practices:

- Policy or other documents developed by international, national, and state governments; industry; and non-government organizations currently applicable to cybersecurity needs and list of sectors/organizations currently using these approaches;
- Limitations of the current approaches and suggestions for modification; and
- Whether sector-specific standards development or a voluntary program should accompany existing frameworks and suggestions as to what relevant U.S. government agencies can do to foster their adoption.

Specific Industry Practices: NIST seeks information about the following specific industry practices: (1) separation of business from operational systems; (2) use of encryption and key management; (3) identification and authorization of users accessing systems; (4) asset identification and management; (5) monitoring and incident detection tools and capabilities; (6) incident handling policies and procedures; (7) mission/system resiliency practices; (8) security engineering practices; and (9) privacy and civil liberties protection. With respect to these specific practices, NIST asks:

- Which practices are widely used and which will be most difficult to implement;
- How the specific practices relate to existing standards and guidelines;
- Which practices are most critical and which might not apply to certain sectors; and
- How organizations can manage risks to privacy and civil liberties arising out of the specific practices.

While threatening to impose significant new regulatory burdens on communications networks, the RFI and Cybersecurity Framework have also created significant regulatory uncertainty about defining and distinguishing between "virtual" and "physical" infrastructure, and could well introduce tension into the commercial relationships between infrastructure owners and providers of so-called "over-the-top" services. The RFI provides a significant opportunity for industry to minimize regulatory burdens by providing input on the implementation of cybersecurity requirements.

During the Cybersecurity Framework development process, NIST will solicit information from interested stakeholders, including critical infrastructure owners and operators, agencies, state and local governments, and others, not just through the solicitation of comments, but also through outreach events and workshops. NIST will hold its first stakeholder meeting on April 3, 2013 at its headquarters in Gaithersburg, Maryland.

Responses to the RFI must be filed by 5:00 p.m. Eastern time on **April 8, 2013**. NIST intends to publish a draft Cybersecurity Framework within eight months.

* * *

For assistance commenting on the NIST RFI or participating in NIST stakeholder outreach, or more information regarding 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.