Morgan Lewis

energy lawflash alert

www.morganlewis.com

Cybersecurity Act of 2012 Introduced

Bill would significantly expand federal regulation of cybersecurity for critical infrastructure protection; NERC CIP requirements likely unaffected.

February 21, 2012

On February 14, a bipartisan group of senators introduced to the U.S. Senate the Cybersecurity Act of 2012, under which the Department of Homeland Security (DHS) would assess the risks and vulnerabilities of critical infrastructure systems and develop security performance requirements for the systems and assets designated as covered critical infrastructure. The bill is sponsored by Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman (I-CT), committee ranking member Susan Collins (R-ME), Commerce Committee Chairman Jay Rockefeller (D-WV), and Select Intelligence Committee Chairman Dianne Feinstein (D-CA). As explained in the statement announcing the measure, "[t]he bill envisions a public-private partnership to secure those systems, which, if commandeered or destroyed by a cyber attack, could cause mass deaths, evacuations, disruptions to life-sustaining services, or catastrophic damage to the economy or national security."

Infrastructure Protection Obligations

Title I of the bill provides the key provisions of the critical infrastructure protection obligations that would be imposed by the bill. Under Title I, DHS, in consultation with entities that own or operate critical infrastructure, the Critical Infrastructure Partnership Advisory Council, the Information Sharing and Analysis Organizations, and other appropriate state and local governments, is required to conduct an assessment of cybersecurity threats, vulnerabilities, and risks to determine which sectors pose the most significant risk. Once the sectors have been prioritized based on risk, DHS, along with the other agencies and organizations, must conduct a cybersecurity risk assessment of the critical infrastructure in each sector. These risk assessments must consider the actual or assessed threat, the threatened harm to health and safety, the threat posed to national security, the risk of damage to other critical infrastructure, the risk of economic harm, and each sector's overall resilience, among other factors. In conducting these assessments, DHS is called upon to cooperate with owners and operators of critical infrastructure.

DHS, in conjunction with the same agencies and organizations, must also develop procedures that will be used to designate certain critical infrastructure at the system or asset level as "covered critical infrastructure," therefore making those systems and assets subject to the cybersecurity requirements developed under the bill. This infrastructure is to be identified based on an analysis of whether damage or unauthorized access to the system or asset could result in any of the following:

- Harm to life-sustaining services that could result in mass casualties or mass evacuation

- Catastrophic economic damage to the United States
- "Severe degradation" of national security

Technology products themselves or services provided in support of such products may not be designated as covered critical infrastructure based solely on the finding that the products are capable of being used in covered critical infrastructure.

Following the identification of covered critical infrastructure, DHS must also develop, on a sector-by-sector basis, cybersecurity performance requirements that require the owners of covered critical infrastructure to remediate the cybersecurity risks identified through the risk assessment performed by DHS for that sector. The bill requires that, in establishing the performance requirements, DHS have a process through which it considers performance requirements proposed by asset owners, voluntary standards development organizations, and other groups, as well as existing industry practices, standards, and guidelines. If DHS determines that the existing or proposed performance requirements are insufficient, DHS is required to develop performance requirements on its own.

Once the covered critical infrastructure is identified and the performance requirements defined, asset owners will be required to take steps to secure the covered critical infrastructure assets and systems, and to that end the bill tasks DHS with promulgating regulations to require covered critical infrastructure owners to do the following:

- Receive notifications of cybersecurity risks
- Implement cybersecurity protections that the owner "determines to be best suited to satisfy" the performance requirements
- Maintain continuity of operations and incident response plans
- Report cybersecurity incidents

Each owner of covered critical infrastructure will be required to certify yearly that it has implemented cybersecurity protections sufficient to satisfy DHS's approved security performance requirements or to submit a third-party assessment regarding compliance with those performance requirements that satisfies certain standards for the training, certification, and independence of the assessors.

The bill provides that DHS may exempt from the performance requirements any system or asset if the owner can demonstrate that the system or asset is sufficiently protected against the risks identified by DHS or that compliance with the performance requirements would not "substantially" improve the security of the system or asset.

Enforcement

The enforcement regime proposed by the bill provides that any federal agency with responsibility for security of the covered critical infrastructure at issue may enforce the regulations. However, DHS itself may enforce the regulations (i) if there is no other appropriate agency, (ii) if DHS is requested to do so by the agency with responsibility for the security of the covered critical infrastructure in question, or (iii) if the agency with responsibility for the security of the covered critical infrastructure fails to take enforcement action as requested by DHS. Civil penalties are available for violations of section 105 of the bill, under which the performance requirements are established. However, no private right of action would exist.

Owners and operators of covered critical infrastructure would be exempt from punitive damages related to identified cybersecurity risks so long as they have implemented security measures that satisfy the performance requirements, are substantially compliant with the performance requirements, and have completed the annual assessments.

Avoiding Duplicative Regulation

While the cybersecurity obligations imposed by this bill would be far-reaching and could conceivably overlap with the Critical Infrastructure Protection (CIP) Reliability Standards approved by the Federal Energy Regulatory Commission (FERC) for certain bulk-power system infrastructure, the bill attempts to carve out existing cybersecurity protections, and provides several mechanisms to ensure that critical infrastructure that is already regulated will not receive duplicative regulation under this proposal.

When developing performance requirements, DHS is required to determine whether there are existing regulations in effect that cover the identified critical infrastructure and address the risks identified by DHS. If such regulations are in place, DHS is instructed to develop performance requirements only if the existing regulations do not provide an appropriate level of security. This will likely require an analysis of the existing CIP Reliability Standards by DHS, including an analysis of whether those standards cover all of the covered critical infrastructure for the electric sector identified by DHS, and whether those standards provide a sufficient level of security to protect against the risks identified by DHS.

Another method by which the existing CIP Reliability Standards framework may remain unchanged is the presidential exemption authority provided under the bill. Pursuant to that provision, the President is authorized to exempt critical infrastructure from these requirements if the appropriate "sector-specific regulatory agency" (FERC for electric infrastructure) "has sufficient specific requirements and enforcement mechanisms to effectively mitigate" the risks identified by DHS.

Additionally, DHS and the other "sector-specific agencies" with responsibility for regulating critical infrastructure security are required to coordinate their efforts to eliminate duplicative reporting or compliance requirements. Similarly, any new rules developed by sector-specific agencies must be coordinated with DHS to ensure that they are consistent with DHS's efforts.

On March 7, Morgan Lewis will be hosting an all-day conference on cybersecurity that will discuss the Cybersecurity Act of 2012 and numerous other topics. View the invitation to access the agenda and to register for the conference.[1]

For more information about the information discussed in this LawFlash, please contact either of the following attorneys:

Washington, D.C.

Stephen M. Spina	202.739.5958	sspina@morganlewis.com
Daniel Skees	202.739.5834	dskees@morganlewis.com

About Morgan, Lewis & Bockius LLP

1. The invitation is also available online at http://www.morganlewis.com/documents/m/Events/2012/ENPG_Cybersecurity-Con_evite_120177.html.

With 22 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.